EXAMINING OBAMACARE'S FAILURES IN SECURITY, ACCOUNTABILITY, AND TRANSPARENCY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 18, 2014

Serial No. 113–156

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

91–961 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
Vacancy

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

EXAMINING OBAMACARE'S FAILURES IN SECURITY, ACCOUNTABILITY, AND TRANSPARENCY

Thursday, September 18, 2014

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, DC.

The committee met, pursuant to notice, at 11:11 a.m., in room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Duncan, Jordan, Chaffetz, Walberg, Lankford, Amash, Meehan, Farenthold, Collins, Meadows, DeSantis, Cummings, Maloney, Clay, Lynch, Connolly, Speier, Cartwright, Kelly, and Lujan Grisham.

Staff present: Ali Ahmad, Professional Staff Member; Melissa Beaumont, Assistant Clerk; David Brewer, Senior Counsel; Steve Castor, General Counsel; John Cuaderes, Deputy Staff Director; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Meinan Goto, Professional Staff Member; Christopher Hixon, Chief Counsel for Oversight; Mark D. Marin, Deputy Staff Director for Oversight; Emily Martin, Counsel; Tamara Alexander, Minority Counsel; Aryele Bradford, Minority Press Secretary; Jennifer Hoffman, Minority Communications Director; Una Lee, Minority Counsel; Juan McCullum, Minority Clerk; Dave Rapallo, Minority Staff Director; and Cecelia Thomas, Minority Counsel.

Chairman ISSA. The committee will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

The Oversight Committee exists to secure two fundamental principles: First, Americans have a right to know that the money Washington takes from them is well-spent; and, second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights.

Our solemn responsibility is to hold government—government—accountable to taxpayers because taxpayers have a right to know what they get from their government. It is our job to work tirelessly, in partnership with citizen watchdogs, to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

Over the past 4 years, the Oversight and Government Reform Committee has conducted vigorous oversight of the implementation of the Affordable Care Act, often called "Obamacare," including the

design and launch of HealthCare.gov. Today the committee focuses on the interconnected issues of security of the Website, accountability within the administration, and, most of all, transparency to the American people.

The Government Accountability Office released a report this week on security of HealthCare.gov. The GAO found the administration failed to take appropriate and sufficient steps to protect HealthCare.gov and associated systems against security and privacy risks. More importantly, the GAO report strongly asserts that security testing is not complete and security weaknesses continue to plague the Website.

One of the principal authors of the GAO report will testify before us today.

The committee has released a report detailing several breakdowns in both accountability within the administration and transparency to the American people during the design and implementation of HealthCare.gov. It is important to understand that, with private-sector, high-profile losses of information due to hackers, there are huge repercussions to those companies, and the government often comes in and further victimizes the companies who have, in fact, been victimized by hackers. And yet, when the government fails to protect involuntarily taken personally identifiable information, there is nobody but people on this dais to try to hold government accountable.

Documents obtained by this committee show factions developed within the agency in charge of implementing Obamacare, the Centers for Medicare and Medicaid Services, or CMS. These factions fought over several issues, including over Website security.

CMS often fought to keep information from their colleagues within the larger Department of Health and Human Services. And, additionally, the administration endeavored to keep the truth and the true nature of the Website's problems out of the public eye. Following the collapse of HealthCare.gov, administration officials refused to admit to the public that the Website was not on track to launch without significant functionality problems and substantial security risks.

Last month, CMS denied the Associated Press access to security documents requested under the Freedom of Information Act. Even more recently, CMS refused to provide the Government Accountability Office documents related to the 13 incidents that we are going to hear about in vague detail here today.

I want to make something very clear. Refusal to cooperate with the GAO, a nonpartisan, government-created entity, refusal to allow access by the whistleblowers under Freedom of Information Act, and refusal to cooperate with even the inspectors general, something we saw here just a few days ago with 47 inspector generals out of 73 complaining with the lack of access even within the executive branch, this is not the most transparent administration in history. And, certainly, the transparency we see here today was only done under subpoena.

We will probably hear today that CMS has offered to brief GAO on these 13 incidents. It is not acceptable after the public scrutiny reveals that they exist and they have been denied, on the eve of a hearing and only after an audit is completed, to then say, "We

would be glad to brief you." That is unacceptable and, quite frankly, one of the most disingenuous things I have ever seen. There were 5 months during the audit to comply with a reasonable request by the Government Accountability Office, and it wasn't done.

Questions of security can no longer be easily dismissed by the administration. In late July, HealthCare.gov suffered a malicious attack from a hacker, and it took nearly 2 months for CMS to identify the intrusion. CMS Administrator Marilyn Taverner, who is with us today, will testify, and we will discuss that in addition to the GAO report.

I am sure we will hear that there was no loss of data, that this was not the main site, and so on. That doesn't change the fact that security risks exist whenever you fail to secure not just the main site but backdoors. Too often, backdoors have been what we have discovered.

In the case of another investigation of this committee, we discovered that the backdoors were something as simple, in one case, as a stolen laptop on which those who stole it later added peer-to-peer software, which then made information on that data base available to the public, potentially. The Federal Trade Commission opened an investigation, and a plaintiff's trial lawyer sued and won money on behalf of people whose information was never actually released. But, in fact, both the government and plaintiff's bars thoroughly enjoyed going after a nonprofit AIDS clinic. I cannot and will not allow our government to put itself at a different standard of accountability.

Last month, the Center for Medicare and Medicaid Services informed the committee that, once again, there were lost emails in response to the committee's subpoena and documents related to HealthCare.gov. This is not an uncommon pattern; this is a pattern of predictability. This administration has not complied with nor caused their key executives, including political appointees, to comply with the Federal Records Act. Administrator Tavenner admitted to deleting her own emails during the time period of Obamacare implementation.

Madam, your actions hinder Congress' investigation and also prevent the public from accessing information under the Freedom of Information Act. It appears as though this administration holds itself to a different level of compliance with historic Federal documents than the last administration or any administration since the passage.

We are also today joined by the Department of Homeland Security's U.S. Computer Emergency Readiness Team, or CERT. The committee has concerns about the team's transparency regarding a hack reported earlier this month.

The administration has already spent a billion dollars on a Website that is still not fully operational and fully not secure. The same government officials responsible for the lack of transparency and accountability a year ago remain in the position of authority.

Questions of security, accountability, and transparency go beyond whether or not you support the President's healthcare law. Many of these issues are not limited to health care and mirror the transparency and accountability concerns raised, again, by 47 out of 73

inspector generals in an unprecedented letter to this and other committees of Congress in August.

Minutes before HHS announced publicly on September 4th that HealthCare.gov had experienced a malicious attack in July of this year, an HHS official contacted my office to give them limited details of the successful hack. During the brief call, HHS gave my staff the name and phone number of a contact at the Department of Homeland Security and suggested my staff contact DHS for more information about the hack itself and the government's response to the hack.

My staff reached out to HHS's suggested contact at DHS on Monday of last week, followed up on Tuesday, and were told that DHS was running—and in parentheses, the request—back with HHS to see if we can all jointly get on the phone, seeing if tomorrow will work. However, my staff followed up on Wednesday and Friday and then on Monday and Tuesday, with no response from DHS.

I would like to note that, despite a week of persistent emails from my staff, DHS was unable to make time to brief our committee even by phone. However, 2 days ago, the minority staff notified me that they were asking for our witness today, DHS, to appear as a witness at today's hearing. I accepted it even though, clearly, this is a witness from an organization that has refused to answer questions or cooperate with the investigation.

When the minority staff reached out to ask if DHS would appear as a witness, DHS was able to produce a witness prepared, apparently in detail, to provide testimony before this hearing today. However, DHS has still not arranged to properly brief our staff or to answer questions that we will be asking here today.

I would like to introduce into the record at this time the correspondence between the staff and DHS as an example of what appears to be a very different treatment from this administration to a request from the majority staff versus a request from the minority staff. And, without objection, it will be placed in the record.

Chairman ISSA. Let's cut to the chase. I have with me three witnesses. Two, very clearly, are not part of transparency in government.

I have no doubt that your organizations have worked diligently with the minority to try to make this hearing good for you. It is not our job to try to make this hearing bad for you, but the American people deserve the truth, not a cozy relationship between the people of your President's party, in covering up the ongoing failure to secure a Website that cost over a billion dollars.

And, with that, I am pleased to recognize the ranking member for his opening Statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

First of all, I want to apologize for running late. The Speaker asked us to be at a joint session of Congress to hear the President of the Ukraine, and many of us were there.

One of our most important jobs in Congress is to help protect the interests of the American people. They demand that government and private companies safeguard their personal information, safeguard their Social Security numbers, their credit cards, and their health information. Nobody wants to get a call from a credit card company saying, your personal information has been compromised.

It could upend your entire life, and it can cause serious financial problems for years.

I believe our committee has the potential to perform a very valuable function in this area. With our extremely broad jurisdiction over multiple Federal agencies and corporate entities, we can help promote robust security standards across the entire government and private sector. To date, however, we have not fulfilled this potential.

Today's hearing is our 29th on the Affordable Care Act and our sixth on HealthCare.gov. I completely agree that the ACA Website must be secure. That is why I am so heartened that, despite all of the challenges with the rollout last year, nobody's personal information has been compromised to date as a result of a malicious attack. Nobody's personal information has been compromised to date as a result of a malicious attack. Now, that could change, so we have to remain vigilant. After all, this is our watch. But, so far, no attacks have been successful in that regard.

There certainly have been attempts. Last week, the Centers for Medicare and Medicaid Services reported that hackers uploaded malware onto a server. But there are several key facts to know about the attack. First, it was not directed at HealthCare.gov alone but a much wider universe of targets. Second, the server that was attacked was a test server that had no personal information on it. Third, the most important, nobody's personal information was compromised as a result.

That incident was investigated by the United States Computer Emergency Readiness Team and the Department of Homeland Security. The director of that team, in her written testimony for today, reports, and I quote, "There is no indication that any data was compromised as a result of this intrusion," end of quote.

Although our committee has spent a tremendous amount of time focusing on the Affordable Care Act and its Website, where no cyber attacks have compromised anyone's personal information to date, we have been disregarding much more serious attacks that have actually compromised a massive amount of personal information of our constituents. We are talking about hundreds of millions of people—hundreds of millions.

For example, on January 14th, more than 8 months ago, I sent a letter requesting a bipartisan hearing with senior officials from Target. As I wrote, "Up to 110 million Americans were subjected to one of the most massive information technology breaches in history when their credit, debit, and other personal information reportedly was compromised," end of quote.

On September 9th, I sent a letter requesting a bipartisan hearing on a major data security breach at Community Health Systems, the Nation's largest for-profit hospital chain. I explained that, quote, "hackers broke into its computers and stole data on 4.5 million patients," end of quote. As I noted, this was, quote, "the largest hacking-related health information breach ever reported," end of quote.

On September 11th, I sent a letter requesting a bipartisan hearing to examine the recent security breach at Home Depot, where our constituents shop. I explained that Home Depot, quote, "has more stores in the United States and a higher total annual sales volume than Target," end of quote. And, quote, "it appears to have

experienced a data security breach for a longer period of time than the data security breach that occurred at Target," end of quote.

And just this Monday, I sent a letter requesting a deposition with the CEO of USIS, the company that conducts more background checks for the government than any other contractor and which had its own breach this summer. And I wrote, and I quote, "Although press accounts have reported that the attack may have compromised the personal information of up to 27,000 Federal employees, government cybersecurity experts now believe this number is a floor, not a ceiling," end of quote. I am talking about the people who work on Capitol Hill. I am talking about the people who work for the Federal Government—up to possibly 27,000.

In response, I received a letter back from the chairman yesterday thanking me for my requests over the past year and acknowledging, and I quote, "These serious incidents merit further review," end of quote.

Mr. Chairman, I thank you for that. I hope we can start on this right away. After all, these are our constituents.

Let me close by highlighting that this is much broader than HealthCare.gov—much broader. GAO, which is also represented here today, warns that the number of cyber attacks is increasing against targets across the Federal Government, and, obviously, the same is true of the private sector. So oversight is certainly called for, and I hope that our committee seizes the opportunity and rises to the challenge.

With that, I yield back.

Chairman ISSA. I thank the gentleman.

Chairman ISSA. At this time, I would like to place in the record examples of State attorney generals' prosecution and relief on private-sector and even public-sector entities and the history of their going after entities for financial damages that allow breaches.

Without objection, so ordered.

Mr. LYNCH. Mr. Chairman, can I get a copy of that?

Chairman ISSA. We will make copies available to all of you. It is all public information. And we did include both your Massachusetts attorney general, Vermont's attorney general, and Maryland's attorney general's actions on behalf of your constituents.

Mr. LYNCH. I appreciate that. Thank you.

Chairman ISSA. Members may have 7 days in which to submit opening Statements for the record.

Chairman ISSA. We now welcome our witnesses today.

Mr. Gregory Wilshusen is the Director of Information Security Issues at the Government Accountability Office and the subject, obviously, of some frustration before he got here today.

Ms. Marilyn Tavenner is the Administrator for the Centers for Medicare and Medicaid Services at the Department of Health and Human Services, thereafter called "CMS" today.

Ms. Ann Barron-DiCamillo is the Director of the U.S. Computer Emergency Readiness Team at the Department of Homeland Security, hereafter probably called "CERT."

Pursuant to the committee rules, all witnesses are to be sworn. Would you please all rise, raise your right hands to take the oath?

Do you solemnly swear or affirm that the testimony you are about to give today will be the truth, the whole truth, and nothing but the truth?

Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

In order to allow sufficient time for your panel and then what I suspect will be a robust series of questions, I would ask that you limit your opening Statement to 5 minutes, although your entire Statements, including additional information that you may want to make available, will be placed in the record.

So, Mr. Wilshusen, please continue.

WITNESS STATEMENTS

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Thank you, Mr. Chairman.

Chairman Issa, Ranking Member Cummings, and members of the committee, I am pleased to be here today as you examine the implementation of the Patient Protection and Affordable Care Act.

As you know, the act requires the establishment of a health insurance marketplace in each State to assist consumers and small businesses in comparing, selecting, and enrolling in the health benefit plans offered by participating private insurers.

CMS is responsible for creating a federally facilitated marketplace for States that do not establish their own. This marketplace is supported by an array of IT systems, including HealthCare.gov, the Website that provides the consumer portal to the marketplace.

My Statement today will summarize the key findings from our recently issued work on the security and privacy protections of the systems supporting HealthCare.gov.

But before I proceed, Mr. Chairman, if I may, I would like to recognize several members of my team who are instrumental in performing this work. With me today is John de Ferrari, Marisol Cruz, Justin Palk, and Mark Canter. In addition, members from GAO's e-Security Lab also participated: Lon Chin, Wes Coile, Duc Ngo, and Michael Stevens.

Chairman ISSA. Could you all please stand so that we can all, at least for a moment, realize your contribution?

Thank you. You may continue.

Mr. WILSHUSEN. Thank you.

HealthCare.gov-related systems, including the core systems of the federally facilitated marketplace and Federal Data Services Hub, represent a complex system that interconnects a broad range of Federal agency systems, State agencies and their systems, and other entities, such as contractors and issuers of health plans. The complexity and interconnectivity inherently introduces risk. Ensuring the security of such a system poses a significant challenge.

To meet that challenge, CMS has undertaken a number of activities to enhance the security and privacy of systems supporting HealthCare.gov. For example, CMS has developed and documented security-related policies and procedures. It developed a process for remediating identified security weaknesses. CMS also created interconnection security agreements with the Federal agencies with

which it exchanges information. And it instituted certain required privacy protections, such as notifying the public of the types of information that will be maintained in the system.

However, CMS has not fully or effectively implemented key technical security controls to sufficiently safeguard the confidentiality, integrity, and availability of the federally facilitated marketplace and its information. For example, CMS did not always require or enforce strong password controls, did not sufficiently restrict systems from accessing the Internet, and did not consistently implement patches in a timely manner.

CMS also had shortcomings in its information security and privacy management program. For example, system security plans for the federally facilitated marketplace and data hub generally contained most required information, but each plan was missing key security information. CMS had also undertaken a series of security-related testing activities that began in 2012, yet these control assessments did not fully identify and test all relevant controls prior deploying the systems. In addition, CMS did not fully assess privacy risk in its privacy impact assessments and had not fully established an alternate processing site for HealthCare.gov systems to ensure that they could be recovered in the event of a disruption or disaster.

To assist CMS, we made six recommendations addressing the shortcomings with the information security and privacy program and 22 recommendations to resolve technical security weaknesses related to access controls and configuration management. CMS concurred or partially concurred with all 28 recommendations and noted that it was taking actions to address each of them.

In conclusion, while CMS has taken important steps to apply security and privacy safeguards to HealthCare.gov and its supporting systems, weaknesses remain that put these systems and the sensitive personal information they contain at an increased and unnecessary risk of compromise.

Mr. Chairman, Ranking Member Cummings, and members of the committee, this concludes my opening Statement. I would be happy to answer your questions.

Chairman ISSA. Thank you.

[Prepared Statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony
Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 11:00 a.m. ET
Thursday, September 18, 2014

HEALTHCARE.GOV

Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses

Statement of Gregory C. Wilshusen, Director,
Information Security Issues

GAO Highlights

Highlights of GAO-14-871T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

PPACA requires the establishment of health insurance marketplaces in each state to assist individuals in comparing, selecting, and enrolling in health plans offered by participating issuers. CMS is responsible for overseeing these marketplaces, including establishing a federally facilitated marketplace in states that do not establish their own. These marketplaces are supported by an array of IT systems, including Healthcare.gov, the website that serves as the consumer portal to the marketplace.

This statement is based on two September 2014 reports examining the security and privacy of the Healthcare.gov website and related systems. The specific objectives of this work were to (1) describe the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assess the effectiveness of programs and controls implemented by CMS to protect the security and privacy of the information and IT systems supporting Healthcare.gov.

What GAO Recommends

In its September 2014 reports GAO made 6 recommendations to HHS to implement security and privacy controls to enhance the protection of systems and information related to Healthcare.gov. In addition, GAO made 22 recommendations to resolve technical weaknesses in security controls. HHS agreed with 3 of the 6 recommendations, partially agreed with 3, agreed with all 22 technical recommendations, and described plans to implement them.

View GAO-14-871T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

September 18, 2014

HEALTHCARE.GOV

Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses

What GAO Found

Enrollment through Healthcare.gov is supported by the exchange of information among many systems and entities. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key information technology (IT) systems supporting Healthcare.gov. These include, among others, the Federally Facilitated Marketplace (FFM) system, which facilitates eligibility and enrollment, plan management, and financial management, and the Federal Data Services Hub, which acts as the single portal for exchanging information between the FFM and other systems or external partners. CMS relies on a variety of federal, state, and private-sector entities to support Healthcare.gov activities. For example, it exchanges information with the Department of Defense, Department of Homeland Security, Department of Veterans Affairs, Internal Revenue Service, Office of Personnel Management, Peace Corps, and the Social Security Administration to help determine applicants' eligibility for healthcare coverage and/or financial assistance. Healthcare.gov-related systems are also accessed and used by CMS contractors, issuers of qualified health plans, state agencies, and others.

While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put these systems and the sensitive personal information they contain at risk. Specifically, CMS established security-related policies and procedures for Healthcare.gov, including interconnection security agreements with the federal agencies with which it exchanges information. It also instituted certain required privacy protections, such as notifying the public of the types of information that will be maintained in the system. However, weaknesses remained in the security and privacy protections applied to Healthcare.gov and its supporting systems. For example, CMS did not

- ensure system security plans contained all required information, which makes it harder for officials to assess the risks involved in operating those systems;
- analyze privacy risks associated with Healthcare.gov systems or identify mitigating controls;
- perform comprehensive security testing of the FFM system, reducing assurance that security controls are operating as intended; and
- fully establish an alternate processing site for Healthcare.gov systems to ensure that they could be recovered in the event of a disruption or disaster.

In addition, a number of weaknesses in specific technical security controls jeopardized Healthcare.gov-related systems. These included certain systems supporting the FFM not being restricted from accessing the Internet and inconsistent implementation of security patches, among others.

An underlying reason for many of these weaknesses is that CMS did not establish a shared understanding of security roles and responsibilities with all parties involved in securing Healthcare.gov systems. Until these weaknesses are addressed, the systems and the information they contain remain at increased risk of unauthorized use, disclosure, modification, or loss.

Chairman Issa, Ranking Member Cummings, and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the implementation of the Patient Protection and Affordable Care Act (PPACA) and Healthcare.gov. As you know, PPACA requires the establishment of a health insurance marketplace in each state to assist consumers and small businesses in comparing, selecting, and enrolling in health plans offered by participating private insurers. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) is responsible for overseeing the establishment of these marketplaces, including creating a federally facilitated marketplace for states that do not establish their own. This marketplace is supported by an array of information technology (IT) systems, including Healthcare.gov, the website that provides the consumer portal to the marketplace, and related data systems.

To facilitate the enrollment process, Healthcare.gov and its supporting IT systems must collect and process individuals' sensitive personal information, such as employment and tax information. Portions of this information may be accessed by multiple organizations, including CMS, other federal agencies, insurers, and state agencies. Accordingly, ensuring the security and privacy of this information is critically important.

My statement today will summarize the key findings from our recently issued work on the privacy and security protections of the Healthcare.gov website and related IT systems.[1] Our specific objectives for that review were to (1) describe the planned exchanges of information between the Healthcare.gov website, supporting IT systems, and the federal, state, and other organizations that are providing or accessing that information, including special arrangements for handling tax information in compliance with legal requirements, and (2) assess the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov. More details on our scope and methodology are contained in the reports.

[1]GAO, *Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls*, GAO-14-730 (Washington, D.C.: Sept. 17, 2014). We issued a second report that had limited distribution because of the sensitive nature of the information it contained.

The work on this statement was based on was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

PPACA directed each state to establish a state-based health insurance marketplace[2] for individuals to enroll in private health insurance plans, apply for income-based financial assistance, and, as applicable, obtain a determination of their eligibility for other health coverage programs, such as Medicaid or the State Children's Health Insurance Program (CHIP). For states that did not establish a marketplace, PPACA required the federal government to establish and operate a marketplace for that state, referred to as the federally facilitated marketplace. For plan year 2014, 17 states elected to establish their own marketplace, and CMS operated a federally facilitated marketplace or partnership marketplace[3] for 34 states.[4]

The act required the marketplaces to be operational on or before January 1, 2014, and Healthcare.gov began facilitating enrollments on October 1, 2013, at the beginning of the first annual open enrollment period established by CMS. The initial open enrollment period ended on April 15, 2014.

[2]PPACA requires the establishment of health insurance exchanges—marketplaces where eligible individuals can compare and select among insurance plans offered by participating issuers of health coverage. In this statement, we use the term "marketplace."

[3]A partnership marketplace is a variation on the federally facilitated marketplace. HHS establishes and operates this type of exchange with states assisting HHS in carrying out certain functions of that marketplace.

[4]These numbers include the 50 states plus the District of Columbia.

Laws and Regulations Establish Requirements for Protecting the Security and Privacy of Personally Identifiable Information

Requirements for ensuring the security and privacy of individuals' personally identifiable information (PII),[5] such as that collected and processed by Healthcare.gov and related systems, have been established by a number of federal laws and guidance. These include the following:

- The Federal Information Security Management Act of 2002 (FISMA), which requires each federal agency to develop, document, and implement an agency-wide information security program.
- National Institute of Standards and Technology (NIST) guidance and standards, which are to be used by agencies to, among other things, categorize their information systems and establish minimum security requirements.
- The Privacy Act of 1974, which places limitations on agencies' collection, access, use, and disclosure of personal information maintained in systems of records.
- The Computer Matching Act, which is a set of amendments to the Privacy Act requiring agencies to follow specific procedures before engaging in computerized comparisons of records for establishing or verifying eligibility or recouping payments for federal benefit programs.
- The E-Government Act of 2002, which requires agencies to analyze how personal information is collected, stored, shared, and managed before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form.
- The Health Insurance Portability and Accountability Act of 1996, which requires the adoption of standards for the electronic exchange, privacy, and security of health information.
- The Internal Revenue Code, which provides for the confidentiality of tax returns and return information.

[5]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

- IRS Publication 1075, which establishes security guidelines for safeguarding federal tax return information used by federal, state, and local agencies.

HHS Responsibilities for Overseeing Implementation of PPACA and Ensuring Security and Privacy of Health Insurance Marketplaces

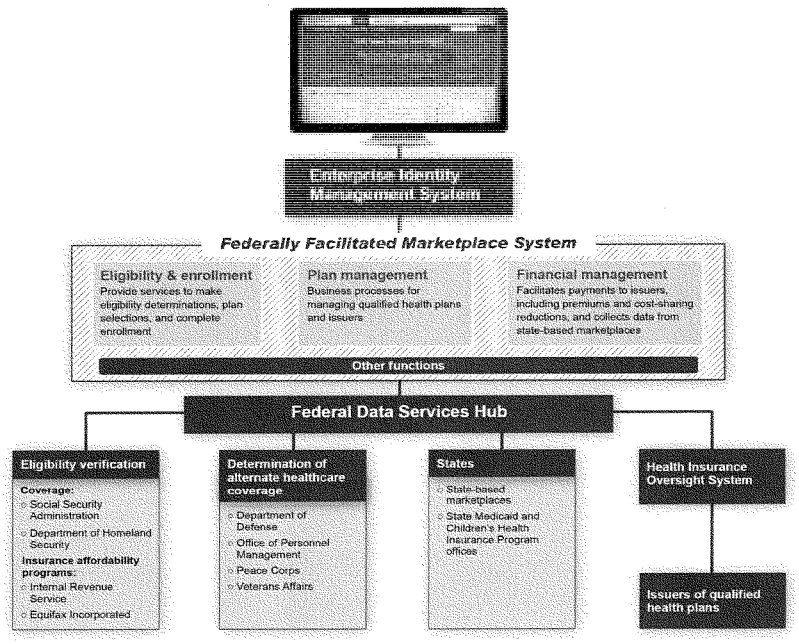
Under FISMA, the Secretary of HHS has overall responsibility for the department's agency-wide information security program; this responsibility has been delegated to the department's Chief Information Officer (CIO). The HHS CIO is also responsible for the department's response to information security incidents and the development of privacy impact assessments for the department's systems.

The CMS Center for Consumer Information and Insurance Oversight has overall responsibilities for federal systems supporting the federally facilitated marketplace and for overseeing state marketplaces. Further, security and privacy responsibilities for Healthcare.gov and supporting systems are shared among several offices and individuals within CMS, including the CIO, the Chief Information Security Officer, component-level information systems security officers, the CMS Senior Official for Privacy, and the CMS Office of e-Health Standards Privacy Policy and Compliance. In particular, the CMS CIO is responsible for implementing and administering the CMS information security program, which covers the systems developed by CMS to satisfy PPACA requirements. The Chief Information Security Officer is responsible for, among other things, ensuring the assessment and authorization of all systems and the completion of periodic risk assessments, including annual security testing and security self-assessments.

Marketplace Enrollment Is Facilitated by Data Exchanges among Many Interconnected Systems and Partners

The process of enrolling for insurance through Healthcare.gov is facilitated by a number of major systems managed by CMS. Figure 1 shows the major entities that exchange data in support of marketplace enrollment in qualified health plans and how they are connected.

Figure 1: Overview of Healthcare.gov and Its Supporting Systems



Source: GAO analysis of CMS data. | GAO-14-871T

The major systems that facilitate enrollment include the following:

The Healthcare.gov website: This serves as the user interface for individuals to obtain coverage through a federally facilitated marketplace. It has two major functions: (1) providing information about PPACA health

insurance reforms and health insurance options and (2) facilitating enrollment in coverage.

Enterprise Identity Management System: This system allows CMS to verify the identity of an individual applying for coverage and establish a login account for that user. Once an account is created using a name and e-mail address, the person's identity is confirmed using additional information, which can include a Social Security number, address, phone number, and date of birth.

Federally Facilitated Marketplace System (FFM): This system consists of three major modules to facilitate (1) eligibility and enrollment, (2) plan management, and (3) financial management. For eligibility, an applicant's information is collected to determine whether they are eligible for insurance coverage and financial assistance. Once eligibility is determined, the system allows the applicant to view, compare, select, and enroll in a qualified health plan. The plan management module is to provide state agencies and issuers of qualified health plans with the ability to submit, certify, monitor, and renew qualifying health plans. The financial management module is to facilitate payments to health insurers, among other things. From a technical perspective, the FFM system relies on "cloud-based" data processing and storage services from private-sector vendors.

Federal Data Services Hub: This system acts as a single portal for exchanging information between the FFM system and other systems or external partners, which include other federal agencies, state-based marketplaces, other state agencies, other CMS systems, and issuers of qualified health plans. The data hub supports, among other things, real-time eligibility queries, transfer of applicant and taxpayer information, exchange of enrollment information with plan issuers, monitoring of enrollment information, and submission of health plan applications.

Healthcare.gov-related activities are also supported by other CMS systems, including a data warehouse system to provide reporting and performance metrics; the Health Insurance Oversight System, which provides an interface for issuers of qualified health plans to submit information about qualifying health plans; and a general accounting system that handles payments associated with advance premium tax credits and cost-sharing reductions.

In addition, CMS relies on a variety of federal, state, and private-sector entities to support Healthcare.gov-related activities, and these entities exchange information with CMS's systems:

- Federal agencies such as the Social Security Administration (SSA), Department of Homeland Security (DHS), and Internal Revenue Service (IRS), along with Equifax, Inc. (a private-sector credit agency under contract with CMS) provide or verify information used in making determinations of a person's eligibility for coverage and financial assistance.
- The Department of Defense (DOD), Office of Personnel Management (OPM), Peace Corps, and Department of Veterans Affairs (VA) assist in determining whether a potential applicant has alternate means for obtaining minimum essential coverage.
- State-based marketplaces may rely on the FFM system for certain functions, and state Medicaid and CHIP agencies may connect to the FFM to exchange enrollment data, which are typically routed through CMS's data hub.
- In addition to accessing the plan management and financial management modules of the FFM, issuers of qualified health plans receive information from the system when an individual completes the application process.
- Agents and brokers may access the Healthcare.gov website on behalf of applicants.
- To facilitate offline, paper-based applications, CMS contracted with a private-sector company for intake, routing, review, and troubleshooting of paper applications for enrollment into health plans and insurance affordability programs.

CMS Established a Security and Privacy Program for Healthcare.gov and Related Systems, but Actions Are Needed to Resolve Weaknesses

While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put the personal information these systems collect, process, and maintain at risk of inappropriate modification, loss, or disclosure. The agency needs to take a number of actions to address these deficiencies in order to better protect individuals' personally identifiable information.

CMS established security-related policies and procedures for Healthcare.gov. Specifically, it

- assigned overall responsibility for securing the agency's information and systems to appropriate officials, including the agency CIO and Chief Information Security Officer, and designated information system security officers to assist in certifying particular CMS systems;
- documented information security policies and procedures to safeguard the agency's information and systems;
- developed a process for planning, implementing, evaluating, and documenting remedial actions to address identified information security deficiencies; and
- established interconnection security agreements with the federal agencies with which it exchanges information, including DOD, DHS, IRS, SSA, and VA; these agreements identify the requirements for the connection, the roles and responsibilities of each party, the security controls protecting the connection, the sensitivity of the data to be exchanged, and the required training and background checks for personnel with access to the connection.

In addition, CMS took steps to protect the privacy of applicants' information. For example, it

- published and updated a system-of-records notice for Healthcare.gov that addressed required information such as the types of information that will be maintained in the system and the external entities that may receive such information without affected individuals' explicit consent;
- developed basic privacy training for all staff and role-based training for staff who have access to PII while executing their routine duties; and
- established an incident-handling and breach response plan and an incident response team to manage responses to privacy incidents,

identify trends, and make recommendations to HHS to reduce risks to PII.

However, when Healthcare.gov was deployed in October 2013, CMS accepted increased security risks because of the following:

- CMS allowed four states to connect to the data hub even though they had not completed all CMS security requirements. These states were given a 60-day interim authorization to connect, because CMS officials regarded this as a mission-critical need. Subsequently, all four states addressed the weaknesses in their security assessments and were granted 3-year authorizations.
- CMS authorized the FFM system to operate even though all the security controls had not been tested for a fully integrated version of the system. This authority to operate was granted for 6 months, on the condition that a full security assessment was conducted within 60 to 90 days of October 1, 2013. In December 2013, an assessment of the eligibility and enrollment module was conducted. However, the plan management and financial management modules, which had not yet been fully developed, were not tested.

CMS Has Not Fully Implemented Security and Privacy Management Controls

Although CMS developed and documented security policies and procedures, it did not fully implement required actions before Healthcare.gov began collecting and maintaining PII from individual applicants:

- **System security plans were not complete.** While system security plans for the FFM and data hub incorporated most of the elements specified by NIST, each was missing or had not completed one or more relevant elements. For example, the FFM security plan did not define the system's accreditation boundary, or explain why five of the security controls called for by NIST guidance were determined not to be applicable. Without complete system security plans, agency officials will be hindered in making fully informed judgments about the risks involved in operating those systems.
- **Interconnection agreements were not all complete.** CMS had not completed security documentation governing its interconnection with Equifax, Inc., but instead was relying on a draft data use agreement that had not been fully approved within CMS. This makes it more difficult for agency officials to ensure that adequate security controls are in place to protect the connection.

- **Privacy risks were not assessed.** In completing privacy impact assessments for the FFM and data hub, CMS did not assess risks associated with the handling of PII or identify mitigating controls to address such risks. Without such an analysis, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems.

- **Interagency agreements governing data exchanges were not complete.** CMS established computer matching agreements with DHS, DOD, IRS, SSA, and VA for its data exchanges to verify eligibility for healthcare coverage and premium tax credits; however, it had not established such agreements with OPM or the Peace Corps. This increases the risk that appropriate protections will not be applied to the PII being exchanged with these agencies.

- **Security testing was not complete.** While CMS has undertaken, through its contractors and at the agency and state levels, a series of security-related testing activities for various Healthcare.gov-related systems, these assessments did not effectively identify and test all relevant security controls prior to deploying the systems.

  For example, the assessments of the FFM did not include all the security controls specified by NIST and CMS, such as incident response controls and controls specified for physical and environmental protection. In addition, CMS could not demonstrate that it had tested all the security controls specified in the FFM's October 2013 security plan, and it did not test all the system's components before deployment or test them on the integrated system. Testing of all deployed eligibility and enrollment modules and plan management modules did not occur until March 2014, and as of June 2014 FFM testing remained incomplete. Without comprehensive testing, CMS lacks assurance that security controls for the FFM system are working as intended.

- **Alternate processing site was not fully established.** CMS developed and documented contingency plans for the FFM and data hub that identified activities, resources, responsibilities, and procedures needed to carry out operations during prolonged disruptions of the systems. It also established system recovery priorities, a line of succession based on the type of disaster, and specific procedures on how to restore both systems and their associated applications in the event of a disaster. However, although the contingency plans designated a site at which to recover the systems, this site had not been established. Specifically, according to

CMS, data supporting the FFM were being backed up at the recovery site, but backup systems are not otherwise supported there, limiting the facility's ability to support disaster recovery efforts.

Security Control Weaknesses Could Threaten Healthcare.gov Information and Systems

CMS did not effectively implement or securely configure key security controls on the systems supporting Healthcare.gov. For example:

- Strong passwords (i.e., passwords of sufficient length or complexity) were not always required or enforced on systems supporting the FFM. This increases the likelihood that an attacker could gain access to the system.
- Certain systems supporting the FFM were not restricted from accessing the Internet, increasing the risk that unauthorized users could access data from the FFM network.
- CMS did not consistently apply security patches to FFM systems in a timely manner, and several critical systems had not been patched or were no longer supported by their vendors. This increased the risk that servers supporting the FFM could be compromised through exploitation of known vulnerabilities.
- One of CMS's contractors had not properly secured its administrative network, which could allow for unauthorized access to the FFM network.

In addition to these weaknesses, we also identified weaknesses in security controls related to boundary protection, identification and authentication, authorization, and configuration management. Collectively, these weaknesses put Healthcare.gov systems and the information they contain at increased and unnecessary risk of unauthorized access, use, disclosure, modification, and loss.

CMS Had Not Established a Shared Understanding of How Security Was to Be Implemented for Healthcare.gov-Related Systems

The security weaknesses we identified occurred in part because CMS did not ensure that the multiple parties contributing to the development of the FFM system had a shared understanding of how security controls were to be implemented. Specifically, CMS and contractor staff did not always agree on how security controls for the FFM were to be implemented or who was responsible for ensuring they were functioning properly. For example, although CMS identified one subcontractor as responsible for managing firewall rules, this responsibility was not included in the subcontractor's statement of work, and staff for the subcontractor said that this was the responsibility of a different contractor. Without ensuring

agreement on security roles and responsibilities, CMS has less assurance that controls will function as intended, increasing the risk that attackers could compromise the system and the data it contains.

CMS Should Act to Improve Security and Privacy Protections for Healthcare.gov

In our September 2014 report, we made the following six recommendations aimed at improving the management of the security of Healthcare.gov:

1. Ensure that system security plans for the FFM and data hub contain all information recommended by NIST.
2. Ensure that all privacy risks associated with Healthcare.gov are analyzed and documented in privacy impact assessments.
3. Develop computer matching agreements with OPM and the Peace Corps to govern data that are being compared with CMS data to verify eligibility for advance premium tax credits and cost-sharing reductions.
4. Perform a comprehensive security assessment of the FFM, including the infrastructure, platform, and all deployed software elements.
5. Ensure that the planned alternate processing site for the systems supporting Healthcare.gov is established and made operational in a timely fashion.
6. Establish detailed security roles and responsibilities for contractors, including participation in security control reviews, to better ensure effective communication among individuals and entities with responsibility for the security of the FFM and its supporting infrastructure.

In an associated report with limited distribution, we also made 22 recommendations to resolve technical security weaknesses related to access controls, configuration management, and contingency planning.

Implementing these recommendations will enable HHS and CMS to better ensure that Healthcare.gov systems and the information they collect and process are effectively protected from threats to their confidentiality, integrity, and availability.

In its comments on our draft reports, HHS concurred with 3 of the 6 recommendations to fully implement its information security program, partially concurred with the remaining 3 recommendations, and concurred with all 22 of the recommendations to resolve technical weaknesses in

security controls, describing actions it had under way or planned related to each of them.

In conclusion, Healthcare.gov and its related systems represent a complex system of systems that interconnects a broad range of federal agency systems, state agencies and systems, and other entities, such as contractors and issuers of health plans. Ensuring the security of such a system poses a significant challenge. While CMS has taken important steps to apply security and privacy safeguards to Healthcare.gov and its supporting systems, significant weaknesses remain that put these systems and the sensitive, personal information they contain at risk of compromise. Given the complexity of the systems and the many interconnections among external partners, it is particularly important to analyze privacy risks, effectively implement technical security controls, comprehensively test the security controls over the system, and ensure that an alternate processing site for the systems is fully established.

Chairman Issa, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be pleased to answer any questions you have.

Contact and Staff Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Other key contributors to this testimony include John de Ferrari, Lon Chin, West Coile, and Duc Ngo (assistant directors); Mark Canter; Marisol Cruz; Sandra George; Nancy Glover; Torrey Hardee; Tammi Kalugdan; Lee McCracken; Monica Perez-Nelson; Justin Palk; and Michael Stevens.

Chairman ISSA. Ms. Tavenner?

STATEMENT OF THE HON. MARILYN TAVENNER

Ms. TAVENNER. Chairman Issa, Ranking Member Cummings, members of the committee, thank you for the opportunity to be here today.

And I want to makeeveryone aware that CMS strives to be as responsive as possible. I understand that we have already provided over 140,000 pages of documents to this committee. Transparency is important, and that is why I am pleased to be here today and have the opportunity to answer your questions. And we will continue to produce documents.

In the almost 5 years that I have had the privilege to work at CMS, my focus has been on how we can best serve our beneficiaries, including seniors on Medicare, adults and children on Medicaid and CHIP, and consumers enrolling in the marketplace. When I come to work each day, I work to expand coverage and competition, reduce cost, improve quality in ways that make a difference in people's lives.

And we are making real and important progress. As of August 15th this year, we have 7.3 million Americans enrolled in the health insurance marketplace coverage, and these are individuals who have paid their premiums. We are encouraged by the numbers of consumers who have paid their premiums and continue to enroll in the marketplace coverage every day through special enrollment periods.

This is the most recent count of people who have coverage throughout the marketplace. Each month, this number will change slightly as consumers transition in and out of coverage as their life circumstances change—everything from getting a new job to moving to a new State or becoming eligible for Medicaid or Medicare.

There is also good news about Medicare. Spending per Medicare beneficiary is growing slower than the overall economy. The Medicare trustees recently projected that the trust fund that finances Medicare's hospital insurance coverage will remain solvent until 2030, 4 years beyond what was projected just 1 year ago.

We strive to make health care safer and better. In the last 5 years, we have seen a 9-percent reduction in harm in hospitals, such as decreased healthcare-associated infections. This represents over 500,000 injuries, infections, and adverse events avoided; over 15,000 lives saved; and approximately $4 billion in avoided costs. This adds up to better health care at a better price, and I know that makes a real difference for real people.

Consumers also trust us with their personal information, and I take that trust very seriously. Security and privacy are one of our highest priorities. CMS has decades of experience in operating the Medicare program and its supporting systems, and we successfully protect the personal information of both beneficiaries and providers. However, we must continue to be vigilant and evolve our assessments and actions to keep up with ever-changing threats.

Consumers can use the marketplace with confidence that their information is safe and take comfort in knowing that no personally identifiable information has been maliciously accessed from the site. Our systems are designed with security in mind, and our focus

on security is ongoing. It did not end when the marketplace launched. CMS conducts continuous monitoring using a 24/7, multilayer, professional security team and penetration testing. Our systems comply with FISMA and standards promulgated by NIST and the Office of Management and Budget.

There is risk inherent in any system. It is simply, sadly, a part of the cyber world in which we all live. We appreciate the work done by the GAO to suggest additional controls to help us further protect against these risks and are always seeking to improve upon the security protections in place.

As we look forward to our second enrollment period, our goal is to buildupon this progress and to address outstanding challenges. We are working to make it as seamless as possible for people to reenroll in coverage and reinforcing our outreach to help more uninsured consumers enroll in coverage. We are making management improvements with clear accountability and are committed to being transparent.

This coming year will be one of visible and continued improvement but not perfection. As problems arise, we will fix them, just as we always have. Throughout my career as a hospital executive, nurse, and public servant, my focus has been on providing people with high-quality health care. I am proud of the progress we have made at CMS, and I hope to continue to work with Congress on our efforts.

Thank you.

Chairman ISSA. Thank you.

[Prepared Statement of Ms. Tavenner follows:]

STATEMENT OF

MARILYN TAVENNER

ADMINISTRATOR,
CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

AFFORDABLE CARE ACT IMPLEMENTATION

BEFORE THE

U. S. HOUSE COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM

SEPTEMBER 18, 2014

House Committee on Oversight & Government Reform
Affordable Care Act Implementation
September 18, 2014

Good morning, Chairman Issa, Ranking Member Cummings, and members of the Committee. I appreciate the opportunity to update you on CMS' progress and our continuing work to implement the Affordable Care Act and provide consumers with affordable access to high quality coverage. As we prepare for the second year of Health Insurance Marketplace Open Enrollment, CMS is building on our successes and lessons we have learned, while continuing our focus on providing consumers with more affordable coverage options and a secure, consumer friendly online Marketplace. CMS remains committed to ensuring that the Marketplace continues to adhere to the stringent privacy and security protocols necessary to protect consumers' personally identifiable information.

A new wave of evidence shows that the Affordable Care Act is working to make health care coverage more affordable, accessible and of a higher quality, for families, seniors, businesses, and taxpayers alike. Thanks to the Affordable Care Act, consumers today enjoy better access to affordable health coverage, stronger protections in the case of illness or changes in employment, and a competitive Marketplace that allows them to choose from and enroll in insurance coverage that is right for them. Millions of people have obtained private insurance coverage in the Marketplace, over seven million children, families, and individuals have gained coverage through Medicaid and CHIP, and more than three million young adults gained or retained insurance under the Affordable Care Act by staying on their parents' plan. The Marketplace is enrolling people every day and is available when people need it – currently consumers are getting coverage through the Marketplace when they qualify for a special enrollment period, available to those that lose employer coverage, get married or have a baby, or have other qualifying life events.

As we plan for the second Open Enrollment, including the first opportunity for many consumers to re-enroll in coverage, we are focused on building on the advances made for consumers during

the first year. Our focus is on providing consumers more choices for coverage and affordable options, assisting them with selecting the right plan for them, and educating first-time and newly insured consumers about their benefits, their eligibility requirements, and their financial protections.

At the same time we are keenly aware of the challenges we face as a new program of this scale matures, particularly one that faced significant challenges in its first year. It is thanks to the work of a committed team heeding the lessons of the last year that we will continue to build on the success of the first year of State-based and Federally-facilitated Marketplace (FFM).

Continued Focus on Privacy and Security

Each and every day, U.S. businesses and government IT systems and individual consumers face a myriad of cyber threats. No website is immune from attempted attacks, and CMS acknowledges that risks exist inherently for every IT system. CMS appreciates the work of the Government Accountability Office and HHS Office of Inspector General to help us identify controls and processes that could be improved to further reduce or mitigate risk.

CMS remains committed to privacy and security protocols to protect consumers' personally identifiable information; consumers can use the Marketplace with the confidence that their personal information is secure. To date, there is no evidence that a person or group has maliciously accessed personally-identifiable information (PII) from the site. The privacy and security of consumers' PII are top priorities for CMS. As part of that effort, CMS has taken many steps and implemented several security controls to secure PII related to the FFM and its supporting databases.

CMS developed the Marketplace systems consistent with Federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. Components of the website that are operational have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institute of Standards and Technology (NIST).

Marketplace systems are also in compliance with all the relevant privacy and security statutes, including the Privacy Act. Additionally, the Internal Revenue Service accepted the CMS Safeguard Procedures Report as certification that the confidentiality of Federal tax information disclosed to CMS would be adequately protected.

Systems Designed with Security as a Top Priority

Privacy and security has been a high priority throughout the development of HealthCare.gov and related FFM systems. CMS has developed a tool, known as the Federal Data Services Hub (the Hub), that provides an electronic connection between the eligibility systems of the Marketplaces to already existing, secure Federal and state databases to verify the information a consumer provides in their Marketplace application. The Hub was specifically designed to minimize security risk by developing a system that does not retain or store PII. The Hub increases efficiency and security by eliminating the need for each Marketplace, Medicaid agency, and CHIP agency to set up separate data connections to each database.

The Marketplace application on HealthCare.gov never asks for personal health information beyond what is normally asked for in Medicaid eligibility applications. This is due to the provisions in the Affordable Care Act, which prohibit issuers from denying applicants insurance based on pre-existing conditions or charging more based on health status. Consumers in the Marketplace do not need to disclose details of their medical history as they might have had to do to apply for health coverage in the past.

An independent security control assessor tested each piece of the FFM that went live October 1 prior to that date with no open high findings. All high, moderate, and low security risk findings for the portions of the website that launched October 1 were either fixed or had strategies and plans that met industry standards in place to fix the findings. In keeping with industry practice, CMS established strong security controls and standards for each state to meet in order to connect to the Hub. These controls and standards are based on Federal security guidelines. Each state had to sign a Computer Matching Agreement, an Interconnection Security Agreement and an Information Exchange Agreement, all of which bind the state to rules and operating procedures

related to data security and privacy. Additionally, each state was required to complete a security plan, a risk assessment which can either be a self-assessment or a third-party assessment, and a corrective action plan to address risks. Every state that was connected to the Hub adhered to these procedures.

Ongoing Security Focus

CMS has implemented other measures to protect PII, including penetration testing, which happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. As part of the ongoing testing process, and in line with Federal and industry standards, any open risk findings are appropriately addressed with risk mitigation strategies and compensating controls. The security of the system is also monitored by sensors and other tools to deter and prevent unauthorized access. CMS conducts continuous monitoring using a 24/7, multi-layer IT professional security team, added penetration testing, and ongoing testing and mitigation strategies implemented in real time. These layered controls help protect the privacy and security of PII related to the FFM.

CMS continues to test security functionality through quarterly Security Control Assessments (SCAs) which is beyond the industry standard. In addition to daily operational security testing, a comprehensive end-to-end Security Control Assessment that meets industry standards will be conducted by independent assessors next month. This Security Control Assessment will test security for open enrollment and plan year functionality.

Affordable Care Act Implementation: Building on Progress in Affordability, Access and Quality

Recent years have seen historically low growth in overall health spending, and a variety of recent data show that slow growth in health care costs is continuing.[1,2] Preventive benefits, including

[1] Council of Economic Advisers. 2014. "Recent Trends in Health Care Costs, Their Impact on the Economy, and the Role of the Affordable Care Act." *Economic Report of the President,* http://www.whitehouse.gov/sites/default/files/docs/erp_2014_chapter_4.pdf.

[2] Jason Furman. "Good News on Employer Premiums Is More Evidence of a Dramatic Change Economic Change for the Better," http://www.huffingtonpost.com/jason-furman/good-news-on-employer-pre_b_5798244.html.

wellness visits and screenings with no cost sharing for Medicare beneficiaries, as well as new incentives to pay doctors and hospitals for improving outcomes, are aimed at improving the quality of the health care that Americans receive.

Thanks to the Affordable Care Act, we are also taking important steps to improve the quality of care for Medicare beneficiaries, while improving Medicare's long-term solvency. More than 8.2 million seniors have saved more than $11.5 billion on prescription drugs since 2010. Medicare Part B premiums are projected by the Medicare Trustees to be the same in 2015 as they were in 2013 and 2014. Additionally, the Medicare Trustees recently projected that the trust fund that finances Medicare's hospital insurance coverage will remain solvent until 2030, four years beyond what was projected in last year's report.[3] Due in part to reforms in the Affordable Care Act, per beneficiary spending is projected to continue to grow slower than the overall economy for the next several years. We have made major progress in improving patient safety, decreasing hospital readmissions, and establishing new payment models such as accountable care organizations aimed at reducing costs and improving quality. These reforms are designed to slow the rise in health care spending while improving the quality of care for beneficiaries. In addition, the Congressional Budget Office (CBO) recently released updated projections[4] providing further evidence that Medicare is stronger today than it was prior to the Affordable Care Act – including that the rate of growth in spending is expected to be slower than the rate of growth in the number of beneficiaries in 2014.

The Affordable Care Act benefits Americans broadly, not simply those who are newly insured. Over the past three years, Americans have benefitted from insurance reforms that have already gone into effect, such as allowing adult children up to age 26 to stay on their parents' insurance, eliminating lifetime dollar limits on essential health benefits, and prohibiting rescissions of insurance because someone gets sick.

[3] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/ReportsTrustFunds/downloads/tr2014.pdf
[4] http://cbo.gov/sites/default/files/cbofiles/attachments/45653-OutlookUpdate_2014_Aug.pdf

Now, in 2014, pre-existing conditions no longer preclude individuals from gaining health insurance, and consumers have better access to comprehensive, affordable coverage. Consumers now have the comfort of knowing that if their employment changes or they lose coverage for any reason, they can purchase affordable coverage through the Marketplace—regardless of their personal health history. New protections also ensure that consumers' premium dollars are spent primarily on medical care, rather than on administrative expenses. Since the Medical Loss Ratio program's inception in 2011, consumers have saved an estimated $9 billion. This year, 6.8 million consumers across all states and markets will receive over $330 million in refunds, with an average rebate of $80 per family.[5]

The market reforms are effective because they have benefits across the health care system. Reductions in the uninsured rate generally mean that doctors and hospitals provide less uncompensated care, the costs of which are often passed along to taxpayers as well as consumers and employers who pay premiums for health coverage. And new pools of people buying insurance means insurers have an opportunity to grow by competing to provide better access to quality, affordable choices, the benefits that consumers are used to in any competitive marketplace. The creation of a successful, viable health insurance market has benefits for all Americans no matter where they get their health insurance.

Reductions in the Uninsured Rate

Several recent reports make clear that the Affordable Care Act is reducing the uninsured rate. A study published in the *New England Journal of Medicine* found that, as compared with the baseline trend, the non-elderly uninsured rate declined by 5.2 percentage points by the second quarter of 2014, a 26 percent relative decline from the 2012–2013 period, corresponding to 10.3 million adults gaining coverage.[6] Other independent surveys all point to the same overarching trend—the success of the Affordable Care Act in lowering the number of uninsured Americans.

---

[5] http://www.cms.gov/CCIIO/Resources/Forms-Reports-and-Other-Resources/Downloads/Final-MLR-Report_07-22-2014.pdf

[6] New England Journal of Medicine, Health Reform and Changes in Health Insurance Coverage in 2014.

Consumers are finding affordable coverage options, a greater choice of plans, and coverage that meets their care needs. The vast majority of consumers who gained private insurance coverage through the Marketplace are paying $100 or less per month. In fact, nearly half of individuals selecting plans with tax credits in the FFM – specifically, 46 percent – were able to get covered for $50 per month or less. For many it was the first time they had a real choice in health plans - during Open Enrollment for the 2014 plan year, consumers could choose from an average of over 40 Marketplace plans.[7] The Commonwealth Fund survey found that nearly two in three of newly-covered consumers who went to the doctor or filled a prescription said they would not have been able to afford or access those services were it not for their new coverage, and more than three in four newly-insured consumers expressed satisfaction with their coverage.

Affordable Care Act Implementation: Building on Progress and Lessons Learned From Year One

As we embark on the second Open Enrollment period, CMS is concentrating now on several critical priorities to build on the progress from the first year of operations. We are focused on increasing the value to consumers by continuing to improve the information, plan options, and affordability of the shopping experience. We are working to ensure that consumers satisfied with their current Marketplace coverage can reenroll, while continuing our efforts to reach those who are eligible, but not yet enrolled in coverage. We are also addressing the execution and technology lessons we learned during the first open enrollment period with a disciplined, highly accountable and visible management structure.

Bringing More Value to Consumers in the Marketplace

Like any marketplace, the Marketplace leverages technology to bring more value, better information and a better shopping experience to consumers. Driven by competition and the significant demand for health coverage, our goal is to expand health plan options with more affordable premiums for consumers.

[7] ASPE Research Brief: Premium Affordability, Competition, and Choice in the Health Insurance Marketplace, 2014, http://aspe.hhs.gov/health/reports/2014/Premiums/2014MktPlacePremBrf.pdf

The Affordable Care Act has increased competition in the market and offered more plan options to consumers. In the coming year we expect insurers to bring more options in more geographic markets, including in markets where consumers have historically had limited options for coverage. While we are still reviewing the proposed plans to ensure they meet the requirements for participation in the Marketplace, we have seen an increase in the number of insurers seeking to participate in the Marketplace in the 2015 plan year. With more choices in year two, consumers should have an even greater opportunity to find a quality health plan that best meets their needs.

As we work to bring greater choice to consumers, CMS is also bringing more value to consumers in the coming year is by improving the transparency for provider networks. CMS will hold insurers to a "reasonable access" standard for network adequacy and will identify provider networks that fail to provide access without unreasonable delay, especially in areas that have historically raised network adequacy concerns, such as hospital systems, mental health providers, oncology providers, and primary care. Many health insurers are strengthening their networks, increasing inclusion of Essential Community Providers, and improving access to prescription drugs. We are also working to prevent cost sharing discrimination so that consumers have access to the appropriate services.

CMS is also continuing to monitor consumers' access to provider directories to help consumers more easily find network providers. Insurers are now expected to provide links that connect consumers directly to provider directories specific to a given plan option without needing to log in, enter a policy number, or navigate through various websites. CMS expects that insurers will maintain these directories and that they will be kept up to date and will include location, contact information, specialty, medical group, institutional affiliations, and whether the provider is accepting new patients—information consumers need to make informed health plan decisions.

While many are already utilizing their new coverage, we know that many consumers have received coverage for the first time in years – some for the first time ever, so they may need a little extra help in understanding their rights and their new coverage. Our From Coverage to Care

initiative helps people with new health care coverage understand their benefits and connect to primary care and the preventive services that are right for them, so they can live a long and healthy life. The goal of the initiative is to help the newly insured navigate the healthcare system, improve their health and insurance literacy, promote patient engagement, and know what services are available in their local community.

For those who are currently enrolled in Marketplace coverage, CMS is working to make the process of renewing coverage as simple as possible. We will encourage everyone to come back to the Marketplace to update their eligibility information and shop for the best coverage option that meets their needs. And for those consumers who are satisfied with their current plan and don't want to change, we will follow the model used by most employers and in the Medicare Advantage and Part D programs, and allow people to automatically re-enroll.

While we know millions have signed up for new coverage, we know more work remains to reach out to those who are not yet covered, to educate them about the benefits of health insurance and assist them in signing up for plans that fit their needs. We recognize these challenges cannot be managed from Washington alone. One of the lessons we learned over the past year was that one of the most effective ways to get people enrolled is through in-person help in their own communities. In a survey of Marketplace assister programs, including Navigators, in-person assisters, certified application counselors, and others, Kaiser Family Foundation found that assistor programs helped an estimated 10.6 million people during the first open enrollment period.[8] We've put a priority on recruiting more organizations to sign up to be Certified Application Counselors and recruiting more local leaders to be in-person assistors. We will also continue working with agents and brokers as they utilize their experience and existing relationships with consumers and small businesses to assist them in enrolling in coverage.

Adding Critical Functionality to Operate the Marketplace

Significant technological improvements are underway to support the operation of the Marketplace in a more automated fashion and to allow consumers to renew their coverage as

[8] http://kff.org/health-reform/report/survey-of-health-insurance-marketplace-assister-programs/

seamlessly as possible this year. Building this functionality means ruthlessly prioritizing efforts to execute on critical capabilities, while setting the course for further improvement and development of new functionality in coming years.

Critical focal areas include completing functionality that was targeted for the first year of development, but has not yet been completed, such as launching an online exchange for small businesses and their employees. In addition, we are building the functionality required for renewing members and adding to the infrastructure to better support open enrollment. As we make these improvements, we are focused on managing our resources efficiently and are conscious of the limited time available for technology development this year.

We have created clear accountability for the leadership of this project. Earlier this year, Secretary Burwell announced a series of organizational changes designed to strengthen the implementation of the Affordable Care Act, including the recent addition of Kevin Counihan as Marketplace Chief Executive Officer, with responsibility and accountability for leading the FFM, and managing relationships with the state Marketplaces. Most recently, he served as Connecticut's Health Insurance Exchange CEO. Our new leadership structure will improve the discipline and focus of the project, enhance communications, and identify risks throughout the project. Like any project of this size, there will always be ongoing challenges, but we are building an operation better suited to identify and resolve them.

Conclusion

The Affordable Care Act is delivering on the promise of access to high quality, affordable health care coverage, while controlling the growth of health care costs. While the Marketplace is still at an early stage, we are hard at work building on the successes and lessons learned from the first open enrollment, and look forward to meeting the needs of consumers and insurers as we continue to learn and improve for future years. The transition to a reformed health insurance market will take sustained effort, persistence, and focus from all stakeholders, but CMS is committed to continuing to deliver on the promise of the Affordable Care Act and improving

health care access, cost, and quality for all Americans. I thank you for the opportunity to update you on our efforts, and look forward to answering any questions you may have.

Chairman ISSA. Ms. Barron-DiCamillo? Is that closer? OK. I will try to do better. Thank you.

STATEMENT OF ANN BARRON-DICAMILLO

Ms. BARRON-DICAMILLO. Chairman Issa, Ranking Member Cummings, and members of the committee, thank you for the opportunity to appear before you today.

We are also making every opportunity and every effort to be transparent at DHS—to be as transparent as possible.

My name is Ann Barron-DiCamillo. I am the Director of US-CERT within the National Cybersecurity and Communications Integration Center, also known as NCCIC. We lead the Department of Homeland Security's efforts in cyberspace to respond to major incidents, analyze threats, and share critical cybersecurity information with trusted partners around the world.

US-CERT is a 24/7 operations center and receives and analyzes hundreds of incident reports a day. We work with public-and private-sector partner organizations and are committed to the protection of privacy and civil liberties for all Americans. At US-CERT, we strive for a safer, stronger Internet for all Americans.

Established in 2003, US-CERT initially focused on securing U.S. Federal systems and networks. DHS's cybersecurity capabilities have grown immensely since the establishment of US-CERT, and we are working more closely than ever with partners across public and private sectors to develop a comprehensive picture of malicious activity and mitigation options.

Cybersecurity is a shared responsibility and a continuous process. Our focus is helping our partners build a resilient and secure ecosystem in cyberspace. Protecting our networks requires coordination across a global cyber community to enhance others' capabilities as we continue to mature our own. While DHS leads the national effort to secure Federal civilian networks, agency heads are responsible for assessing the risk to their systems and taking appropriate measures to secure their networks. US-CERT supports agency heads and chief information officers in carrying out these responsibilities.

I am here today in a technical capacity to provide findings from our analysis of the compromised test server at HealthCare.gov.

US-CERT was notified of an incident by CMS, who has the oversight responsibility of HealthCare.gov. We conducted analysis of the images provided to us by CMS and found evidence of malware on a test server. As Stated by Ranking Member Cummings, our analysis concluded that there was no indication of personally identifiable information—also known as "PII"—exposure and no indication of data exfiltration. Additionally, there is no evidence of any lateral movement within the network or further infection.

We have provided CMS a report with these findings as well as mitigation recommendations. Additionally, we were able to share indicators from our analysis so that agencies, partners, and stakeholders could better protect their own networks. We are currently in discussions with HHS to provide further onsite support.

DHS remains committed to working with its Federal and private-sector partners no create a safe, secure, and resilient cyberspace.

And I look forward to answering any questions that you might have.

Chairman ISSA. Thank you.

[Prepared Statement of Ms. Barron-DiCamillo follows:]

Testimony

Ann Barron-DiCamillo

Director, U.S. Computer Emergency Readiness Team

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Regarding

Examining ObamaCare's Failures in Security, Accountability, and Transparency

September 18, 2014

Introduction

Chairman Issa, Ranking Member Cummings, and members of the Committee, I appreciate the opportunity to discuss the Department of Homeland Security's (DHS's) efforts to improve the cybersecurity posture and capabilities of civilian Federal agencies, including the Department of Health and Human Services (HHS).

Roles and Responsibilities

DHS is the lead for securing and defending Federal civilian unclassified information systems against cyber threats and enhancing cybersecurity among critical infrastructure partners. To this end, DHS ensures maximum coordination and partnership with Federal and private sector stakeholders while working to safeguard the public's privacy, confidentiality, civil rights and civil liberties. Within DHS's National Protection and Programs Directorate (NPPD), the Office of Cybersecurity and Communications (CS&C) focuses on managing risk to the communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery to incidents affecting critical infrastructure and government systems.

CS&C executes its mission by supporting 24x7 information sharing, analysis, and incident response as well as facilitating interoperable emergency communications and advancing technology solutions for private and public sector partners. We also provide tools and capabilities to strengthen the security of Federal civilian executive branch networks, and engage in strategic level coordination with private sector organizations on cybersecurity and communications issues.

DHS leads the national effort to secure Federal civilian networks. Federal agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems within their agency, or operated on behalf of their agency by a contracted entity, in accordance with the Federal Information Security Management Act (FISMA). Agency heads are provided the flexibility and authority to delegate those responsibilities to the agency's Chief Information Officer (CIO) in order to ensure compliance with the requirements outlined within FISMA and the associated memoranda and directives. These authorities include programs to assess, inform and report on the agencies' status and capabilities relative to FISMA guidance.

Although each Federal department and agency retains primary responsibility for securing and defending its own networks and critical information infrastructure, DHS leads efforts to plan and implement strategic management of information security practices across the Federal departments and agencies. The Department provides assistance to departments and agencies by collecting and reporting information regarding cybersecurity posture and risks; disseminating cyber alert and warning information to promote protection against cyber threats and the resolution of vulnerabilities; coordinating with partners and customers to attain shared cyber situational awareness; and providing response and recovery support to agencies upon their request. Pursuant to current authorities, DHS must be asked by the Federal departments and agencies to provide the aforementioned direct support. The Department focuses its support of Federal networks through the following activities:

- **FISMA**: The Office of Management and Budget (OMB) has delegated operational responsibilities for Federal civilian cybersecurity to DHS, establishing the Department as

the lead in promoting and coordinating the cybersecurity posture of Federal civilian executive branch networks. FISMA requires program officials and agency heads to mitigate cybersecurity risks based upon each agency's particular requirements. DHS receives FISMA reporting and monitors agency status to ensure the effective implementation of this guidance.

- **Continuous Diagnostics and Mitigation (CDM)**: The CDM program focuses on FISMA security metrics that have a direct impact on Federal civilian departments' and agencies' cybersecurity. By empowering Federal civilian agency CIOs and Chief Information Security Officers (CISOs) with situational awareness regarding their risk posture and with ongoing insight into the effectiveness of security controls, CDM will provide these partners with resources necessary to identify and fix the worst cybersecurity problems first.
- **National Cybersecurity Protection System**: Also referred to as EINSTEIN, this program delivers a range of capabilities including intrusion detection, analytics, intrusion prevention, and information sharing. These capabilities provide a technological foundation that enables DHS to help secure and defend the Federal civilian executive branch networks against advanced cyber threats by providing improved situational awareness, identification, and prevention of malicious cyber activity.

DHS Services

DHS offers additional capabilities and services to assist Federal agencies and stakeholders based upon their cybersecurity status and requirements. The Department engages agency CIOs and CISOs through a variety of mechanisms including information sharing forums

as well as through the National Cybersecurity and Communications Integration Center (NCCIC)[1] in direct response to a specific problem/issue or identified threat. These include:

- **Incident response:** During or following a cybersecurity incident, DHS may provide response capabilities that can aid in mitigation and recovery. Through the NCCIC, DHS further disseminates information on potential or active cybersecurity threats to public and private sector partners. When requested by an affected stakeholder, DHS provides incident response through the United States Computer Emergency Readiness Team (US-CERT) or the Industrial Control Systems-Cyber Emergency Response Team.
- **Assessing security posture and recommending improvements:** Upon agency request, DHS conducts Risk and Vulnerability Assessments to identify potential risks to specific operational networks systems and applications and recommends mitigation.
- **Providing technical assistance:** DHS may provide direct technical assistance to agencies. For example, by assessing agency compliance with and progress toward aggregating network traffic into Trusted Internet Connections, DHS assists in reducing access points and protecting the perimeter of agency networks.

Recent Report of Malware

DHS has been and continues to interact with HHS — to include healthcare.gov — in the same manner as with all other Federal entities regarding cybersecurity: by making available its portfolio of capabilities and services. In doing so, we inform, educate and increase the cybersecurity capacity of all civilian Federal departments and agencies.

[1] The NCCIC, a 24x7 cyber situational awareness, incident response, and management center, is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

At HHS's request, the NCCIC's US-CERT worked with HHS to analyze and mitigate the effects of a Distributed Denial of Service (DDoS) malware package that was found on a single test server. This type of malware is not designed to extract information and there is no indication that any data was compromised as a result of this intrusion. DHS continues to monitor the situation and will help develop and implement precautionary mitigation strategies in coordination with HHS as necessary.

Conclusion

Evolving and sophisticated cyber threats present a challenge to the cybersecurity of the Nation's critical infrastructure and its civilian government systems. DHS is committed to reducing risks to Federal agencies and critical infrastructure. We will continue to leverage our partnerships inside and outside of government to enhance the security and resilience of our Federal networks while incorporating privacy and civil liberties safeguards into all aspects of what we do. Thank you again for the opportunity to provide this information, and I look forward to your questions.

Chairman ISSA. I will start with you then.

When did you find out you were going to appear here today?

Ms. BARRON-DiCAMILLO. I believe I was informed on Monday.

Chairman ISSA. And when did you begin preparing for today's hearing?

Ms. BARRON-DiCAMILLO. When I was informed on Monday.

Chairman ISSA. OK.

Has CERT done a security testing of HealthCare.gov?

Ms. BARRON-DiCAMILLO. We were provided images from CMS of the compromised test servers, and we provided analysis——

Chairman ISSA. I appreciate that. The question was, has CERT conducted any security testing of HealthCare.gov's vulnerabilities?

Ms. BARRON-DiCAMILLO. No. As I Stated in my opening remarks, we——

Chairman ISSA. So when Ms. Tavenner says there have been no loss of personally identifiable information, if you don't know the vulnerabilities, how would she know that to be true?

Ms. BARRON-DiCAMILLO. I believe that CMS conducts their own scanning and testing, but I am happy to——

Chairman ISSA. Did you verify their scanning and testing to be sufficient?

Ms. BARRON-DiCAMILLO. We would be happy to provide that information——

Chairman ISSA. Did you?

Ms. BARRON-DiCAMILLO. I haven't been provided any details on the scanning——

Chairman ISSA. So you don't know that?

Ms. BARRON-DiCAMILLO. Within the test network?

Chairman ISSA. Yes. It boils down to, you are here as an expert that I didn't expect from an organization that refused to give my staff any briefing related to it——

Ms. BARRON-DiCAMILLO. And I do apologize for that. I was under the impression that our staff was working with your staff to answer those questions. I'm happy to answer——

Chairman ISSA. No. As of yesterday afternoon, they put people who didn't have technical expertise on, who told us they would get back to us. That is after more than a week of information we have already put in the record where we were denied that.

Maybe I will go on to GAO.

I am going to ask, first of all, your indulgence. When this hearing is over, I would like you to accept the—pardon me?

Mr. CUMMINGS. No, I——

Chairman ISSA. Oh, OK.

Mr. CUMMINGS. I wanted to hear what you had to say.

Chairman ISSA. That can happen.

I would like you to accept a briefing and do a supplemental related to the 13 breaches.

Mr. WILSHUSEN. OK.

Chairman ISSA. Ms. Tavenner, I am going to presume that you will agree that he will have full access to all information related to that so that GAO may develop specific additional recommendations based on the actual breaches, if you will, the 13 incidents.

Ms. TAVENNER. Yes, sir.

Chairman ISSA. OK. That will allow us to get what we don't have here today, and I appreciate that.

But, Mr. Wilshusen, you have gone through an extensive amount. Would you describe for the committee the level of cooperation you believe you got? We have heard what you didn't get. Are there some good-news stories in the cooperation as you did your investigation, or your audit?

Mr. WILSHUSEN. Well, there is some good news and then some not-so-good news, Mr. Chairman.

As we began our audit—and, generally, we do receive good cooperation from the agencies that we audit as it relates to receiving information requests that we provide. In this case, initially, there were delays in providing certain documents that we had requested. In addition, CMS attempted to put certain restrictions on some of the documents. And——

Chairman ISSA. Did they cite why they were restricting? Are you just not trustworthy?

Mr. WILSHUSEN. No, no. I think they indicated that they were concerned about the security—the sensitive security information in——

Chairman ISSA. So they don't trust you.

Mr. WILSHUSEN. I wouldn't say that, sir, no.

But we elevated the issue within GAO and within the Department, and we reached and agreement to where we would be able to and they did provide the information for us to look at.

Chairman ISSA. So, at the end of it all, there was no reason—after it was elevated, there was no reason that they should have denied it to begin with.

Mr. WILSHUSEN. In my view, no. They should have provided it earlier. But, at the same point, you know, they had a concern about the security of the information, so they tell us. But, you know, their motivation would be probably better addressed by the Administrator.

Chairman ISSA. OK. Limited time, and I want to sort of set the stage for what others on both sides of the aisle may ask here.

When you looked at the robustness of how they determined with such certainty that there had been no breaches, no loss of personally identifiable information, were you satisfied that all those procedures were robust enough that, with the certainty that Ms. Tavenner said that no losses had occurred, that no losses had occurred?

Mr. WILSHUSEN. Well, we did not receive actual security incident reports on these incidents, at least on the 13. We did receive a written response to an interrogatory, in which they indicated that, at least for the 13, that there was certain PII that was compromised or disclosed to an individual, but it was a consumer. It was due to a technical glitch in——

Chairman ISSA. Wait, wait, wait. I want to understand.

Mr. WILSHUSEN. Right.

Chairman ISSA. So personally identifiable information was lost or disclosed?

Mr. WILSHUSEN. Was disclosed, according to their description. But——

Chairman ISSA. OK.

Ms. Tavenner, others will ask additional questions, but your opening Statement said none had been lost. How can we reconcile "none has been lost" with a sworn Statement that some has been lost?

Ms. TAVENNER. I think what my Statement said is there were no malicious attacks on——

Chairman ISSA. Oh. Oh, so if you just screw up and put the public's information out, it is OK because it wasn't a malicious attack?

Ms. TAVENNER. No, sir, I don't think any time we put consumer information out there it is OK. But I think——

Chairman ISSA. OK. So my time has expired, and I want the ranking member to have full time.

I just want to make it clear that wordsmithing of "no malicious was done" versus "accidental"—just as we discovered at the time of the launch that, if I went to the section above, you know, where the URL normally is, when that thing was launched, if I simply typed in a different number or a different State code, I could have looked at somebody else's record. That was part of what you guys had wrong on the day of the launch, is that you could simply go to somebody else's record by changing that long streak at the top, meaning no code. That wouldn't have been malicious, I guess, except that if somebody were doing it to see what they would get, that would be a little bit malicious.

So when you say no personally identifiable information was lost through malicious, what you are saying is you don't know how much was lost, you just believe that the definition of "malicious" wasn't met. Is that right?

Ms. TAVENNER. I actually—and I think this relates to the personal incidents. And I do think that we want to cooperate with the GAO on that, and we are happy to review those. And I think——

Chairman ISSA. Thank you. Your desire to want to cooperate after we bring you here involuntarily for a hearing is most appreciated, but, quite frankly, you should have cooperated with the GAO beforehand.

Ms. TAVENNER. Sir, I think the—I always like to cooperate with the GAO and the OIG. And we have had over 140 open audits underway, and I think we have cooperated. I would also like to say I came here voluntarily.

Chairman ISSA. Thank you.

The distinguished gentleman from Missouri is now recognized for 5 minutes.

Mr. CLAY. And thank you, Mr. Chairman. Thank you for—and thank the ranking member for yielding his time.

Mr. Wilshusen, GAO found that HealthCare.gov had security weaknesses when it was first launched in part because of a lack of adequate oversight of security contractors. Is that right?

Mr. WILSHUSEN. We found that, with respect to when it was first deployed—and recognize that our audit occurred subsequent to the initial deployment—we found that, based on a review of the documents, there were certain vulnerabilities in controls that had not been tested at that time and that there were a few vulnerabilities that had been identified through testing through which the CMS had accepted in order to provide an authority to operate——

Mr. CLAY. Those responsibilities were incumbent upon the contractor, correct?

Mr. WILSHUSEN. Well, overall responsibility, it rests with the——

Mr. CLAY. With the contractor? Or——

Mr. WILSHUSEN. I believe—I think, in some cases, there may be incidents and we did identify weaknesses that were operated on systems operated by a contractor. But that was subsequent——

Mr. CLAY. OK.

Mr. WILSHUSEN. That was during the course of our audit, not—that doesn't necessarily pertain to prior to the deployment of the system.

Mr. CLAY. Sure. And the GAO report found that there was not a shared understanding of how security was implemented among all entities involved in the development and security testing of the Website. Is that correct?

Mr. WILSHUSEN. Yes, that's correct. And what we found, too, is that in certain instances where CMS told us who was responsible, or the contractor that was responsible for certain tests, such as implementing security on a firewall——

Mr. CLAY. Yes.

Mr. WILSHUSEN [continuing]. It went to that contractor. The contractor indicated that it was not his responsibility, that it was another contractor, and that responsibility was not identified in that contract's Statement of work.

Mr. CLAY. Yes, but scenarios like this obviously increase the likelihood of security risks. Is that correct?

Mr. WILSHUSEN. Yes, sir.

Mr. CLAY. And was there a specific CMS official or group that was responsible for overseeing the security testing of HealthCare.gov? Is there a group?

Mr. WILSHUSEN. Well, overall, the CMS CIO and CISO—I'm sorry—Chief Information Officer and Chief Information Security Officer have, I would say, overall responsibility for reviewing and assuring the security over the system.

Mr. CLAY. Now, for a project of this magnitude, shouldn't an agency official with a broad understanding of IT security testing oversee contractors?

Mr. WILSHUSEN. I would say yes.

Mr. CLAY. And was that the case here?

Mr. WILSHUSEN. I would say that, you know, there is—that CIO/CISO would be the individuals that would have that responsibility overall.

Mr. CLAY. OK. So who would the CMS official be that would have that kind of understanding of IT security testing? Was there a person in place?

Mr. WILSHUSEN. Yes. Either they had the CMS CISO. In addition, there are several individuals that were responsible for aspects related to the security over the HealthCare.gov. There is also an information systems security officer that has responsibility for assuring that, you know, security controls are properly implemented.

Mr. CLAY. And, you know, the issues with IT security management did not start with HealthCare.gov. As a matter of fact, this is a broader government problem that needs to be addressed, don't you think?

Mr. WILSHUSEN. GAO has been reporting information security and Federal information security as a governmentwide high-risk area since 1997. And so, sadly, yes, it is a broad government issue.

There have been weaknesses—just as an example, for Fiscal Year 2013, 18 out of the 24 major Federal agencies covered by the Chief Financial Officers Act reported either a material weakness or a significant deficiency in their information security controls for financial reporting purposes. Twenty-one out of the 24—or IGs at 21 out of the 24 agencies also cited information security as a major management challenge. So yes.

Mr. CLAY. And so it would be fair to say that all Internet-facing systems, both in the Federal Government and the private sector, involve some risk. Is that correct?

Mr. WILSHUSEN. Given the nature of the Internet and the capabilities and prevalence of hackers who might try to exploit vulnerabilities, yes. The answer is there is risk in conducting online transactions.

Mr. CLAY. Thank you so much for your responses.

And, Mr. Chairman, I yield back.

Chairman ISSA. I thank the gentleman.

We now go to the gentleman from Florida for 5 minutes.

Mr. MICA. Thank you, Mr. Chairman.

And I have a copy of your report dated September 2014. And, in that, you, in fact, State and GAO found—first of all, I think you found that the testing was not complete and that the whole program was rolled out with weaknesses in security and protection of privacy. Would that be an accurate Statement?

Mr. WILSHUSEN. Yes.

Mr. MICA. OK.

I also see that you say that the GAO report strongly asserts that testing of the Website still remains insecure. Is that correct?

Mr. WILSHUSEN. I would say that the testing of HealthCare.gov and the supporting systems has not been comprehensive——

Mr. MICA. So even to date we have risks. Is that correct?

Mr. WILSHUSEN. Today we have risks.

Mr. MICA. Security risks, privacy information risks. OK. Thank you.

And there was a—the rollout—they actually rolled this out, I saw in the report too—I guess four States had not even taken action to secure privacy?

Mr. WILSHUSEN. I would characterize it more as they had not met CMS's——

Mr. MICA. Right.

Mr. WILSHUSEN [continuing]. Security requirements.

Mr. MICA. Security requirements. And we will have those for the record, the States.

Mr. MICA. So it is incomplete testing.

Then I see, basically, a coverup of the failure that took place. Did you see any of that?

They were trying—I went through some of these emails and some of the record the committee has. I don't know if you saw this. But it looks like quite a coverup, or they tried to not let the public know the failure of the rollout and the failure of them to protect this information. Is that correct?

Mr. WILSHUSEN. I'm sorry, I could not comment on that because I have not seen the——

Mr. MICA. Oh, I can tell you. It is page after page. I mean, I can't even use some of the language used here.

Mr. Chairman, I would like to have some of this submitted in the record, this report.

Chairman ISSA. Without objection, so ordered. The entire report will be placed in the report.

Mr. MICA. OK.

It is astounding. Again, "This is a [blanking] Disaster." I mean, this is one of the HHS people who saw what was going on at CMS.

Politico has a 2-day story that talks about the issues and most detailed explanation, but it is just stating overwhelming traffic that couldn't have been replicated and tested.

I mean, just one point after another of the coverup. And I think, unfortunately, people like Ms. Tavenner were involved in some of the coverup.

Did you ever attempt, ma'am, to have any emails or records deleted as to what was going on in the failure?

Ms. TAVENNER. I'm not aware of the emails. I've not seen the emails you are responding to, so I can't answer that.

Mr. MICA. Uh-huh. Uh-huh. Well, I have one email here, and you had asked that it, in fact, be deleted. And I can supply you with a copy of it. But it says, "Please delete this email." And it goes on to detail what was going on, the failure that was going on.

First of all, there was a company by the name of Serco that was employed to—or retained, a contract of $1.2 billion, is that correct, to process the paper applications?

Ms. TAVENNER. We retained Serco. I don't have the amount in front of me.

Mr. MICA. Uh-huh. Well, again——

Ms. TAVENNER. I'm happy——

Mr. MICA [continuing]. This email talks about Serco and the failure of the proper processing. There were problems with processing the paper applications.

Ms. TAVENNER. Congressman Mica, I'm happy to take a look at the email.

Mr. MICA. Yes. And you had nothing to do with the awarding of a $1.2-billion contract, you would tell the committee too, right?

Ms. TAVENNER. I don't understand the question that you're asking me.

Mr. MICA. Of the Serco contract to process paper.

Ms. TAVENNER. I'm actually not part of the——

Mr. MICA. Here you're talking about Serco and the problems of the paperwork. You're asking for deleting of information.

Then I looked a little bit into Serco, and the Serco scandal grows. Did you know that Serco had been awarded the contract, a $1.2-billion contract, while they were being investigated? It's a British, U.K. Firm, and they were being investigated for some fraudulent activities in the U.K. As they were being awarded a $1.2-billion contract.

Ms. TAVENNER. No, sir, I did not——

Mr. MICA. You weren't aware of any——

Ms. TAVENNER. And I think I Stated that last year in a hearing.

Mr. MICA [continuing]. Of the background.

Again, I think we need to put this—Mr. Chairman, I would like to put this email in the record, where the witness asks that we delete this particular email and it dealt with the problems at Serco at that point.

Chairman ISSA. Without objection, so ordered.

Mr. MICA. Finally, are you aware that you violate Federal law when you ask to delete information like this?

Ms. TAVENNER. Again, Congressman, I would need to see the email in order——

Mr. MICA. OK.

We'll provide the witness, if we could, with——

Chairman ISSA. We will pause quickly.

If you will send it down to her. I think you might as well get it quickly done.

I would ask unanimous consent to stop the clock and give her an opportunity to read it.

Thank you.

Mr. MICA. Just simply, is that your email, and did you ask to have it deleted? At the beginning, it States pretty clearly your intention.

Mr. Chairman, I'll defer to you to get a response from the witness.

Ms. TAVENNER. This email is from me, yes, sir. That's accurate. And this email was written to Julie Bataille, who at the time was involved in the call center. And I think this is about the call center information. And I think that I asked that she delete this email because it involved sensitive information regarding the President's schedule, and I think that's actually the area that's redacted.

But, no, it is not normally my custom to ask—sometimes I would ask that things be "close hold" or "do not forward." But, in this case, it involved the President's schedule, if I remember this correctly.

Mr. MICA. So, again, Mr. Chairman, I would also—I want the entire content of the email entered into the record and the reference further down to Serco.

Thank you. Yield back.

Chairman ISSA. Thank you.

I would just briefly, if I could have an indulgence—why would the President's schedule after the fact have any relevance to being needed to be deleted? I hear you, but the President's schedule becomes very public in realtime within a very short period of time.

Ms. TAVENNER. So I can't answer the reason why this is redacted. I didn't make the decision to redact it. That's done by our oversight——

Chairman ISSA. But you were surmising that it had to do with the President's schedule. The President's schedule is not all that secretive, and, after the fact, it has no relevance for protection.

Ms. TAVENNER. I understand.

Chairman ISSA. And, under the Federal Records Act, your communication is to be retained, correct?

Ms. TAVENNER. And it was retained. My immediate staff was copied on that, and that's why you have it. It was retained.

Chairman ISSA. OK. So deleting it doesn't change the fact that it had to be retained for the Federal Records Act.

Ms. TAVENNER. It is retained.

And, in fact, if you are asking about our response to NARA, we did that out of an abundance of caution because we weren't sure. Because I didn't necessary retain some emails if they related to scheduling changes and this sort of thing. So, going back to the issue of transparency and trying to be forthcoming about information, we decided to notify NARA.

Chairman ISSA. OK. I would hope that the unredacted versions of all this would be made available to the GAO. And I would ask simply that unredacted versions be seen by the GAO to see if, in fact, it's consistent with what we're hearing here today.

Mr. MICA. Mr. Chairman, a unanimous request——

Chairman ISSA. The gentleman will State his request.

Mr. MICA. I have articles about "Serco Scandal Grows" and people paid to do nothing and processing Serco's checkered past, "White House Hired Sham Foreign Company for Obamacare," and a Forbes article, "The Unhealthy Truth About Obamacare's Contractors."

I'd like these to be——

Chairman ISSA. Without objection, so ordered.

Mr. MICA. Thank you.

Chairman ISSA. And, with that, we'll go to the gentleman from Pennsylvania for 5 minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman.

And thank you to the witnesses for joining us here today.

One of the most critical features of the Affordable Care Act is that it expands Medicaid eligibility to millions of low-income American adults. Prior to the ACA, Medicaid eligibility was restricted primarily to low-income children, their parents, people with disabilities, and seniors. In most States, adults without dependent children were not eligible for Medicaid.

According to a study issued in April 2014 by the Kaiser Family Foundation, only about 30 percent of poor, non-elderly adults had Medicaid coverage in 2012 and uninsured rates for poor adults were more than double the national average.

Under the ACA, Medicaid eligibility can be expanded to cover all non-elderly adults with incomes below 138 percent of the Federal poverty level.

Administrator Tavenner, is that correct?

Ms. TAVENNER. Yes, sir, I believe that is correct.

Mr. CARTWRIGHT. All right.

So the Federal Government pays States 100 percent of the costs for the first 3 years and then phases that down—phases its match down to about 90 percent in 2020. Despite this enormous level of Federal assistance, more than 20 States have decided not to participate in the expansion, leaving millions of their own citizens without health care.

Administrator Tavenner, can you comment on the coverage gap that is resulting from these decisions not to expand Medicaid in those States?

Ms. TAVENNER. Yes, sir.

I would start first by saying, with Pennsylvania's recent decision, we are now at 27 States, I believe, plus the District of Columbia, whohave decided to expand Medicaid. And, obviously, if you look at a lot of independent studies, there is a noticeable difference in the States that have decided to expand Medicaid in terms of lowering the number of uninsured.

We're going to continue to work with those remaining 20-something. And we meet with them on a regular basis to do what we can to encourage folks to expand.

Mr. CARTWRIGHT. Now, by not participating, aren't the States that aren't leaving billions of Federal dollars on the table that could be used to improve the health of their own citizens?

Ms. TAVENNER. Yes, sir, they are. And it also has economic consequences for those States, as well.

Mr. CARTWRIGHT. Of course.

Now, recently, some Republican Governors, as you have alluded to, who had originally refused to expand Medicaid have now reconsidered their original decisions and have submitted Medicaid expansion plans for CMS's approval. For instance, in my own State of Pennsylvania, as you mentioned, they decided to expand Medicaid, which will now provide health insurance to 600,000 low-income adult individuals in our State.

Administrator Tavenner, how will Medicaid expansion in Pennsylvania impact the health of its citizens?

Ms. TAVENNER. I certainly can get you information from independent studies, but there is a definite correlation between coverage of insurance and long-term health improvement.

Mr. CARTWRIGHT. Good.

Now—and I don't want to leave this question out. Other than political posturing by the Pennsylvania Governor, are you aware of any good reason why 600,000 good Pennsylvanians went without coverage for an extra 9 months from the rest of the States that expanded Medicaid right away?

Ms. TAVENNER. No, sir. We want everyone to expand and expand quickly.

Mr. CARTWRIGHT. Well, Administrator Tavenner, why do you think Republican Governors are so divided on the issue of Medicaid expansion?

Ms. TAVENNER. Sir, I can't answer that. I'm not sure. I'm sure each State has their reasons. We just try to work with them and meet them where they want to be.

Mr. CARTWRIGHT. All right.

Do you expect to work with additional Governors who previously opposed Medicaid expansion but are now considering reversing their decisions?

Ms. TAVENNER. Absolutely.

Mr. CARTWRIGHT. Well, I want to say I thank you for coming here today, and I thank for you testimony.

I hope that Governors in States that have so far not elected to expand Medicaid will reconsider, will consider the impact on their communities, to take advantage of this historic opportunity to lift up all of the Americans in their States, as well.

Thanks again, Administrator Tavenner.

And I yield back.

Chairman ISSA. Would the gentleman yield?

Mr. CARTWRIGHT. I am out of time.

Chairman ISSA. Oh, OK. Well, at some future time, I'm happy to work with you and explain Republican Governors to your satisfaction.

With that, we go to gentleman from Utah, perhaps a man that will someday be a Republican Governor, for 5 minutes.

Mr. CHAFFETZ. Reclaiming my time, I thank the chairman.

And thank you all for being here.

Ms. Tavenner, a question for you about the Oregon exchange. The American taxpayers put in some $304 million to develop that State exchange. Now they want to come over and make a transition.

Did you or anybody at CMS conduct a cost-benefit analysis to determine that the switch to the Federal exchange was the most cost-effective for the taxpayers?

Ms. TAVENNER. Yes, sir. We did an analysis of what it would cost for us to bring in the two additional we're bringing in this year, Nevada and Oregon. And we did—I wouldn't say it would be a sophisticated analysis, but we did a cost analysis. And, as you might imagine, when we already have 36 States in the exchange, adding 2 more is cost-effective.

Mr. CHAFFETZ. Could you share that analysis with us? Is that something you could provide to us?

Ms. TAVENNER. Certainly.

Mr. CHAFFETZ. What is the additional cost?

Ms. TAVENNER. I don't have that in front of me, but I'm happy to get it for you.

Mr. CHAFFETZ. When is a good time—when would I raise the flag and say, "All right, that's been long enough"? Can you give me a sense of the time?

Ms. TAVENNER. We should be able to get you that in a few days.

Mr. CHAFFETZ. Very good. Thank you. I appreciate that.

Ms. TAVENNER. It is part of our bill that is ongoing???????

Mr. CHAFFETZ. A few more questions about that.

What is being done to claw back—I mean, there's $304 million. Is that money all gone? Is there some of that coming back? Is somebody going to jail? What's going on with it?

Ms. TAVENNER. Each State—and, again, I am——

Mr. CHAFFETZ. I want to talk specifically about Oregon.

Ms. TAVENNER. Yes.

Mr. CHAFFETZ. That seems to be the most egregious.

Ms. TAVENNER. I think Oregon has very actively gone after their contractor, and I think that's been in the press. But I am happy to get you more details——

Mr. CHAFFETZ. But what is the Federal Government doing? It was Federal taxpayer dollars—correct?—that went into it.

Ms. TAVENNER. Yes. These were actually grants awarded to States, and so the contract is between the State and the contractor. So the States were working that initially.

Mr. CHAFFETZ. So CMS, Health and Human Services, Department of Justice, the Federal Government—I mean, pick your entity—we're doing nothing to claw back those dollars?

Ms. TAVENNER. Ultimately—I think it's a little early in the decisionmaking right now. States are going after it on the basis of their individual contracts.

Mr. CHAFFETZ. But the Federal taxpayers give $304 million, and we just say, "Well, it's up to Oregon to figure out what to do."

Ms. TAVENNER. We are obviously working with the State.

Mr. CHAFFETZ. When we gave these grants, was there no condition or expectation that it would work? I mean, was there a deal that said that—did we just literally hand them over the money and we don't care what happens? I mean, it ultimately didn't work, correct?

Ms. TAVENNER. What we did are a series of progress reports and requirements with the States. And I'm happy to get you that information, as well.

Mr. CHAFFETZ. I'm just trying to get some degree of specificity. I haven't heard you yet say we're doing something to try to claw back nearly a third of a billion dollars.

Ms. TAVENNER. I think what I've said is that States are doing that right now. And we are cooperating with States.

Mr. CHAFFETZ. And so—but why is the Federal Government not doing anything?

Ms. TAVENNER. We are cooperating with States. The contract is between the State——

Mr. CHAFFETZ. So we're just waiting for Oregon to tell us something.

Ms. TAVENNER. We are working with Oregon and other States. That's all I can say right now.

Mr. CHAFFETZ. And, Mr. Chairman, I mean, I don't know how——

Chairman ISSA. That's all—just what she said, it's all she's going to say. She won't answer your question.

Mr. CHAFFETZ. I know. I just think it is something that the Congress legitimately should look at. We give out $300-plus million, and we just call it a day and move on?

Ms. Tavenner, is there any criteria or guidance for States who want to drop out and move to our exchange? Have you issued—or how do you evaluate those? Or do you just say "yes"?

Ms. TAVENNER. Well, we obviously have a list of criteria and requirements for the State to move from a State-based exchange to move to the FFM.

These entities stay State-based exchanges. They can continue to do their marketing, their outreach. What we are doing is the FFM support. And there are criteria they have to meet for us to move them back into the system. And I am happy to share that with you.

Mr. CHAFFETZ. OK. So you can—in that package?

Ms. TAVENNER. Yes. We have that.

Mr. CHAFFETZ. Yes. In a few days, you'll share that with me, as well. I appreciate that.

Ms. TAVENNER. We have a lot of documentation.

Mr. CHAFFETZ. Yes, OK. Thank you. I appreciate it.

And, again, for my colleagues here, I just—we really have to look at this. It's stunning to think that we would hand out by the hundreds of millions of dollars to States and have no recourse, and if it doesn't work, we just kind of throw up our hands and say, "Well,

it's up to somebody else to figure it out." That is not the way we should operate. It is pretty stunning and very dissatisfying and doesn't produce results. It's not responsible, it's not accountable, and very frustrating.

I yield back.

Chairman ISSA. I thank the gentleman.

We now go to the gentleman from Massachusetts who was here first, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

I want to thank the members of the panel for your willingness to come here and help the committee with its work.

Ms. Tavenner, generally, the way things work is that the private sector has far more resources than, oftentimes, our government entities, and they are better prepared, better incentivized to keep data secure. And that troubles me because I see a list of—I am also on the Financial Services Committee, as well. And we've been dealing with Home Depot. We've been dealing with Target. We've been dealing with JPMorgan Chase, the largest bank in the United States of America. We're still not sure about the breadth of that breach, but we're concerned about it.

We have Heartland Payment Systems; that was 134 million people in the United States. KB Financial Group, 104 million people. Global Payments system, 950,000 people to 1.5 million; we're not sure yet. They even breached the Iranian banks, about 3 million people. That was probably us who did that. Morningstar, 184,000 people. Citigroup, 360,000 people.

So you've got all these big firms. Especially JPMorgan Chase, they've got some very, very smart people. They have an extreme financial interest, as well as a reputational interest, to hang on to that data.

And so I'm just worried with the—with, sort of, the botched rollout, the difficulty with the State exchanges, including in my State of Massachusetts. We've had a bunch of data breaches related to health care.

Are you sure that you can sit here under oath today and tell me that nobody's breached the, you know, HealthCare.gov site and that the folks whose healthcare information, tax information, personal information—that it remains secure today as we sit here?

Ms. TAVENNER. So let me answer that in a couple of ways. And I will go back to the chairman's point about transparency, as well.

I dare say there is very little that concerns me more on a daily basis than the security of this Website, for a host of reasons. It's a new project. It has been very, very visible in the press on a daily, if not hourly, basis. And we do have the difficulty in the rollout.

We have, even within our limited resources, spent a great deal of time and money securing the Website. We have been able to meet FISMA standards, OMB standards, HIPAA standards. But I will always worry about the safety and security of the Website.

We've talked about the earlier incident with the malware. And yesterday I was informed of another case, not related to HealthCare.gov, but an independent site, if you will, that was working with the cloud, with Website material, where there was another malware incident. Now, there was no personal information.

This is something that I don't even have the details of. But these are the types of things that worry me every day.

We meet about security weekly. We review every——

Mr. LYNCH. Yes. I'm not hearing the answer to my question. And I appreciate all of that. Believe me, I really do. But I only have a minute left, and I think you're going to burn all my time here.

So there's no guarantee that therehas been no breach. I don't want to put it that way, but you don't seem to be able to give me a guarantee that there is not——

Ms. TAVENNER. Well, to date, we have had no malicious breach. We've had no breach of personal information.

Mr. LYNCH. OK. OK. That's fair enough.

Let me ask you: One of the problems we're having with out credit card issuers—and I am just using this as an analogy—is that, for them, you know, that's product. They sell information. I think sometimes, by selling it, they bring on the breach themselves. But they also compile it so that these credit card companies have 15, 20 years' worth of data there all sitting there waiting to be hacked. So my purchases at Home Depot, you know, 10, 15 years ago are still part of that data grouping.

Do we do anything to put firewalls up so that if there is a breach of the medical information that we can somehow limit the damage?

Ms. TAVENNER. So, first of all, yes, it's part of the design of the system. If you remember the hub, no information is stored on the hub. So that was one step.

Second, we do not keep any medical information. There is some personal information, but we don't have a need for medical information. So that's not stored within the FFM.

The only thing that is stored in the FFM itself, separate from the hub, is the ability to work appeals of cases for people who say, "I didn't get a tax credit. I should have gotten a tax credit." So we keep it minimal, but we do have some storage——

Mr. LYNCH. But is that tax information in there?

Ms. TAVENNER. No. There's not tax information. There can be—sometimes people can State their income, but there is not tax information.

Mr. LYNCH. OK. All right.

My time has expired. Thank you for your indulgence, Mr. Chairman.

Chairman ISSA. Thank you. Thanks for a very good round of questioning.

We now go to Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman.

Ms. Tavenner—I'm over here. Want to go ahead, and I'll speed through some of these questions.

Ms. Tavenner, can you confirm that CMS will not change their open enrollment dates? I know we had so many different dates that changed before. Can you confirm to the American people and, really, to the providers that those open enrollment dates will not move?

Ms. TAVENNER. The open enrollment date for this year is November 15th through February 15th.

Mr. MEADOWS. And those will stay firm?

Ms. TAVENNER. Yes, sir.

Mr. MEADOWS. No changes.

Ms. TAVENNER. No changes.

Mr. MEADOWS. They can count on it. OK. That's good news.

All right. How about window-shopping? Last time, you had to actually enroll, put your—I had to go on—when I was shopping, I actually had to sign up to be able to figure out what I want. Is that going to be available?

Ms. TAVENNER. Window-shopping will be available, and you would not have to sign up this year.

Mr. MEADOWS. So we're going to be able to compare plans——

Ms. TAVENNER. That's right.

Mr. MEADOWS [continuing]. Without having to put in any personal data.

Ms. TAVENNER. Yes, sir.

Mr. MEADOWS. OK. Great.

So let me go a little bit further into this. Bryan Sivak has come and shared testimony here with this committee. Are you familiar with who he is at HHS?

Ms. TAVENNER. I know who Bryan is, yes.

Mr. MEADOWS. OK.

Let me read—when we were looking at the rollout, he says, "So to your question"—this was him in an email—"So to your question, how am I feeling about the launch, not good. Kind of heartbroken, actually. Whatever launches, if functional, will only technically meet the criteria of launching the exchange. It will be riddled with confusing and hard-to-use compromises. But I really don't know. I'm not seeing anything that's being delivered. It's just piecing things together kind of through the grapevine."

And so there was not a real communication going on between CMS and HHS during the whole HealthCare.gov launch?

Ms. TAVENNER. I am not familiar with that email. At least I don't think I am. I——

Mr. MEADOWS. Well, I mean, I guess the question is, was there a whole lot of coordination between HHS and CMS technology people going through? Because I have been led to believe that HHS only found out really what was going on through informants.

Ms. TAVENNER. Well, we did weekly updates with HHS on the Website——

Mr. MEADOWS. So they didn't have to have informants to find out what was going on?

Ms. TAVENNER. I can't remember if Bryan was in those meetings or not, but I wouldn't think they would need informants.

Mr. MEADOWS. OK.

Did Bryan recommend to you that the Website launch should be delayed because of security testing concerns?

Ms. TAVENNER. Bryan did not recommend to me that the launch should be delayed. Bryan did discuss in a——

Mr. MEADOWS. Because he shared with the committee that he did. So are you sure that he did not say that we should not delay the launch because of security concerns?

Ms. TAVENNER. I think I need to finish my sentence.

Mr. MEADOWS. My apologies.

Ms. TAVENNER. That's all right. The rest of that sentence is: There was a discussion about would it be possible to beta test or

launch a few States as opposed to bringing up the entire FFM. And I and the team did not think that was possible.

Mr. MEADOWS. And why did you not follow his advice?

Ms. TAVENNER. About the beta site?

Mr. MEADOWS. Well, about delaying it.

Ms. TAVENNER. Yes. So——

Mr. MEADOWS. I mean, you say "beta site," I say "delay."

Ms. TAVENNER. Yes.

Mr. MEADOWS. But whether you're right or I'm right, why did you not follow his advice?

Ms. TAVENNER. Well, I didn't think that it was possible, the way that the FFM was configured, to do that, nor did I think that it was necessary.

Mr. MEADOWS. OK. You shared your testimony earlier; you shared your resume. What part of your resume included IT background? Because that was his expertise. You sounded like you're a healthcare provider, not an IT expert.

Ms. TAVENNER. Well, I am a healthcare provider. I've probably become more of an IT expert in the last year. But I was taking——

Mr. MEADOWS. But at this particular—this was in January. So at what particular point did your IT expert outweigh his?

Ms. TAVENNER. Actually, taking the recommendations of our IT expert team inside CMS, as well as our CMS contractors, who I felt were a lot closer to this issue than Bryan——

Mr. MEADOWS. All right. So now we can look backward and realize that the rollout was a disaster. So what do you think of your IT expertise within CMS today? Was Bryan right, we should have delayed it?

Ms. TAVENNER. I don't know that Bryan was right. I know that——

Mr. MEADOWS. Was he closer to right than your team?

Ms. TAVENNER. Not necessarily. I know that we have come a long way in our launch. And, as I said earlier, we have 7.3 million people paying premiums across——

Mr. MEADOWS. I didn't ask how many had signed up. This is about security, and he had a concern in January about security, and yet you ignored his advice. Why would that have been?

Ms. TAVENNER. Because I had my own IT team who conveyed to me that they were confident in the project.

Mr. MEADOWS. All right.

I yield back. I am out of time.

Chairman ISSA. If either of the other witnesses want to comment on the answer to the gentleman's question about, a year ago, was the site ready and should it have launched in retrospect?

Mr. WILSHUSEN. Well, I would just say that, at the time it was launched, that CMS did accept increased risk from a security perspective.

Ms. BARRON-DICAMILLO. Not having reviewed the data that the CMS IT team had, I wouldn't feel comfortable in commenting associated with that. I think it's important to have eyes on the project and be part of the team to make those decisions. It's very difficult as a third-party partner participant to make that kind of assessment without the actual knowledge and data.

Chairman ISSA. Well, as a former businessman, I would say that a site that couldn't accommodate a few hundred people simultaneously signing on and people waiting for weeks or months, security wasn't the reason that that should not have launched. But I appreciate that you're here on security today.

The gentlelady from New York, a place where IT comes first for many of her constituents, is recognized for 5 minutes, Ms. Maloney.

Mrs. MALONEY. That's true. And that's true of the west coast, too.

I just want to note that this is the committee's 29th hearing on the Affordable Care Act and the sixth on the Website.

Chairman ISSA. We've got two more to go.

Mrs. MALONEY. Oh, come on. Please.

I want to focus on some very positive things, and that is the cost growth is slowing to historic lows. And that was one of the huge challenges that we confronted the whole time that I have been in Congress, is just the whopping cost in health care in our country.

Now, contrary to some of my colleagues' claims that the Affordable Care Act is causing healthcare costs to skyrocket, there have been multiple reports recently that show that the growth of healthcare spending in the United States is slowing to historically low levels. And that is good news for everyone.

Administrator Tavenner, earlier this year, the Centers for Medicare and Medicaid Services issued its national health expenditure report. Are you familiar with that report?

Ms. TAVENNER. I am familiar with that report.

Mrs. MALONEY. Well, the report found that national health spending grew by just 3.7 percent in 2012, a near-record low, and the fourth consecutive year of slow growth of healthcare costs.

In your opinion, what factors are driving this historically low rate of growth?

And I'd like the others to chime in, too, if you would like to add to her response.

Ms. TAVENNER. I think that we all felt it was a combination of things: certainly, the recession early on; but as time went by and we continued to see this historic low growth, I think some of the actions in the Affordable Care Act have made a difference.

And it is an ongoing conversation I have with my actuary. And I think he would agree, if he were siting here with me, that it's both. But the Affordable Care Act has made a difference.

Mrs. MALONEY. Mr. Wilshusen?

Mr. WILSHUSEN. I'm sorry, that was outside the scope of my review, so I can't really comment on it.

Mrs. MALONEY. OK.

Any comment, Ms. Barron?

Ms. BARRON-DICAMILLO. That is something that I have not been involved in as the Director of US-CERT.

Mrs. MALONEY. OK. Fine.

Well, earlier this month, CMS released its national health expenditure projections for 2013 through 2023. And according to these estimates, national health expenditures grew just 3.6 percent in 2013. Is that correct?

Ms. TAVENNER. I believe that is.

Mrs. MALONEY. This is the lowest rate of growth since the Federal Government began keeping such statistics since 1960. I would call this a very positive development in public policy. Would you agree, Ms. Tavenner?

Ms. TAVENNER. I would totally agree.

Mrs. MALONEY. What about the next 10 years? We're always looking ahead. I know CMS projects an uptick in health spending overall due to the large number of people who are newly insured through the Affordable Care Act, but what about per-enrollee health costs?

Ms. TAVENNER. So, going back to that report, I think the trend is expected to move back up, with the number of individuals in Medicare and others. But I think that stresses the importance of our success in tying together delivery system reform, payment and quality, and why that works is critical that we continue it.

Mrs. MALONEY. Well, why will they grow more slowly than before the Affordable Care Act?

Ms. TAVENNER. I think because of some of the measures that we've put in place with the Affordable Care Act, such as tying payment to quality, tying payment to outcome, looking at things such as accountable care organizations, kind of transforming the delivery system, which is a work in progress.

Mrs. MALONEY. Now, the Kaiser Family Foundation recently released an annual employee health benefit survey. And this report indicates that the slowdown in health spending also extends to employer-sponsored insurance—more good news. And according to Kaiser, premiums in employer-sponsored health plans grew only 3 percent in 2012.

So I would like to ask you—that's tied for the lowest rate of growth since Kaiser started measuring the growth of employer healthcare plans. And is that report correct? Do you agree with the Kaiser report with the data you've been looking at?

Ms. TAVENNER. Yes, I've reviewed the Kaiser report, and employer insurance does tend to follow what we're seeing in Medicare and Medicaid. So yes.

Mrs. MALONEY. Well, this seems to be very good news for the American consumers and our overall delivery of healthcare service. So I'm very pleased with these reports. And what do they say? Numbers don't lie. And the numbers are showing that it's showing an improvement. So I want to congratulate you and your colleagues on your work to help brings this to the American people.

Thank you.

Ms. TAVENNER. Thank you.

Chairman ISSA. Thank you.

The gentlelady from California, Ms. Speier.

Ms. SPEIER. Mr. Chairman, thank you.

And thank you to our witnesses.

First of all, I'd like to congratulate you. You have lived through the real-life "Survivor" show and have succeeded.

I find the fact that we have engaged in the most thorough, repetitive review of the implementation of the ACA as an incredible waste of your time.

Now, there is a lot of good news, as my good colleague from New York has just underscored. And it is really quite interesting to me

that, for the longest time, there were all those who were panning the Affordable Care Act, saying, we'll never get the numbers. And then, lo and behold—and you announced it earlier, Ms. Tavenner, I believe—over 7.3 million subscribers. Correct?

Ms. TAVENNER. Correct.

Ms. SPEIER. And then the hew and cry was, well, they won't pay for it; they'll pay 1 month, and then they won't pay any longer, and it will fall on its face.

That hasn't been the case either, has it?

Ms. TAVENNER. No, ma'am.

Ms. SPEIER. OK.

So the chairman of the committee and a number of Republicans just sent you a letter, and I want to read it out loud, one segment of it.

"In order to enroll beneficiaries in the exchange, HealthCare.gov collects, obtains, and retains massive amounts of personally identifiable information about millions of Americans. This information includes Social Security numbers, personal addresses, income and employment records, and tax return records. It is extremely important that CMS and the other Federal agencies involved in the exchanges properly protect and maintain this sensitive information."

Now, I actually agree with that Statement, and I presume you agree with that Statement.

Ms. TAVENNER. Yes, I do.

Ms. SPEIER. And having agreed with that Statement, have you, to date, had any cyber attacks that have resulted in personally identifiable information being stolen?

Ms. TAVENNER. We have not had any malicious attacks on the site that have resulted in personal identification being stolen. As the chairman rightfully brought up earlier, we did have some technical issues on the front end that we had that were our own doing that we had to——

Ms. SPEIER. That's right. But we're in the present day, and let's look to where we are and where we're going. OK.

Now, meanwhile, Target's security breach included 110 million Americans that were potentially affected. That's 110 million. You're certainly aware of that.

Ms. TAVENNER. Yes, I am.

Ms. SPEIER. So my staff checked the U.S. Census Website, and it says the total population of the United States is 319 million. So more than a third of Americans potentially had their personally identifiable information breached, stolen, as the result of that Target data breach. But, strangely, there wasn't any interest by this committee to have a hearing on that, affecting potentially a third of the American people.

Let's see, 110 million people affected and no hearing; zero people affected, and we've had dozens of hearings. It seems like our priorities are not quite on what the American people would be interested in.

Now, we do know, as a result of Target, that the hacking came from outside this country. It appears it came from Russia or from some region near there. And rather than trying to find out where these hackers are coming from and how we can forestall them,

we're going to waste more of your time asking you a number of questions about issues that haven't even impacted.

Now, some would say, well, except that's a private business. Well, how about USIS? USIS has a contract with the Federal Government. It does security checks. And 27,000 people have had their personal information stolen from USIS, a Federal contractor. And have we had a hearing on that? Nope. It appears that's not important either.

So I want to just commend you all for recognizing that you have to do this no matter what, come to these committee hearings. You do it with great respect, and we appreciate that. I hope we can send you back to do work that the American people would like you to do.

And I yield back.

Chairman ISSA. We now recognize the gentlemen from Maryland for 5 minutes.

Mr. CUMMINGS. I want to thank all of you for being here today as we come to the end of this hearing.

I'd just—you may—Ms. Tavenner and others, you may never hear the full thank-yous of people who are going to stay alive because of what you and your colleagues have done. And I really mean that. There are people—there's a mother who is now going to be alive, that may have been suffering from cancer, breast cancer, like a lady in my district, couldn't get treatment, but she's alive. She got treatment.

I have a sister that does a lot in the area of breast cancer, and they were waiting—they had women who had been tested, and they were waiting for the Affordable Care Act to pass and to come into effect so they could get treatment. I have come to you today and to your colleagues to thank you.

I tell the story that, when the Affordable Care Act came up, I had one prayer. I came to the floor early. I sat on the front row, and I had one prayer. I said, "God, do not let me die before I vote for it." And the reason why I said that is because I've seen so many people who were sick and could not get well.

You know, Johns Hopkins is smack-dab in the middle of my district—a great hospital, one of the greatest in the world. People fly from all over the world to come to Johns Hopkins. And there are people standing on the outside, could not get in, but the treatment was in there.

And so, you know, I know your colleagues are looking on, and I just don't want—I know they have been through a lot.

And I remember when we had the Website problem, and many were saying, oh, we can never get through this, oh, you know, this is just so horrible. And everybody was warning that everything would collapse. But you know what I said? This is a can-do nation. This is a can-do nation. And we need to definitely do when it comes to the health of every single American.

And I listened to what you said a moment ago about how, day after day, you worry about making sure that people's information is protected. We could not pay you enough or pay your colleagues enough to go through what they have been through and to worry as you have worried and to do everything in your power to be protective of the American people. And, yes, you're going to be criti-

cized. Yes, folks are going to try to say all kinds of things about you. But I have come here at this moment to simply say thank you. Thank you for my constituents. Thank you for constituents—our constituents all over this country.

And, you know, sometimes I think about illness, and a lot of people—I wonder if people have not been ill themselves when they see other people in the position of getting sick or sicker and dying. I wonder whether or not they have ever been ill. And that troubles me because—I think President Obama said it best, and I wish I had coined this phrase myself. He said, sometimes we have an empathy deficit—an empathy deficit.

And so I take just a moment to thank you and just have just a few questions.

I'd like to ask you about the attack by the hackers last summer against HealthCare.gov. It is my understanding that this attack was not limited to HealthCare.gov alone but included a broader universe of targets. Is that right?

Ms. BARRON-DICAMILLO. So based upon the analysis that our team did, it was a typical kind of malware that's dropped for denial-of-service attacks. So, basically, they were trying to create a node and a botnet to use for denial-of-service attacks. So, yes, they look at resource servers like this to use them for those types of attacks.

Mr. CUMMINGS. And the hackers were able to place malware on a server, but it was a test server that did not have any personal information. Is that correct?

Ms. BARRON-DICAMILLO. Based upon the analysis that our team did, it was a test server that was deployed with its out-of-the-box configuration, meaning that the password—the default password hadn't been updated.

Mr. CUMMINGS. I just have two more questions.

As I understand it, the type of malware at issue is called denial-of-service——

Ms. BARRON-DICAMILLO. Uh-huh.

Mr. CUMMINGS [continuing]. Malware, which is designed to slow down or even shut down the system but not extract information. Is that right?

Ms. BARRON-DICAMILLO. Correct. The malware is to use the resource of the server as part of this botnet. And so it wasn't targeting the server; it was using the resource of a server as part of the botnet for another victim.

Mr. CUMMINGS. And so how common are these kinds of denial-of-service malware attacks?

Ms. BARRON-DICAMILLO. I'm sorry?

Mr. CUMMINGS. How common are they?

Ms. BARRON-DICAMILLO. They're very frequent. They happen every day across the globe on the Internet.

Mr. CUMMINGS. So the bottom line is, at least as of now, no personal information was transmitted outside the agency. Is that right?

Ms. BARRON-DICAMILLO. Correct. The breach was discovered by CMS. It was alerted to us. We looked at the images that were provided. There was no exfiltration of data. There was no loss of PII due to the segmentation of the network. This is a test network sep-

arate from the production network. So there was no lateral movement into the production network associated with this activity.

Mr. CUMMINGS. All right. Thank you.

Ms. BARRON-DICAMILLO. Thank you.

Chairman ISSA. Well, I guess—I've still got more questions, but let me just make some Statements, and then I'll ask a couple more questions.

You know, Ms. Speier has left, and it's unfortunate because Mr. Lynch was here earlier, and when this was all being said about when are we going to hold all kinds of hearings, they forgot to mention that there's a committee that Mr. Lynch belongs to, the Financial Services Committee, and they've held hearings because they oversee the financial community, meaning Home Depot, Target, these other companies they're referring to. Those fall under that committee's primary oversight because these were financial-transaction-related.

My staff also mentions that the Federal Trade Commission, the Department of Justice, the CFPB, and the FDIC also are looking into each and every one of those.

So, with tens of millions of dollars, countless agencies and individuals looking at each of these, the question is, Ms. Tavenner, who's been looking at you?

Mr. Wilshusen, in a nutshell, one of the things that you said at the beginning was they didn't have strong passwords, so somebody could put in a short password and not change it. Is that correct?

Mr. WILSHUSEN. That's correct. We identified several technical security control weaknesses with HealthCare.gov and its supporting systems.

Chairman ISSA. So somebody who didn't change the password created a huge vulnerability, particularly if they had a high level of access. Is that right?

Mr. WILSHUSEN. If they used a weak password that could be easily guessed, that would be an increased risk.

Chairman ISSA. So "Marilyn" and her birth date, if that were used, would have been easy to guess, certainly would have been tried.

Did they have advanced lockout systems in detection and reporting?

Mr. WILSHUSEN. One of the things—I don't want to get too detailed into the types of security controls so we don't give any information——

Chairman ISSA. Yes, we don't want to tell how weak it still is. I understand that, so I'll be a little bit careful on that. But there are techniques that, if they were in place, would have been much more secure.

Mr. WILSHUSEN. Sure. And the weaknesses that we identify are all—can be corrected and resolved almost immediately.

Chairman ISSA. So what you found a year into this site was they were not using best practices.

Mr. WILSHUSEN. We identified several weaknesses that increased risk and unnecessarily increased preventable risk.

Chairman ISSA. We pay a huge premium for CIOs, Senior Executive Service. We, the Congress, have authorized special high pay, a quarter of a million dollars and more, to get certain people with

special expertise. And we've had some of them before this committee.

You're telling us, a year into this site, they simply have not put in what people would consider best practices in some cases, such as a requirement for a strong password and periodic changing of them and a lack of redundancy on passwords—common things that protect sites, right?

Mr. WILSHUSEN. Yes, those things should be done. Yes.

Chairman ISSA. You know, what's amazing is Target and Home Depot had those kinds of protections, but there was a malicious attack from a foreign nation with advanced tools, some of those tools being exactly the tools that our CIA and NSA use to go after the worst of the worst, and we succeed all the time.

So what I'm finding here today is that everyone wants to talk about organizations that employed, in many cases, best practices, that did their best, and then were targeted by very advanced networks, criminal networks, networks that may even have had the KGB's successor helping them hack. And they want to talk about those rather than a lack of commonsense, simple practices to secure a Website. Isn't that true?

Mr. WILSHUSEN. I would say that probably the majority of Federal incidents that occur within the Federal Government could be resolved, perhaps prevented, if agencies would practice strong cybersecurity. There's always going to a risk that you come across an entity, a foreign intelligence service that has very sophisticated techniques that may be difficult to protect against, at least to prevent. But, by and large, many security incidents could be corrected and prevented if the agencies practiced strong security controls.

Chairman ISSA. Now, even without seeing the 13 compromises that occurred, you were able to make, and CMS accepted, a lot of suggestions that are improving the site here today.

Mr. WILSHUSEN. Yes. We've looked at the security controls over those devices that we looked at and identified vulnerabilities that could be corrected. And CMS concurred with each of the 22 technical recommendations that we're making.

Chairman ISSA. So all of the talk about this robust team, all of those experts brought in from Silicon Valley, special people that worked on the President's reelection, all those people had missed those 22 points.

Mr. WILSHUSEN. That I can't answer in terms of——

Chairman ISSA. Well—but when suggested these, did they say, oh, we were already doing them, we just forgot? Or did they say, we weren't doing them and now we will?

Mr. WILSHUSEN. I would just say that we identified them during the course of our review, and they've accepted our findings and indicated that they will implement our recommendations.

Chairman ISSA. You're very kind.

Ms. Tavenner——

Mr. MEADOWS. Would the gentleman yield for just one quick point?

Chairman ISSA. Of course.

Mr. MEADOWS. A lot has been talked about in terms of the different sites and Home Depot and Target. And I was one of those that shopped at Target, and I have a new credit card today.

There are two distinct differences. One is I'm not compelled by law to shop at Target. I am compelled by law to sign up for Obamacare. There's a huge difference.

Mr. Chairman, what happens is that those are voluntary transactions, of which I don't have to give my Social Security number to them. I give them a credit card, and I do a transaction. It's very different for HealthCare.gov.

I thank the gentleman.

Chairman ISSA. That's very true. I thank the gentleman.

We now go to the gentlelady from New Mexico, who has arrived, for a round of questioning.

Ms. LUJAN GRISHAM. Mr. Chairman, thank you very much for recognizing me.

And I want to thank the panel here today.

And I share many of my colleagues' concerns that we should be doing the very best to protect information. And, certainly, we've led in the private-sector world, with HIPAA and related requirements, on security protections and working diligently and tirelessly to make sure that patient protection, patient privacy, and now financial information must be protected.

And I think that the point is important that every person must sign up and be insured through the Affordable Care Act. And I want to just read this because I think it bears—in the context of this hearing, I think it bears repeating.

So, in GAO, in the March 2013 report, found that the Federal Government continues to face cybersecurity challenges, including designing and implementing risk-based cybersecurity programs at Federal agencies, establishing and identifying standards for critical infrastructures, and detecting and responding to and mitigating cyber incidents.

And, since that report, we've got 28 GAO additional recommendations that I know that we've been talking about today in this hearing.

In fact, GAO has designated Federal information security as a high-risk area in the Federal Government since 1997. And I think that there isn't anyone in this committee or anyone in Congress or the public that doesn't think that more should be done and that, in fact, that we embrace every potential positive, productive, professional recommendation moving forward.

And so, given that, Ms. Tavenner, knowing that the upcoming November open enrollment period is coming for millions of Americans who will be shopping on the exchanges, how prepared are you to take these 28 recommendations and others to assure protection?

Ms. TAVENNER. Yes, ma'am. Let me start with the 22 technical recommendations. Nineteen of those have been resolved, fully mitigated, or will be further reviewed prior to open enrollment. So those will be handled. Of the six other recommendations, we are in the process of either completing—have completed those or will complete those prior to open enrollment.

Ms. LUJAN GRISHAM. And based on the 19 that you have identified, Ms. Tavenner, and the remaining measures to implement, you are confident that not only are they implemented but they're tested and will have, to the greatest degree—I mean, I might disagree with some of my colleagues, that we can do everything in our

power, and those hostile, those negative, those who intend us harm and intend to access that information for their own gain will find ways to do that. I want to make sure that we are doing everything that we know that mitigates and prevents and gives us the opportunity to also detect when there has been a problem.

You're confident that these will be tested and in place by the open enrollment period?

Ms. TAVENNER. I am confident. But we will never quit continuing to try to improve the process. Our work with the Department of Homeland Security, our work with GAO, OIG will always be looking for improvements.

Ms. LUJAN GRISHAM. I appreciate that. And given that we know we are working on another issue in my State, I appreciate your attention to that and your coming.

Mr. Chairman, we're working a behavioral health issue. For me, it all ties to making sure that consumers have confidence that they're protected in a way that CMS is responsible to protect those citizens, that they are clear that your responsibility and oversight is paramount to the work that you do, and that the access to health care is only as good as making sure that the information and the protections that are required by law are, in fact, in place and that they can go to CMS when there is a problem and have that resolved objectively and appropriately.

And I really appreciate your attention to all those matters.

Ms. TAVENNER. Thank you.

Mr. CUMMINGS. Would the gentlelady yield?

Ms. LUJAN GRISHAM. I yield.

Mr. CUMMINGS. Ms. Tavenner, I just want to make sure that I understood what you just said, that—and I agree with every word that my colleague just said. But you're saying that there are six recommendations left. Is that right?

Ms. TAVENNER. There were six major—and please correct me, Greg, if I get any of these wrong—there were six major recommendations. And we're in the process of completing those, and some of them are done. And the answer to those is all of them would be done prior to open enrollment.

Mr. CUMMINGS. And open enrollment starts when?

Ms. TAVENNER. November 15th.

Mr. CUMMINGS. So we can—can this committee—would you let us know officially when they are done?

Ms. TAVENNER. Yes, sir. I think——

Mr. CUMMINGS. To the chairman and myself? I'd really appreciate that.

Ms. TAVENNER. Yes, sir.

Chairman ISSA. If the gentlelady would further yield?

The earlier report we had is you didn't agree to all six, but you agreed to three out of the six. You now will agree and complete all six?

Ms. TAVENNER. So I think in some of them we partially concurred, but we're getting the work done, whether we totally agreed or not.

I think there were some things—for instance, there was a different description of how we did security testing versus what GAO wanted. That wasn't an action we would change, but we under-

stand where they're coming from. We just have a different way of getting the security testing done.

The rest of these, things such as the privacy impact Statement, we will have that done. That was a documentation issue. The computer matching agreements with Peace Corps and OPM, we agreed with that, and we'll get that in place prior to open enrollment. Also a security agreement governing Equifax, we agreed with that; we'll complete that.

Of the 22 technical recommendations, 19 we have already done, the others we're reviewing. And I'll be happy to do something in writing back to the chairman and to the ranking member.

Chairman ISSA. I think we both would appreciate it.

Ms. TAVENNER. All right.

Chairman ISSA. The gentlemen from North Carolina?

Mr. MEADOWS. I wanted to followup on one thing, Ms. Tavenner. And, really, as we start to focus on some of these other issues, it takes our eyes off of the core issue, and that's what the ranking member was talking about, is providing health care really to the American public. And that is your primary responsibility. I can tell that you take that seriously.

It is a distraction, to say the least, when we have a billion dollars spent on a Website that doesn't work, security issues that are there. But along that same time, there was a rule that came out with regards to Medicare Part D in January, a rule that really would limit some of the options of our seniors, a rule that you came, much to your credit, and said we are not going to do. And I want to say thank you for doing that on behalf of millions of senior citizens who would have seen choices limited.

Do I have your assurances here today that we are not going to put forth a rule that is similar in nature to that rule that was brought back? I very rarely have an opportunity to have you in a public forum under oath. And so, on behalf of millions of Americans, do I have your assurances that we are not going to do it?

I think you made a good decision. My mom, who is a senior citizen, thinks that you made a good decision. So do I have your assurances that we will not see a similar rule?

Ms. TAVENNER. I am not interested in bringing back the pieces that we pulled.

Mr. MEADOWS. OK. That is a good almost answer. So do you have your——

Ms. TAVENNER. Well——

Mr. MEADOWS [continuing]. Assurances, yes or no?

Ms. TAVENNER. You have my assurances that I won't bring back the things I just pulled. How about that? I don't have the whole——

Mr. MEADOWS. Or something similar.

Ms. TAVENNER. Or something——

Mr. MEADOWS. Let me tell you the reason why. And it gets back to—CBO indicates that much of the reason it is working so well is the competitive nature that we have. I mean, that is what the study says. And yet we are going to limit competition. We are going to limit options for our seniors—some cancer, some antidepressants, some antiepileptic. These are serious things.

And so you and I can banter back and forth, but really what I need is, on behalf of the American people, your assurances here today that that is not going to happen.

Ms. TAVENNER. Now you are bringing in specifics. I am not interested in bringing back the drug categories, if that's the question. I am not interested in bringing that back.

I am interested in promoting competition, promoting private market. And I think we have tried to do that with the marketplace rules, as well. So we would continue to work——

Mr. MEADOWS. So we are not going to limit competition, and we are not going to narrow what people can get.

Ms. TAVENNER. That would be my preference, yes, sir.

Mr. MEADOWS. That's your assurance?

Ms. TAVENNER. That's my assurance.

Mr. MEADOWS. All right. Thank you.

I yield back.

Chairman ISSA. Could you yield to me?

Mr. MEADOWS. Sure. I would be glad to.

Chairman ISSA. Briefly, item four from the GAO says, "Perform a comprehensive security assessment of the FFM, including the infrastructure platform and deployed software elements."

Now, initially, that was one you said "no" to. Are you saying you will perform that full system-wise test and have it done by November 15th? Because that's sort of the one that GAO couldn't—we can't know what we don't know until you do that. Is that right?

Ms. TAVENNER. I think we get into a discussion of style here. It is our intention—and we will complete a full, end-to-end assessment, security assessment, prior to open enrollment, yes, sir. That is scheduled for later this month or October.

I think where we got into a different conversation had to do with infrastructure and platform in our definitions, but I think our intentions are the same.

Chairman ISSA. Why don't we let—Greg, if you would give us the rest of that.

Mr. WILSHUSEN. Right. As long as the tests that they perform include how the applications interface with the operating platforms—and the infrastructure to look at it in totality is going to be critical. Because certain vulnerabilities on levels or layers of the security could affect the security of the other components of it because there are a number of components involved with this Website and its supporting systems and a number of different entities involved with their operation——

Chairman ISSA. And so, for the layperson out there, would it be fair so say that, for example, when software opens a portal on a particular piece of equipment that that can create a vulnerability in one type of hardware that it wouldn't in another, that that's the kind of thing—that they have to look at the actual hardware they are using, what it interfaces with and so on. Isn't that right?

Mr. WILSHUSEN. To include looking at the firewalls and the routers and switches that support it, as well as the operating systems and how they're being configured, yes, sir.

Chairman ISSA. And, I presume, any remote access devices, any VPNs, any of that, would be part of it. Because all it takes, if I understand right, is one PC that has a VPN connection that isn't in

the software, but once you put it in, it can create a separate vulnerability, right? And that's what you're looking for.

So if I saw the heads nod—and I like that—the two of you are going to—one of you is going to come back to the ranking member and myself if this agreement that you're going to do that by November 15th doesn't happen. Is that right? Maybe both of you.

Mr. WILSHUSEN. I would be willing to work with your staff to do some follow-on——

Chairman ISSA. I think that's all that Mr. Cummings and I would like to know, is that since you're shaking your heads and smiling now, that if that stops between now and November 15th, one of you will tell us.

Mr. WILSHUSEN. Yes, sir.

Chairman ISSA. Mr. Cummings?

Mr. CUMMINGS. I mean, I'm going to encourage you to do that. Just do it, please.

Ms. TAVENNER. We will do that.

Mr. CUMMINGS. And I'm not trying to be smart. I mean, Ms. Tavenner, I know that—and all of you—I know you're trying to do what is in the best interests of the American people. I understand that. But it seems as if what we want is the highest level of best practice.

Am I right, Mr. Chairman? The highest level.

Chairman ISSA. Absolutely.

Mr. CUMMINGS. And, Ms. Tavenner, I couldn't help but—when I was thanking you on behalf of my constituents, I could see a tear come up in your eye. And, you know, so often I think Federal employees—a lot of people don't realize that a lot of our employees, most of them, are not in government for the money. They're in it—and I have people coming trying to work for our committee all the time who are willing to take reduction of salaries from the private sector because there's something about this that feeds their souls, something about lifting up the public and making their lives better.

And so, to all of you and to all of the Federal employees who may be listening out and the ones behind you, Ms. Tavenner, and all the ones that may be in the audience and up here, I just want to thank you very much.

Thank you.

Chairman ISSA. Thank you.

And I understand the gentlelady from New Mexico—did you have any followup questions, Ms. Grisham?

Ms. LUJAN GRISHAM. Mr. Chairman, I don't. I was thanking you. And I appreciate both the leadership of the chairman and the ranking member to assure that we get feedback. And they represented very effectively all of my concerns and points. So thank you very much for your leadership.

Chairman ISSA. Thank you.

I've got a couple very quick wrap-ups that came out of these. And big smile because we're nearing the end.

There was a question about more people being insured. And I just have to ask, is Medicaid insurance?

Ms. TAVENNER. In my opinion, Medicaid is insurance for sure.

Chairman ISSA. So——

Ms. TAVENNER. But that was not part of what I was——

Chairman ISSA. But the actual level of insurance under Medicaid that was talked about, it's Medicaid insurance. That's what's lowering the number of uninsured, is Medicaid.

Ms. TAVENNER. Plus the marketplace. Both are lowering that number.

Chairman ISSA. Which is then subsidies, primarily.

Ms. TAVENNER. So——

Chairman ISSA. The actual number of people who are receiving unsubsidized health care has gone down. Is that right?

Ms. TAVENNER. You know,—and I don't have all the reports in front of me, but, actually, the number of people insured off the exchange without subsidy is also rising. I don't have the latest private insurance. Private insurance had a negative trend that had been going on for the last 10 years. That seems to have kind of stabilized out. If you add Medicaid and you add the marketplace exchange with or without subsidy, I think that's what you're seeing——

Chairman ISSA. Sure.

Well, the reason is that—those questions led to this, sort of, feeling that everything was better, but isn't it true that the Medicare trustee Charles Blahous—or "Blahous"—he projected that by 2021 the impact of the Affordable Care Act will be a $346-billion to $527-billion increase in the deficit, essentially because the government is going to pay that 190 percent for Medicaid, the government is going to provide those subsidies. And the government is, in fact, the taxpayer. So the deficit will rise based on the money that buys that insurance. Is that true?

Ms. TAVENNER. I am not familiar with that report.

Chairman ISSA. OK. But the government is—general tax revenues are, in fact, paying for these subsidies and for Medicaid. It doesn't come out of a trust fund. Medicaid is ordinary income tax. Is that correct?

Ms. TAVENNER. I'm sure that you know that, Mr. Chairman. I don't——

Chairman ISSA. For the record, Medicaid is paid out of income tax, and much of Medicare is paid out of income tax. The trust fund, when we talk about it, pays only a small part of what our seniors reflect.

Now I have really the final question, and it's one that deeply concerns me. And it wasn't the main topic today, but it's right in your lane.

On May 15th, you projected 8 million as an enrollment number. August, it's now 7.3 million. What happened to that 700,000 to 800,000 people? Why was there such a precipitous drop?

Ms. TAVENNER. So the 8 million individuals—and I think that number was after the end of open enrollment—had signed up. And I think, during the course of the next several months, individuals may have either gotten employer-sponsored insurance, they may have found out they were eligible for Medicaid instead of the marketplace, and some individuals may have decided not to go forward and pay.

I think there was always——

Chairman ISSA. Well, that's a great question. And the reason I asked that question is, you know, people were asserting that signing up meant nothing and paying meant everything.

How much of that 700,000-plus drop were people who did not pay? Or do you know?

Ms. TAVENNER. I don't know that information.

Chairman ISSA. Wouldn't it be all of those people did not pay?

Ms. TAVENNER. I don't think we'll know that till the end of the year. And then we will probably——

Chairman ISSA. Well, let me ask the question a different way. Because, you know, I am an old businessman. People signed up; they were, therefore, insured. Is that correct? They enrolled; they were insured.

Ms. TAVENNER. These were people who signed up for a plan. But, in order to get insured, you had to make a payment.

Chairman ISSA. Well, no. They were insured right away, and then, if they didn't make the payment, they went off.

Ms. TAVENNER. Within 90 days, right.

Chairman ISSA. So they basically got a free ride; 700,000 people got a free ride. They had coverage, and if something catastrophic happened, they could make a payment. And if something catastrophic didn't happen, they could just let it drop.

Ms. TAVENNER. I don't think we know that information.

Chairman ISSA. Oh, no, this is a structural question that I know you must know or the technical people behind you must know.

If 8 million people sign up—let's just say 8 million people sign up, and not the 700,000 who dropped, but let's just say 50 people out of 8 million had a health event, and they weren't going to pay, they just signed up on a lark because it's a free ride to sign up, but then they had a health event, did they get to go to the doctor during that 90 days because they had signed up and hadn't yet paid?

Ms. TAVENNER. Yes.

Chairman ISSA. So the system as it is today is an incredibly easily gamed system, if I understand correctly. Three hundred and 16 million Americans could all sign up and get 90 days worth of free insurance, and if nothing happens, there's no downside to their just letting it lapse by not making a payment. Is that right?

You don't done them. You don't go after them. You don't followup. You don't sue them for the coverage they had but never paid for, do you?

Ms. TAVENNER. Which, I think, is why it's important to know that, as of August, 7.3 million were making their payments and were still continuing the insurance——

Chairman ISSA. So 7.3 million people may have made small payments because they were highly subsidized or larger payments because they weren't. Are you prepared to release those figures anytime soon so we understand, of the 7.3 million, how many of them, if any—well, there would be some—were completely unsubsidized, how many were partially subsidized, how many were substantially subsidized?

Ms. TAVENNER. Yes, we will have that information. And as soon as we have it, we will release it. But, yes, we will be able to talk about numbers.

Chairman ISSA. Estimate of when?

Ms. TAVENNER. I don't have an estimate, but I'm happy to get that for you.

Chairman ISSA. OK.

Being an old businessman, I must admit that giving people 90 days free and no retrospective look to find out whether, in fact, they were maybe dual-insuring, maybe just signing up for a lark, to me, means that your initial figures are of no value and that people should be cynics and say we don't know how many people have signed up.

But next year, starting November 15th, I'm presuming that if GAO is going to estimate the signups, they are going to be able to only use—that if you get 8 million again, they can assume that 7.3 is the net number, right?

Ms. TAVENNER. I think 7.3 is a really strong number. And I would remind you that those individuals who sign up and get tax credits still have a reconciliation process next April. Right?

Chairman ISSA. Yes, we're looking forward to that part to see if there's a clawback.

My parting question: This committee held a hearing on the issue of over $15 billion owed to the American people by the State of New York for excess payments in violation of the law, in violation of CMS maximums. That falls under your watch. Have you done anything to reclaim that $15 billion?

Ms. TAVENNER. Yes, sir, we have. We initiated——

Chairman ISSA. And have you gotten any of it back?

Ms. TAVENNER. We recently initiated that. I don't think we have gotten any of it back yet, but we sent the—basically the request for recovery.

Chairman ISSA. You've made a request for recovery.

Ms. TAVENNER. We follow our normal process.

Chairman ISSA. Do you have the authority to simply withhold, the way you would to a private entity? You know, if I'm a doctor and I overbill $15 billion or maybe some minor amount less than that if I'm less hardworking, the first thing you would do is would cutoff payments for services, right? You simply wouldn't send them a penny.

You're sending millions or billions of dollars to New York every month, aren't you?

Ms. TAVENNER. So I can brief you or your team on this in some detail. Initially, what we would do, whether it's a doctor or an entity or whatever, is we ask them how they would like to repay us. And we normally——

Chairman ISSA. I wish that were true.

Ms. TAVENNER. I think that——

Chairman ISSA. I've had too many healthcare entities who make it very clear, your people come in, you make a determination, the moment you make a determination they basically have to quit their practices and go into an appeal process, and in the meantime they're not receiving a penny, and you claw back.

So do you want to State that in a way that the private-sector people don't call me up and say, how did you let her say that you give people lots of time and ask them how they'd like to repay it?

Ms. TAVENNER. Well, and I think you know I was on that private-sector side for quite a period of time. And so if there is a question of overpayment, yes, CMS will make you aware of an overpayment situation——

Chairman ISSA. And then claw back real fast.

Ms. TAVENNER. Unless you want to pay them up front, in which case——

Chairman ISSA. If you're able to write a $15-billion check, they won't deduct from the revenue.

Ms. TAVENNER. Right.

Chairman ISSA. Is New York prepared to give you a $15-billion check?

Ms. TAVENNER. I can't speak for New York.

Chairman ISSA. But right now New York and perhaps others owe the American people money from excess payments, and they're not being treated the way private sector is being treated. They're being treated a little bit with kid gloves. Fifteen billion is a lot of money.

Ms. TAVENNER. Actually, we went through the first year, and we made a request or demand for the money. And I'm happy to brief your staff on that.

Mr. MEADOWS. Will the gentleman yield?

Chairman ISSA. Of course.

Mr. MEADOWS. You have hit on an area that we have had a number of hearings already with regards to RAC audits. And I would implore you to treat New York the same way you're treating the constituents in my home State of North Carolina. Because very quickly what you do is you put private companies out of business because you deny the claim and you say, you either pay up or you go home.

And if you're not going to treat New York the same way you treat North Carolina, I've got a real issue with it, Ms. Tavenner.

Ms. TAVENNER. So we would treat New York the same way we treat every other State. And——

Mr. MEADOWS. Well, no, I'm talking about government versus private.

Ms. TAVENNER. We would treat——

Mr. MEADOWS. Because I'm talking about private companies.

Ms. TAVENNER. I'm sorry. We would treat New York the same way we would treat anyone who owes us funds.

Now, New York—I just got this information from my staff—has appealed this decision, which is the same option that anyone has.

Mr. MEADOWS. Right. And a private company, when they appeal, the answer is the same: Pay up in 5 years or go out of business.

Ms. TAVENNER. I understand.

Mr. MEADOWS. I mean, the statute says 60 months. I know it very well.

Ms. TAVENNER. I know. We have treated States the same way we treat providers.

Mr. MEADOWS. All right. So they are going to have to pay up within 60 months, New York?

Ms. TAVENNER. I'm happy to get you information. I just don't have it in front of me. But we treat——

Mr. MEADOWS. All right.

I yield back. Thank you, Mr. Chairman.

Chairman ISSA. I thank you both.

And we'll go to the ranking member.

And I appreciate your staff's assistance. Because although it's an issue that you know is never going away before this committee, it wasn't the main subject for today.

Mr. Cummings?

Mr. CUMMINGS. I want to go back to the 7.3 million people who paid their premiums and, I guess, around 700,000 who did not. There are all kinds of reasons, I guess, why people may not pay their premiums, and a lot of people in our society are still struggling with all kinds of things.

You talked about a reconciliation process. Can you talk about that for a moment?

Ms. TAVENNER. The way that it works is individuals—the 90-day grace period is set up to give individuals an opportunity to pay. At the same time, they start to receive tax credits. These tax credits are reconciled the next year on their income tax returns. If people have underpaid on their APTC, then they are likely to get a tax credit back. If they have overpaid, meaning if they've received a higher APTC than intended based on their income, they may owe the Federal Government back. And that's part of the partnership we have with IRS.

I don't think that the 700,000 is—in fact, I was very pleased to know that we have payment levels of 90 percent. This is a brand-new program. This has never been done before. I think by the end of 2014 and as we start to look back on 2014 we'll understand the circumstances. I expect, in some cases, they may have moved. They may have gotten married. They may have gotten insured. They may have lost their income and gone on Medicaid or into the uninsured ranks. We will only know that as we do a lookback. And we're careful not to look back too early.

Mr. CUMMINGS. And these are not necessarily people trying to game the system.

Ms. TAVENNER. No, sir.

Mr. CUMMINGS. I mean, I see folks every day that they're still being informed as to what the Affordable Care Act is all about——

Ms. TAVENNER. Right.

Mr. CUMMINGS [continuing]. And trying to make it—one singer says, "Working 9 to 5 just to say alive."

Ms. TAVENNER. That's right.

Mr. CUMMINGS. But in my district sometimes they're working two jobs just to stay alive. And so they're struggling trying to manage all this information, trying to do the best they can to take care of their families, and many of them going through some very difficult circumstances.

Ms. TAVENNER. That's right.

Mr. CUMMINGS. All right. Thank you very much.

Ms. TAVENNER. Thank you.

Chairman ISSA. The gentleman from Virginia, normally the first to arrive. We've just finished round three and the close. Would the gentleman have some questions?

Mr. CONNOLLY. I thank the chairman.

Chairman ISSA. The gentleman is recognized.

Mr. CONNOLLY. I was on the House Foreign Affairs Committee with the Secretary of State. Forgive me for being late.

Chairman ISSA. Well, I'm sure the questions there were provocative, so——

Mr. CONNOLLY. Yes.

Welcome, to the panel.

Mr. Wilshusen, would it be unreasonable of us to suggest that no company, no government, no individual should feel entirely secure and safe in the digital age?

Mr. WILSHUSEN. I would say if you're referring to use of online transactions on the Internet and the like, that there are certainly risks associated with that, just given the weakness in the nature of the Internet as well as the competency and prevalence of hackers who might wish to exploit those weaknesses.

Mr. CONNOLLY. The issue of securing public and private information systems, I assume, is not something unique to the Affordable Care Act implementation.

Mr. WILSHUSEN. No. It's an issue for any computer system operated by any agency, any organization. There is always a need to protect that information. And, certainly, as we mentioned earlier, you know, within the Federal Government, GAO has been identifying Federal information security as a governmentwide high-risk area since 1997.

Mr. CONNOLLY. Right. Since 1997.

Mr. WILSHUSEN. Yes, sir.

Mr. CONNOLLY. Two administrations ago.

Mr. WILSHUSEN. Probably.

Mr. CONNOLLY. Right.

Ms. Tavenner, hello, and welcome to our committee——

Ms. TAVENNER. Thank you, sir.

Mr. CONNOLLY [continuing]. I think. It may not have been entirely a felicitous beginning of this hearing, but I welcome you. And thank you for your work.

But let me ask you a question. One of the things we hear about the rollout of the Website in retrospect is that the coordination of IT management is disparate, not always focused, and perhaps was seen as a technical issue while, you know, CMS and the Department of Health and Human Services were focused on, sort of, the bigger picture and the reforms getting in place and the pieces finally fitting into the mosaic, and maybe this got short shrift. And it turned out to be the achilles heel. And the whole enterprise was at risk because of this failure, which was a technology issue.

In looking back on it, what lessons did you learn as a manager? And is there some validity to that critique, from your point of view?

Ms. TAVENNER. Yes, sir, I think there is some validity to that critique. And some of the lessons learned and changes that we've made early on in year 1 but definitely for year 2 is we needed a systems integrator. We needed someone to help with the coordination. We needed a clear point of accountability. We needed better communication. And you're right; there was probably more time spent on the nontechnical components, and we didn't realize the technology was as difficult as it was.

So those were lessons learned. I think we've put changes in place. We are very, very happy with the number who signed up.

We have—year 2 is going to be an equally hard year. It won't be perfection; it will be greatly improved. And we're looking forward to finding some more uninsured and helping folks get coverage.

Mr. CONNOLLY. Thank you. Thank you for that candid response.

Final question, Mr. Wilshusen: Are you familiar with the bill that the chairman and I have coauthored called FITAR, the Federal Information Technology Acquisition and Reform Act? A mouthful.

Mr. WILSHUSEN. A little bit, sir, but not completely.

Mr. CONNOLLY. Well, that bill tries to get at how the Federal Government manages IT procurement and acquisition. And it addresses, inter alia, how the Federal Government is managed. And I think it's based on the conclusion that it's not well-managed and it's very inefficient and there are too many people with the titles "CIO." And what could go wrong with that? The estimate is $20 billion of the $82 billion that we spend on IT acquisition every year is at least inefficiently used, sometimes downright, unfortunately, wasted.

Is it GAO's position that we do need some IT updates and reforms to, kind of, update on Clinger-Cohen, which was almost 20 years ago? And in technology 20 years is light years.

Mr. WILSHUSEN. Well, sir, that's actually outside my particular area. I focus on information security and privacy issues. We have others that——

Mr. CONNOLLY. But aren't——

Mr. WILSHUSEN. But I can get that answer to you.

Mr. CONNOLLY. That would be fine. But isn't information security related to how well we're managing our IT assets?

Mr. WILSHUSEN. Oh, certainly. And, certainly, there is need for improvements in how IT is secured within the Federal Government, and that's an implementation issue. And we're also on record that FISMA, which is the Federal Information Security Management Act that governs information security across the government, could also be updated and modified.

Mr. CONNOLLY. Well, again, I believe this committee and, again, the chairman, ranking member, and I have been involved in that, as well. But the House has certainly tried to address that, and we've found bipartisan common ground on these issues. I urge you to look at the bill and see how it applies to your particular area.

Mr. WILSHUSEN. I will.

Mr. CONNOLLY. I thank you.

And, Mr. Chairman, thank you for allowing a shameless plug for our legislation one more time.

Chairman ISSA. Well, in closing, it's not shameless, but it's a good plug.

You know, I'll close—because, Ms. Tavenner, we'll probably try to do everything without having you back, and I think we're on the right track. This is a committee that does legislation on a very bipartisan basis, in most cases, and it doesn't get reported. And then we have oversight, and perhaps it's not as bipartisan, and it often does get reported.

I do think today's hearing was worthwhile. I believe that, hopefully, Mr. Cummings and I both expect that there will be a little

bit more certainty as to the security that will come out of the Website.

CMS is critical to the American people. Your role has been expanded, perhaps, more with the Affordable Care Act than any item before.

And Mr. Cummings often talks about the Federal work force and certainly about the good work that's being done. I want to close by saying that just because we give you a hard time over item after item, just because a number of Members asked about, "What about these billions of dollars that were given to States for their failed Websites?", doesn't mean we think it's easy. Just the opposite. We know it's hard. We want government to oversee itself to the greatest extent possible. And it's the reason that we do appreciate and support the GAO, we do appreciate and support the inspectors general, and that we try to be, if you will, their supporters in order to get the kinds of certainty and, when necessary, reforms that are necessary.

So I want to thank you for being here today. I think this was an informative hearing.

And, with that—Mr. Cummings gives me a "yes"—we stand adjourned.

[Whereupon, at 1:30 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Questions for
The Honorable Marilyn Tavenner
Centers for Medicare and Medicaid Services

Representative James Lankford

September 18, 2014 Hearing:
"Examining ObamaCare's Failures in Security, Accountability and Transparency"

1. **I have serious concerns about the way in which the Centers for Medicare and Medicaid Services (CMS) and the Office of Medicare Hearings and Appeals (OMHA) are handling provider appeals generated by Recovery Audit Contractors (RACs). A provider appealing an improper payment determination is entitled to, under law, receive an independent decision from an independent decision-maker – in this case, an Administrative Law Judge (ALJ) at OMHA – within 90 days of filing a request for an ALJ hearing. It has been well-documented by the OIG, GAO, and several Congressional Committee hearings that providers are not able to have their cases heard and determined before the 90-day limit. On its website, OMHA admits "The average processing time for appeals decided in fiscal year 2014 is 398.1 days."**

   Nonetheless, CMS collects recoupments from providers still waiting to have their claim heard. Small business, like DME providers, suffer from cash flow challenges after CMS recoups and holds the provider's payments for several years before they get to the ALJs, and, as a result, many good providers have gone out-of-business.

   In light of these problems, is there any reason we should not move the date that a provider has to refund money because of a RAC audit to the date after which the appeal is completed—if not on a permanent basis, then at least until ALJ appeals can be heard in 90 days, as required by the law?

Answer: CMS does not have statutory authority to modify its debt collection regulations in the manner you suggest. Section 1893(f)(2)(A) of the Social Security Act limits CMS's recoupment of Medicare overpayments only during the first two levels of appeal and does not authorize suspension of debt collection during subsequent appeals. In the absence of express statutory authority to further delay recoupment, CMS has no statutory authority to delay recoupment after the second level of appeal. However, CMS is authorized to grant a provider or supplier an extended repayment schedule of up to 60 months if repayment of an overpayment constitutes a hardship (Social Security Act § 1893(f)(1); 42 CFR 401.607). Additionally, if the provider or supplier ultimately is successful in its ALJ appeal, CMS is required to return all monies collected on the debt. If CMS collected any portion of the debt through involuntary recoupment and a favorable appeal decision was obtained by the provider from the ALJ or subsequent level of appeal, the provider will be paid interest on the principal amount recouped.

2. **CMS recently announced that it would offer a one-time administrative settlement to any hospital willing to withdraw pending Medicare claims appeals in exchange for a "timely partial payment" of 68% of the net allowable amount. According to the agency, these settlements will serve to reduce backlog of appeals. Please address the following:**
    a. **Did CMS seek comment through the rulemaking process, or seek provider and stakeholder input to arrive at its decision to offer a settlement program? Please explain how CMS came to the conclusion that 68% is a proper settlement amount to offer to providers.**

Answer: The Department of Health and Human Services (HHS) established a Departmental interagency workgroup in 2013 to address the Medicare appeals backlog. The workgroup included leaders from the three agencies involved in the Medicare appeals process: CMS, the Office of Medicare Hearings and Appeals (OMHA), and the Department Appeals Board. HHS conducted a thorough review of the appeals process and developed a series of administrative initiatives that both OMHA and CMS are implementing to reduce the current backlog of pending appeals and the number of appeals that reach OMHA. One of the initiatives we presented as part of the workgroup's strategy was the pursuit of settlements.

HHS determined 68 percent was an appropriate settlement offer based on our knowledge of the types of claims at issue and the associated value of the services performed. MedPAC has found that the comparable average inpatient reimbursement can vary compared to the average outpatient reimbursement. Therefore, in determining the appropriate settlement offer, we examined the denied amounts, the tendency of hospitals to appeal decisions, and the vulnerability that hospitals and CMS faced throughout the appeals process. We also considered other factors such as services that may have been provided during the inpatient stay for which no Part B reimbursement is allowed, and other savings measures that both the Government and hospitals may achieve.

    b. **Part B providers also have a multitude of appeals in this backlog and as small businesses, they do not have the resources to ride out the severe disruption to their cash flow that this appeals baeklog has been creating. Does the agency have plans to extend this settlement offer to Part B providers?**

Answer: At this time, CMS does not have plans to extend settlement offers to Part B providers. However, CMS and OMHA are engaging in a series of administrative initiatives targeted at reducing the appeals backlog and processing appeals in a timely fashion.

3. **In its September 2013 report, the HHS OIG found that "In FYs 2010 and 2011, RACs identified half of all claims they reviewed as having resulted in improper payments totaling $1.3 billion. CMS took corrective actions to address the majority of vulnerabilities it identified in FYs 2010 and 2011; however, it did not evaluate the effectiveness of these actions. As a result, high amounts of improper payments may continue. Additionally, CMS did not take action to address the six referrals of potential fraud that it received from RACs." Please comment on the following:**

a. What corrective actions has CMS taken to date to reduce the rate at which improper payments are made?

Answer: CMS continues to improve its process of developing corrective actions to prevent improper payments. The development of corrective actions is an agency-wide collaborative effort.

CMS has established a process to take corrective actions for program vulnerabilities based on Recovery Auditor reviews. Information related to Corrective Actions from the Recovery Auditors reviews can be found in the Report to Congress: Recovery Auditing in Medicare and Medicaid for FY 2012.[1] CMS reviewed the six RAC referrals of potential fraud referenced in the HHS OIG report and took appropriate action, including referring providers to the Zone Program Integrity Contractor (ZPIC), Medicare Administrative Contractor (MAC) and OIG. One of the referrals resulted in a revocation from Medicare.[2]

b. Can CMS demonstrate the rate at which improper payments are made has decreased? Please cite specific statistics rather than dollar amounts.

Answer: The factors contributing to improper payments are complex and vary from year to year. CMS acknowledges that it takes time for providers to change their documentation behavior to comply with new policies, and as such, it is not unusual to see slight increases in improper payment rates following the implementation of new policies to strengthen the integrity of the Medicare program. In addition, due to the timeframe in which the improper payment measurement is conducted, the impacts due to current corrective actions are not measurable until a future point in time. For example, a major contributing factor to the Fiscal Year (FY) 2013 Medicare FFS improper payment rate was the implementation of new home health documentation requirements that became effective in 2011. CMS has consequently proposed modifications to these documentation requirements, which will become effective in January 2015. The impact of these policy changes will not be fully reflected in the improper payment rate until the FY 2017 measurement.

4. Does CMS have the statutory authority to allow providers with a proven track record of proper payments – demonstrated by either zero improper payments over a period of time, or by a high rate of winning appeals – to be audited with less frequency?

Answer: In February 2014, CMS announced a number of changes to the Recovery Audit

[1] See page 21 of http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/Report-To-Congress-Recovery-Auditing-in-Medicare-and-Medicaid-for-Fiscal-Year-2012_013114.pdf

[2] See page 25 of http://oig.hhs.gov/oei/reports/oei-04-11-00680.pdf.

Program that will take effect with the new contract awards as a result of stakeholder feedback.[3] CMS believes that improvements to the RAC program will result in a more effective and efficient program, including improved accuracy, less provider burden, and more program transparency. One of the improvements is that Additional Documentation Requests (ADR) limits will be adjusted in accordance with a provider's denial rate. Providers with low denial rates will have lower ADR limits while providers with high denial rates will have higher ADR limits.

5. Does CMS have the authority to deny payment to an audit contractor when it identifies payments that are later ruled proper through the appeals process?

Answer: CMS has many safeguards in place to ensure Recovery Auditors are not financially incentivized to inappropriately deny claims. Recovery Auditors are paid on a contingency fee basis; the amount of the contingency fee is a percentage of the improper payment recovered from, or reimbursed to providers. If the claim is overturned at any level of appeal, the Recovery Auditor does not receive a contingency fee payment.

6. Recently, CMS announced that it will begin enforcing income and immigration status verification under the Affordable Care Act. The announcement reads, in part:

> **"CMS is also providing an update on individuals with citizenship and immigration data matching issues. In August, we sent letters to about 310,000 Federal Marketplace consumers who had not submitted any outstanding citizenship or immigration documents after numerous requests. We've made progress in resolving these cases. We received hundreds of thousands of documents in response to the September 5 deadline, resulting in a decrease from 966,000 as of the end of May to 115,000 as of September 14. To date, 115,000 individuals with citizenship and immigration data matching issues have not responded to our numerous contacts and will be receiving notices saying their last day of Federal Marketplace coverage is September 30, 2014. Those who submit information that confirms their eligibility after the deadline may be eligible for a special enrollment period to enroll in coverage." Please comment on the following:**
>
> **a. Please explain what constitutes a "data matching issue."**
> **b. Were people with "data matching issues" able to obtain benefits?**
> **c. If it turns out that people with "data matching issues" obtained and used their benefits, will CMS ask recoup those costs?**

Answer: After consumers complete Marketplace applications, the Marketplace verifies the information consumers attest to against Federal, state, and third-party data sources. Consumers experience regular changes in income and other life circumstances, including changes in

[3] http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/RAC-Program-Improvements.pdf

employment and marital status. As a result, consumers may have more up to date information about their current situation than what is reflected in the data sources used by the Marketplace. Mismatches between these data sources and information consumers attest to in their applications result in data matching issues. As required by statute, consumers with data-matching issues are asked to submit additional documentation to verify the information they attested to on their applications. That we are verifying data does not necessarily mean that a consumer has provided false information or that he or she is ineligible for financial assistance such as the advance premium tax credits (APTCs) that reduce his or her monthly premium costs or cost-sharing reductions that can lower out-of-pocket costs. For example, even a trusted electronic data source may not contain the most updated information about a consumer's individual circumstance, like a recent change in income. This step simply means that the information on an application does not match the information in trusted data sources and therefore needs additional verification.

The law contemplated data-matching issues and requires the Marketplace to provide benefits to applicants who are otherwise eligible for a period of time to allow the applicants to submit the required documentation; this is known as the inconsistency period. The statutorily-required approach of providing benefits during the inconsistency period balances consumer access to health coverage with controls for program integrity.

Consumers must attest to all the information in their applications under penalty of perjury and acknowledge that any over or underpayment of tax credits would be reconciled on their annual tax filings. At the end of the tax year, every tax filer on whose behalf APTCs were paid, including those who had data matching issues, must file a Federal income tax return to reconcile APTC paid to the QHP issuer on the tax filer's behalf and the actual amount of the premium tax credit that the tax filer is entitled to claim for the enrollee—a process enrollees acknowledged when they applied for financial assistance.

Representative Jason Chaffetz

1. **Will CMS spend additional federal funds to assist individual state exchanges reboot or fix their exchange systems, such as Maryland and Massachusetts? If so, please list the state, the amount for each state, and the source of funding.**

Answer: States may request funding for a variety of Exchange implementation functions. CMS carefully reviews each application. States do not receive award funds upfront, but gradually draw down from an account reserved for approved expenses. A full list of grants provided to all states is available on the CMS website.[4]

2. **Will CMS spend federal funds to transition Oregon and Nevada into the federal exchange? If so, what amount of federal dollars will CMS spend on each state, and what is the source of funds for such a transition?**

3. **Has CMS conducted any analysis to determine the costs and benefits of transitioning state exchanges in Oregon and Nevada to the federal exchange? Please provide the analysis.**

    a. **Did CMS consider the cost of transitioning the reported 100,000 enrollees in the Oregon Exchange onto the federal exchange? What is the cost to taxpayers for this transition?**

Answer to #2 and #3: For 2015, Oregon and Nevada will use the Federally-facilitated Marketplace (FFM) eligibility and enrollment systems while continuing to carry out other responsibilities of State-based Marketplaces (SBMs), including consumer outreach and plan management. The FFM is a scalable platform, meaning that the marginal cost to provide eligibility and enrollment functionality for two additional states is minimal and lower than CMS' initial estimates.

CMS conducted a cost estimate earlier this year, which indicated that the initial costs for IT and systems changes to add the first additional State would total approximately $21 million, and that there would be a $2 million to $4 million incremental cost for each additional state. CMS obligated $7.3 million in FY 2014 to complete the IT and system changes related to the transition for Oregon and Nevada, which is less than previously estimated and no additional expenses related to IT and systems changes for the transition are anticipated. Neither Oregon nor Nevada has requested additional grant funding in order to transition to the FFM eligibility and enrollment platform.

4. **Can any state transition back to the federal exchange? What criteria does CMS use to assess whether or not a state will be permitted to transition to the federal exchange?**

[4] http://www.cms.gov/CCIIO/Resources/Marketplace-Grants/index.html

Answer: Yes; the November 30, 2012 Funding Opportunity Announcement (FOA) clarifies that §1311(a) grant funds allow states the flexibility to transition between Marketplace models over time.

Chairman Darrell Issa

1. **Has CMS conducted audits of state use of federal grants in building their Exchanges and other ACA related IT systems? If so:**

    a. **Which states has CMS audited? When were these audits conducted? Please describe the scope of the audits.**

    b. **Which states does CMS intend to audit? When will these audits be conducted? Please describe the scope of these audits.**

Answer: Audits are an important part of CMS' financial oversight process. Each state grantee is required to prepare an A-133 Audit within nine months of the close of the state's fiscal year or within 30 days of the audit's performance, whichever is sooner, when it receives a Federal grant equal to or in excess of $500,000 in a single fiscal year. The audit is a third-party objective review of internal controls and assesses the adequacy of accounting and financial reporting systems. CMS regularly monitors A-133 Audit findings for Establishment grantees and oversees the development and execution of corrective action plans (CAP) to alleviate risk. These audits are performed, as required, by the state grantees that meet the above criteria. CMS reviews any findings from such audits and ensures that a state, as required, develops and implements corrective action plans. These audits are only one aspect of the oversight of the Exchange Program.

2. **How much has CMS spent on grants to states to establish Health Insurance exchanges, to date?**

Answer: As of September 2014, the total amount of Establishment grants awarded to 27 states and the District of Columbia is approximately $5.1 billion.

3. **Why did CMS decide to stop releasing monthly enrollment reports in May 2014, and who made the decision to stop releasing the reports?**

    Answer: For the 2014 benefit year, CMS followed the process we did for Medicare Part D, releasing monthly enrollment reports during the first open enrollment period.

4. **On what date will CMS publish information on 2015 premiums for qualified health plans sold on the federal exchange? What will this information contain?**

Answer: CMS is in the process of reviewing plan and rates submissions for QHPs to be offered

on the FFM. We plan to post 2015 rates and plans in the FFM at one time, once this review process is completed, just as we did for the 2014 plan year. Data will be included on final 2015 rates in the individual and small group markets for plans offered inside and outside of the Marketplace for all states and the District of Columbia. This information will be available prior to the start of open enrollment on November 15th.

5. **On what date will CMS publish information on the number of individuals enrolled in qualified health plans in the exchange?**

Answer: HHS released regular enrollment reports throughout the first open enrollment, and plans to provide similar information during the second open enrollment period.

6. **What actions has CMS taken to recoup the over $300 million taxpayer dollars spent on the Oregon exchange?**

Answer: State grantees are responsible for administering grant funding, and state procurement laws govern in disputes between states and their chosen contractors. States have the authority to try to recoup funds from any vendor/contractor when work is not satisfactory.

7. **Given the poor performance of several state exchanges' during the last open enrollment period, what steps has CMS taken to ensure that there is not a repeat of similar functionality problems?**

Answer: For the States that experienced serious issues during open enrollment last year, CMS and the states developed mutually agreed-upon corrective action plans, and sets of CMS-developed milestones for assessing each State's readiness and progress for open enrollment this year.

8. **CMS's conflict of interest provisions in the RFP for systems integration work notes that a conflict of interest exists when the systems integrator is also helping to design, develop or maintain information systems that support the health insurance marketplace, or when the systems integrator or an affiliate is a qualified health plan. Given these provisions, please explain CMS's conflict of interest analysis with respect to current contractor, QSSI/Optum, including CMS Principal Deputy Administrator Andrew Slavitt's employment at Optum until June 2014.**

Answer; QSSI is owned by Optum, which is an operating division of UnitedHealth Group. CMS follows Federal contracting guidelines, which require us to evaluate all contracts to ensure that they do not have any conflicts of interest before making an award. Additionally, because conflicts of interest may arise at any point in time, the base contract upon which CMS awarded the task order to Optum/QSSI contains an Organizational Conflict of Interest (OCI) clause that requires the contractor to notify CMS when they become aware of situation that could present a conflict.

Regarding the concerns about the appointment of CMS Principal Deputy Administrator Andrew Slavitt, he has received a memo from the Department of Health and Human Services Associate General Counsel for Ethics, our Designated Agency Ethics Official, that details restrictions and conditions on his participation in certain matters involving QSSI/ Optum. This memo is publicly available through the United States Office of Government Ethics.[5]

9. According to press reports, the federal exchange is not recalculating the subsidy amounts for enrollees who auto-renew for 2015 plan years. This raises concerns the exchange will not provide accurate subsidy amounts to those who do not reapply for coverage. Why did CMS choose not to recalculate subsidies for enrollees who opt to auto-renew their existing coverage?

Answer: As part of the renewal process in the FFM, generally, if consumers do nothing, they will be auto-enrolled in the same plan with the same advance payment of the premium tax credit and other financial assistance, if applicable, as the 2014 plan year. Consumers are encouraged to return to the Marketplace to make sure they are getting all the financial assistance they qualify for, and to shop for the plan that best suits their needs. Consumers whose 2013 Federal income tax returns indicate that they had very high household incomes, or who did not give the Marketplace permission to check updated tax information for annual eligibility redetermination purposes, will be auto-enrolled without financial assistance if they do not return to HealthCare.gov. This process will help provide continuity of coverage and safeguard taxpayer dollars. If a consumer chooses to return to the Marketplace to review their plan options and update their income or any other information, this will trigger an eligibility determination, just like for new consumers. Their information will be verified using 2013 tax return information and other data through the Data Services Hub, and an updated APTC will be calculated. Consumers must return to the Marketplace to report life changes throughout the year, including changes in income.

a. Given that some overpayments will not be recoverable due to statutory restrictions, what steps is CMS taking to minimize improper payment of exchange subsidies?

Answer: Consumers must attest to all the information in their applications under penalty of perjury and acknowledge that any over or underpayment of advance premium tax credits would be reconciled on their annual tax filings. After a consumer submits an application, the information they submit is checked against Federal, state and third-party data sources through the Data Services Hub electronically and almost instantaneously. Mismatches between these data sources and information consumers attest to in their application result in a data matching issue. In addition, consumers are required to notify the Marketplace of any changes to household income, family size or other factors that would affect their eligibility. At the end of the tax year,

[5] http://oge.gov/DisplayTemplates/SearchResults.aspx?query=slavitt

every tax filer on whose behalf Advanced Premium Tax Credits (APTCs) were paid must file a Federal income tax return to reconcile APTC paid to the QHP issuer on the tax filer's behalf and the actual amount of the premium tax credit that the tax filer was is entitled to claim for the enrollee—a process enrollees acknowledged when they applied for financial support.

10. In response to a question from Mr. Mica concerning your request to CMS official Julie Bataille that an email you sent her be deleted, you testified that "I think that I asked that she delete this email because it involved sensitive information regarding the President's schedule, and I think that's actually the area that's redacted."

a. Question: Please provide a citation of the federal law, regulation, or policy, whether issued by HHS, CMS, or by the White House Office of Management and Budget, which supports the rationale that a sensitive email concerning the President's schedule can be deleted.

Answer: In this case, I did not want this sensitive information distributed throughout the agency. The email was not deleted and was retained.

11. In January 2014, CMS replaced CGI Federal, the previous contractor, with Accenture with a no-bid, "letter" contract. At the time, the accompanying justification for other than full and open competition stated that this contract was estimated to be worth $91.1 million and that this "one-year contract action is an interim, transitory solution to meet the Agency's immediate and urgent need."[6] A latest search in USASpending.gov shows the following awards to Accenture - all cost-reimbursement contracts, categorized as "Not Competed," based on "Urgency"[7]:

1/11/2014	**$45M**
2/21/2014	**$15M**
4/25/2014	**$45M**
5/13/2014	**$7M**
5/16/2014	**$13.6M**
5/23/2014	**$18.4M**
6/5/2014	**$31.3M**
6/26/2014	**$15M**
Total:	**$190.4M**

[6] CENTERS FOR MEDICARE AND MEDICAID SERVICES, JUSTIFICATION FOR OTHER THAN FULL AND OPEN COMPETITION (2014), available at: https://www.fbo.gov/utils/view?id=0f3df4e32f0c17dbf3dbe289eb99dbb9.

[7] See USA Spending, USASpending.gov (Last visited Sep. 30, 2014), *available* at: http://www.usaspending.gov/search?form_fields=%7B%22recipient_name%22%3A%22accenture%22%2C%22spending_cat%22%3A%5B%22c%22%5D%2C%22fyear%22%3A%5B%222014%22%5D%2C%22agency%22%3A%5B%227530%22%5D%2C%22dept_ignored%22%3A%5B%227500%22%5D%7D

a. Please provide the list of all sole-source contract actions (including modifications) and obligation value to Accenture since January 2014.

Answer: On January 11, 2014, CMS awarded a sole source contract to Accenture Federal Services to replace CGI Federal as the FFM contractor. CMS executed a letter contract which authorized the contractor to begin work immediately but required a negotiation to finalize the terms and conditions, including the estimated cost and fee. The letter contract obligated $45 million in order for Accenture to have funding to get them started. As of September 2014, CMS has issued nine modifications which have finalized the amount for the initial contract, and incorporated contract changes that have added additional requirements and functionality. Following is a summary of each contract action with Accenture.

1/11/2014	$45 million - Letter Contract authorizing Accenture Federal Services to immediately begin developing the FFM financial management service areas and other associated services described in the Statement of Work.
2/21/2014	Modification 1 - $15 million - Change Order to provide specific direction regarding the delivery of the SHOP portion of the Marketplace website.
4/25/2014	Modification 2 - $45 million - Definitization of the letter contract for the development and maintenance of the FFM website application and to add incremental funding. Definitization is a contracting term meaning the agreement on, or determination of, the contract terms and price.
5/13/2014	Modification 3 - $7 million - Change Order issued to add Regional Tech Support.
5/16/2014	Modification 4 - $13.6 million - Add Value Added Services (CMS obligated a total cost plus award fee of $13.6 million for the value-added services), to establish an optional contract line item for Transition Out services and to add a deliverables table. The transition out services is optional only and would cover the effort required to transition the work to a new contractor if necessary.
5/23/2014	Modification 5 - $18.4 million - Definitization of the change order issued as Modification 1 for the Development and Maintenance of the Federally-facilitated Small Business Health Options Program (FF-SHOP Marketplace). This modification established a total cost plus award fee of $33.4 million ($15 million plus $18.4 million) for the SHOP work.
6/5/2014	Modification 6 - $31.3 million - Add the remaining portion of incremental funding to fully fund the development and maintenance of the FFM website application. Modification 2 used a funding mechanism called incremental funding, in which one obligates a portion of the funding with the intention of obligating remaining portions later. This modification obligated the remaining portion.
6/26/2014	Modification 7 - $15 million - Change Order issued to add additional development needs. Includes additional support for Production, Operations, Environments, and FFM VDC Migration.
7/31/2014	Modification 8 - $0 - Incorporated the Organizational Conflict of Interest

Clause into the contract and revised the Statement of Work.

b. For each discrete contract, please provide a list of top 10 highest paid contractor/subcontractor individuals under the Accenture cost-reimbursement contract, including job title, description of duties, hourly rates and indirect rates.

Answer: The Accenture contract includes a clause that requires the contractor to provide, as part of its annual registration requirement in the System for Award Management database, the names and total compensation of each of the most highly compensated executives. The clause does not require every subcontractor to report this information. This information is available at usaspending.gov.

c. Was Accenture asked to redo any work delivered by CGI? If so how much was spent?

Answer: CMS ended its cost plus fixed fee contract with CGI, and awarded a new cost plus award fee contract with Accenture. CMS awarded this type of contract because it better controls cost and rewards performance. Additionally, CMS and Accenture finalized a definitive one-year agreement with well-defined requirements within the Scope of Work.

Pursuant to the Statement of Work, Accenture was to provide design, development, testing, implementation support, software licensing, application defect fixes, security process and protocol integration, and technical services to support the FFM.

d. The Federal Acquisition Regulation (FAR) states that the total period of performance of a contract awarded using such sole-source justification may not exceed the time necessary to meet the unusual and compelling requirements. Moreover, the selection of cost-reimbursement contract type by CMS means the contractor bears no cost-risks in its contract performance, which means the taxpayers do. What is the current timeline for <u>competitively</u> awarding Accenture's successor contract after the current sole-source contract expires in January 2015?

Answer: A competitive procurement is already underway for the follow-on contract for the development and maintenance support for the FFM. CMS posted a solicitation on Federal Business Opportunities (FBO) on July 16, 2014 requesting all responsible and interested contractors submit proposals for the FFM successor contract. CMS has posted a notice of our intent to negotiate a sole source contract action with Accenture to extend their performance period on the FFM contract through July 31, 2015. CMS is currently evaluating proposals submitted in response to the solicitation and is working to award the new contract as expeditiously as possible.

e. What steps will CMS take to ensure that the successor contract is competitively and transparently awarded?

Answer: CMS issued a solicitation in FBO for the re-competition on July 16, 2014. CMS used the procedures for full and open competition described under FAR Part 15 for this procurement.

f. How will CMS ensure that the solicitation requirements for new competitive contracts are designed to be fair to all commercial vendors and do not favor the incumbent?

Answer: CMS used the fullest and most competitive procedure available to solicit proposals for this effort. CMS encouraged all responsible sources to submit proposals. Prior to release of the solicitation, CMS ensured that the requirements and evaluation criteria were prepared in a manner that promoted and provided for full and open competition.

g. What will CMS do if a new competitively awarded contract is not in place in time for a handoff from Accenture?

Answer: CMS has posted a notice of our intent to negotiate a sole source contract action with Accenture to extend their performance period on the FFM contract through July 31, 2015.

Representative Tony Cardenas

1. **CMS' Medicare "Two Midnights" Hospital Admissions policy's arbitrary time-based admission criteria did not achieve the clarity it intended, and has instead caused more confusion among the hospital and provider communities and Medicare beneficiaries. It has encountered widespread bipartisan criticism in both chambers of Congress - as witnessed through Congressional hearings and comment letters - and is opposed by many key stakeholders in our health care delivery system. Can you explain what the justification is for keeping the rule in place?**

Answer: Because of statutory requirements, the Medicare payment rates for inpatient and outpatient hospital stays differ. Services furnished to hospital inpatients are generally billed under the Hospital Inpatient Prospective Payment System (IPPS), while services furnished to outpatients are generally billed under the Hospital Outpaticnt Prospective Payment System. Therefore, when a Medicare beneficiary arrives at a hospital in need of medical or surgical care, the physician or other qualified practitioner must decide whether to admit the beneficiary for inpatient care or treat him or her as an outpatient. Previous CMS guidance provided for a 24-hour benchmark, instructing physicians that, in general, beneficiaries who need hospital care for less than 24 hours should be treated as outpatients, while those requiring hospital care for more than 24 hours may be admitted as hospital inpatients. Thc two-midnight policy, as finalized in the FY 2014 IPPS Final Rule, modified the previous guidance to specify that the relcvant 24 hours are those encompassed by two midnights (78 FR 50945).

CMS solicited comments on alternative payment approaches for short inpatient stays and is working closely with stakeholders to explore the possibility of additional exceptions to the two midnight rule. CMS looks forward to continuing to work with stakeholders and the Congress to further improve payment policy around the complex issues surrounding short hospital stays.

2. **Since CMS has acknowledged the shortcomings of the "Two Midnights" Policy, can you elaborate on alternative plans your agency has for addressing the confusion and inconsistent application of the Policy in the determination of inpatient or outpatient hospital status for Medicare beneficiaries? How will CMS fix this problem, and what quality benchmarking standards will be used to track its success moving forward? Can you assure the stakcholder community that medical necessity reviews will be a critical component of your alternate approach?**

Answer: To help hospitals understand and fully comply with thc two-midnight policy, CMS implemented a probe and educate strategy whereby Medicare Administrative Contractors (MACs) conducted pre-payment reviews on a sample of short-stay inpatient claims from each hospital, for dates of admission between October 1, 2013, and March 31, 2014, to determine compliance with the two-midnight rule. Claims for inpatient admissions that were determined not reasonable and necessary pursuant to the two- midnight rule were denied, and the MACs provided further education regarding the rule.

As part of this strategy, we also prohibited the Recovery Auditors from conducting any post-payment patient status reviews of claims with dates of admission between October 1, 2013 and March 31, 2014. CMS used this opportunity to engage in a dialogue with stakeholders on the two-midnight rule. As we began hearing from stakeholders that more time was needed to understand the policy, we extended the probe and educate strategy through September 30, 2014. The Congress further extended the probe and educate strategy and the prohibition on post-payment patient status review of claims by Recovery Auditors through March 31, 2015. We believe these extensions will allow hospitals and other stakeholders time to fully benefit from the probe and educate strategy.

3. The new "Two Midnight" threshold injects a time based admission criteria into a doctor's decision about whether to admit a patient - isn't this counter to the entire personalized approach to caring for beneficiaries?

Answer: Longstanding guidance in the Medicare Benefit Policy Manual has provided a 24-hour benchmark to be used in making inpatient admission decisions as well as the clinical judgment of the physician. The Manual (Section 10, Chapter 1) states, "Physicians should use a 24-hour period as a benchmark, i.e., they should order admission for patients who are expected to need hospital care for 24 hours or more, and treat other patients on an outpatient basis. However, the decision to admit a patient is a complex medical judgment which can be made only after the physician has considered a number of factors, including the patient's medical history and current medical needs, the types of facilities available to inpatients and to outpatients, the hospital's by-laws and admissions policies, and the relative appropriateness of treatment in each setting."

The two-midnight rule, as finalized in the FY 2014 IPPS Final Rule, modified the previous guidance to specify that the relevant 24 hours are those encompassed by two midnights (78 FR 50945). However, unlike previous guidance which required ordering practitioners to prospectively support complex medical decisions regarding the acuity of hospital care, under the new policy, all medically necessary hospital services may be considered when supporting an expectation of a stay spanning two midnights, including services provided before an inpatient order is effectuated. Moreover, we continue to expect that physicians will make the decision to keep a beneficiary in the hospital when clinically warranted and will order all appropriate treatments and care in the appropriate location based on the beneficiary's individual medical need.

Martin, Emily

From: Martin, Emily
Sent: Tuesday, September 16, 2014 10:54 AM
To: 'Sinha, Sushant'
Cc: 'Mehta, Coleman'; Goto, Meinan
Subject: RE: Oversight Committee Request

Sonny,

Any update on our briefing request from last Monday?

Thanks,
Emily

From: Martin, Emily
Sent: Monday, September 15, 2014 2:42 PM
To: 'Sinha, Sushant'
Cc: 'Mehta, Coleman'; Goto, Meinan
Subject: RE: Oversight Committee Request

Sonny,

Any update on our briefing request from last Monday?

Thanks,
Emily

From: Martin, Emily
Sent: Friday, September 12, 2014 3:23 PM
To: 'Sinha, Sushant'
Cc: Mehta, Coleman; Goto, Meinan
Subject: RE: Oversight Committee Request

Sonny,

Will we be able to set up the call today? We reached out Monday and would like a briefing time arranged as soon as possible.

Thanks,
Emily

From: Sinha, Sushant [mailto:SKS@hq.dhs.gov]
Sent: Wednesday, September 10, 2014 6:09 PM
To: Martin, Emily
Cc: Mehta, Coleman; Goto, Meinan
Subject: Re: Oversight Committee Request

Hi Emily,

Sorry today was crushingly busy.

We are targeting friday for a phone call.

Is there a time then that can work?

Lmk.

From: Martin, Emily [mailto:Emily.Martin@mail.house.gov]
Sent: Wednesday, September 10, 2014 06:04 PM
To: Sinha, Sushant
Cc: Mehta, Coleman; Goto, Meinan <Meinan.Goto@mail.house.gov>
Subject: Re: Oversight Committee Request

Sonny,

Any update on briefing times?

Thanks,
Emily

From: Martin, Emily
Sent: Tuesday, September 09, 2014 03:30 PM
To: 'Sinha, Sushant' <SKS@hq.dhs.gov>
Cc: Mehta, Coleman <Coleman.Mehta@HQ.DHS.GOV>
Subject: RE: Oversight Committee Request

Sonny,

That sounds great. I appreciate your help – please let us know what times will work.

We can also make ourselves available Thursday morning, if that makes scheduling easier.

Thanks,
Emily

From: Sinha, Sushant [mailto:SKS@hq.dhs.gov]
Sent: Tuesday, September 09, 2014 3:29 PM
To: Martin, Emily
Cc: Mehta, Coleman
Subject: Re: Oversight Committee Request

Hi Emily, when we discuss the status of other agencies cyber status, we do so with the agency present.

I am running this back with hhs to see if we can all jointly get on the phone, and am seeing if tomorrow can work.

I'm hoping to get a response on this soon.

Is this acceptable?

Let me know if/when you can.

Best,
Sonny

202-578-5595

From: Martin, Emily [mailto:Emily.Martin@mail.house.gov]
Sent: Tuesday, September 09, 2014 03:23 PM
To: Sinha, Sushant
Subject: FW: Oversight Committee Request

Sushant,

I wanted to follow up on this request. Are there any times tomorrow that we can set up a call?

Thank you!
Emily

From: Mehta, Coleman [mailto:Coleman.Mehta@HQ.DHS.GOV]
Sent: Monday, September 08, 2014 6:37 PM
To: Martin, Emily
Cc: Goto, Meinan; Tallmer, Matt; Sinha, Sushant
Subject: Re: Oversight Committee Request

Emily, thanks for your email. I've added Sonny here who can help coordinate a call.

Vr, Coleman

Director, Legislative Affairs
DHS National Protection and Programs Directorate
202-580-9654

From: Martin, Emily [mailto:Emily.Martin@mail.house.gov]
Sent: Monday, September 08, 2014 05:55 PM
To: Mehta, Coleman
Cc: Goto, Meinan <Meinan.Goto@mail.house.gov>; Tallmer, Matt <Matt.Tallmer@mail.house.gov>
Subject: Oversight Committee Request

Mr. Mehta,

Lauren Aronson from CMS gave me your information as a contact regarding the Healthcare.gov hack. Our staff has some questions about the incident, and would like to set up a short call to discuss your role in the investigation and what you have learned about the hack.

Would you be available for a call tomorrow or Wednesday?

Thank you,
Emily

Emily Martin
Counsel
Committee on Oversight & Government Reform
Darrell E. Issa, Chairman
202.226.9457

For the Record- Data Breach Prosecutions & Investigations

The enclosed media reports and public announcements represent a small sample of investigations into and prosecutions for exposing consumer personal data as conducted by multiple state attorneys general as well as the Department of Health and Human Services itself. Key examples of the enclosed area summarized below

State Attorneys General— 14 Examples Enclosed

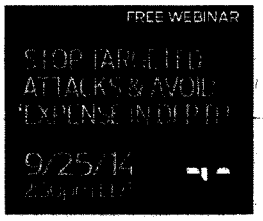
- Massachusetts Attorney General Martha Coakley won a case against a Bay state restaurant group after it had been hacked and malware uploaded to its servers. The group paid a $110,000 fine and entered into a security upgrade program.
- Vermont Attorney General William Sorrell settled with HealthNet, Inc and Health Net of the Northeast, Inc over allegations that the company waited too long to notify consumers of a potential for exposed personal information after a hard drive was lost.
- CVS settles with Maryland AG Doug Gansler in August 2013 for $250,000 for substandard disposal procedures for customer information.
- Anthem Blue Cross settles with California Attorney General Kamala Harris for $150,000 and technical upgrades to better protect consumer data, after consumer social security numbers were printed on letters mailed to its Medicare and Medicare Part D customers.

HHS Investigations and Settlements under HIPPA—25 Examples Enclosed

- HHS settles with Affinity Health Plan in August 2013 for $1.2 million after the firm returned leased photocopies to the leasing company without first erasing the hard drive, potentially exposing protected consumer health data.
- BlueCross BlueShield of Tennessee fined $1.5 million in 2012 when an intruder stole 57 hard drives which contained protected health information. However, even HHS acknowledged that the information would be very difficult to extract from the hard drives.

CVS agrees to $250K data privacy resolution with Maryland AG

Author Name **Patrick Ouellette** | Date **August 30, 2013** | Tagged Administrative Safeguards, Health Data Breach, Health Data Encryption, Health Data Security, HIPAA, Patient Privacy, Pharmacy Data Breach, PHI, Physical Safeguards, State Patient Privacy Laws, Technical Safeguards



CVS Pharmacy, Inc. and Maryland CVS Pharmacy, LLC reached a $250,000 agreement this week with Attorney General Douglas F. Gansler's Consumer Protection Division because it didn't do enough protect patient data in the eyes of the AG.

This settlement also resolved allegations that CVS sold and offered for sale products after their expiration dates had passed, but it's noteworthy that it's taken five years since the original accusations that dated back to 2008 to resolve the issue. CVS has since said in a statement that it agreed to the settlement to avoid the time and expense of further legal proceedings.

The Consumer Protection Division had received complaints that CVS pharmacies had been discarding records containing patients' protected health information (PHI) in open dumpsters. This violated Maryland's Consumer Protection Act, which says it's an unfair and deceptive trade practice for a business to attempt to dispose of records containing its customers' PHI without taking reasonable steps to protect against unauthorized access to or use of them.

"This settlement speaks to the health and wellbeing of all consumers," said Attorney General Gansler to somd.com. "Expired products don't belong on store shelves and we know that individuals' personal information, if exposed, could lead to serious problems."

Under the terms of the settlement, according to legalnewsline.com, CVS will maintain, revise and enforce new policies for the disposal of protected health information, conduct internal monitoring, implement an employee training program for handling and disposing of patient information and report any noncompliance to the division for three years.

Calif. attorney general focuses on retailers'data theft

Elizabeth Weise, USATODAY

8:12 p.m. EST February 27, 2014

(Photo: Mark Duncan, AP)

SAN FRANCISCO — California Attorney General Kamala Harris on Thursday elevated cybersecurity to a major focus of the state's top crime-fighting agency.

Harris said the personal information of 21.3 million Californians has been compromised in the past two years. Nearly three-quarters of the 300 data breaches were at retailers.

California is one of the few states that require companies to report when the data of 500 or more customers is stolen. Several members of Congress, prompted by a huge data breach at Target late last year, are calling for laws requiring companies to report when something like that happens.

As many as 110 million people were caught up in the Target breach, including 7.5 million California accounts.

In 2012, the first year California required reports, the state logged 131 breaches. In 2013, that number climbed to 170.

Harris' office also disclosed that California is leading a multistate investigation into the massive holiday-season consumer data theft at discount retailer Target and luxury retailer Neiman Marcus — breaches that left tens of millions of customers at risk.

To aid small businesses dealing with the increasing cyberthreats, Harris' office has posted an online pamphlet.

Titled *Cybersecurity in the Golden State*, it outlines how businesses can prepare to reduce risks to their customers and themselves.

"Technology has created new opportunities and new risks for California businesses, including cyberattacks," Harris said. "This guide offers specific, straightforward recommendations to help businesses continue to thrive by reducing cybersecurity risks to employees and customers."

Her office created the pamphlet because small businesses don't always realize they are at risk and don't have the "cybersecurity experts and money to burn" that larger companies have, said Nick Pacilio, spokesman for the attorney general.

Half of reported hacking attempts in California in 2012 targeted businesses with fewer than 2,500 employees, and nearly a third of all attacks were aimed at businesses with fewer than 250 employees.

The pamphlet suggests:

• Businesses should assume they are a target. Being small and unknown is no protection

• Company executives need to be involved. Cybersecurity isn't just an IT problem.

• Companies need to know what kind of data they have and where the data are stored.

• Data should be encrypted.

• Businesses should do online banking only through secure browser connections. Limits should be set on wire transfers.

• Employees need to be educated about security.

• Strong passwords are a must.

• Businesses should have a disaster plan in place in case they are attacked.

Data breaches already reported for 2014 include:

• A processing error on the L.A. Care Health Plan payment website allowed some members to see the names, addresses and identification numbers of other members.

• The Freeman Company in Dallas accidentally sent some employees the W-2 forms of other employees.

• The e-mail of a medical provider at the University of California, Davis Health System was breached by a "phishing" scam that allowed malicious software to potentially access the provider's e-mail account. That might have revealed patients' names, medical records and clinic visits.

Contributing: The Associated Press

Read or Share this story: http://usat.ly/1bPbE9P

STOLEN CREDIT DATA (/TOPIC/66F729E1-5F90-4DB7-ABFC-266640C86A77/STOLEN-CREDIT-DATA/)

Feds warn retailers about hacking software

(/story/money/business/2014/08/22/govt-warns-us-retailers-about-hacking-software/14465319/)

(/story/money/business/2014/08/22/govt-warns-us-retailers-about-hacking-software/14465319/)

Alicia A. Caldwell and Jeff Horwitz

Hackers hit up to 25,000 fed workers

(/story/money/business/2014/08/22/official-says-hackers-hit-up-to-25000-fed-workers/14464417/)

(/story/money/business/2014/08/22/official-says-hackers-hit-up-to-25000-fed-workers/14464417/)

Stephen Braun

Supervalu becomes latest to suffer data breach

(/story/money/business/2014/08/15/supervalu-becomes-latest-to-suffer-data-

CaliforniaHealthline
The Daily Digest of News, Policy & Opinion

DMHC, Blue Shield Announce Data Breach Affecting 18K Calif. Doctors

Thursday, July 10, 2014

RELATED TOPICS:

- Health Care Providers
- Privacy

The Social Security numbers of about 18,000 California physicians were accidentally released with other data by Blue Shield of California and the state Department of Managed Health Care, *Medical Daily* reports (Wolford, *Medical Daily*, 7/9).

Details of Incident

The incident occurred after Blue Shield of California included doctors' Social Security numbers in required monthly filings to the state Department of Managed Health Care. The filings also included doctors':

- Business addresses;
- Business phone numbers;
- Medical group names;
- Names; and
- Practice areas.

Those records then were available to the public under the state's public records law. DMHC distributed the filings in response to 10 public records requests without removing the doctors' Social Security numbers (Williams, *Computerworld*, 7/7). The requests were from other insurers, the insurers' attorneys and two members of the media (Jayanthi, "Hospital CIO," *Becker's Hospital Review*, 7/9).

Blue Shield, DMHC Response

In a letter to affected doctors, Sarah Ream with DMHC wrote, "As a result of this incident, the DMHC and Blue Shield have instituted additional protections to safeguard against future inadvertent disclosure of confidential personal information."

Ream said there is no evidence that the data have been used for identity theft, but the agency is offering a no-cost subscription to a fraud-alert service. In

RELATED ARTICLES

4.6M California Residents Affected by Health Data Breaches Since 2009, HHS Data Show
July 8, 2014

Officials Report Data Breach Involving 34K Patients at Santa Rosa Medical Facility
June 13, 2014

L.A. County Strengthens Data Security Requirements in Response to Recent Medical Data Breach
May 29, 2014

MOST VIEWED MOST COMMENTED

Brown Signs Bill Guaranteeing Paid Sick Leave for California Workers

Anthem, Seven California Health Systems Team Up To Form HMO

California Implements Medi-Cal Coverage for Autism Treatment

View All

EVENTS

SEP 19 2014 NEPO Summit
Sept. 19-21, Riverside

SEP 22 Health 2.0 Fall Conference
Sept. 22-24, Santa Clara

SEP 23 13th Annual IHA Stakeholders Meeting
Sept. 23, Los Angeles

addition, DMHC is implementing software to scan files for private data and issuing reminders to insurers about not including Social Security numbers in monthly filings (*Medical Daily*, 7/9).

According to *Computerworld*, DMHC also is contacting the entities that requested the public files and asking that they destroy the CD's data in exchange for a new CD that does not include the Social Security numbers (*Computerworld*, 7/7).

Meanwhile, Blue Shield is revising its policies for preparing and submitting the monthly filings to DMHC, according to Ream's letter (*Medical Daily*, 7/9). Sean Barry, a Blue Shield spokesperson, said the insurer also is offering affected providers one year of no-cost credit monitoring (*Computerworld*, 7/7).

View All »

15 of 15 DOCUMENTS

Class Action Reporter

July 2, 2014

EBAY INC: Attorney General to Investigate Data Breach

SECTION: Vol. 16 ISSN: 1525-2272

LENGTH: 464 words

The Connecticut Law Tribune reports that two of the state's top lawyers are urging Connecticut consumers who use eBay to change their passwords as soon as possible in light of a cyberattack on the online market place.

Attorney General George Jepsen and state Department of Consumer Protection Commissioner William Rubenstein said that eBay announced on May 21 that the cyberattack had compromised a database of encrypted passwords and other non-financial data. There are about 660,000 active eBay users in Connecticut, the company says, though it is not clear how many may be impacted by the breach. The online company will send emails to all their users, and customers will be prompted to change their password upon signing into their eBay account.

"My office will be looking into the circumstances surrounding this breach as well as the steps eBay is taking to prevent any future incidents," said Mr. Jepsen. "However, the most important step for consumers to take right now is to change their password and to choose a strong, unique password that is not easily guessed."

It's likely that Mr. Jepsen's office won't be the only one looking into the eBay breach. Several technology-oriented websites are reporting that while eBay's data breach reportedly started three months ago, the company detected it only two weeks ago, and didn't inform the public until May 21.

The eBay breach has exposed customer names, email addresses, physical addresses, phone numbers, and birthdays -- all of which had not been encrypted. Financial information, which had been encrypted on PayPal, was apparently not affected.

The attack on eBay affected 233 million accounts. That makes it much larger than the attack on Target last December, which resulted in the theft from the retailer of approximately 40 million credit card records and 110 million personal data records Rubenstein said that anyone "who had been using their eBay password for other internet or email accounts should immediately

assign different passwords for those accounts to protect them from being accessed through this breach. While it's not recommended, many people use the same password over and over. Recent massive data breaches underline the importance of personal password management -- keep your passwords unique for each account."

The Attorney General's Office and Department of Consumer Protection recommend that all consumers regularly change passwords and PIN numbers, whenever possible, to help protect personal and financial information. They also advise consumers to beware so-called "phishing" scam emails in the wake of the breach and avoid clicking on links or opening attachments on any unsolicited emails.

Assistant Attorney General Matthew Fitzsimmons, head of the Attorney General's Privacy Task Force, is assisting Mr. Jepsen with this matter.

AMERICAN BANKER.

btn

BANK TECHNOLOGY NEWS

Connecticut Attorney General Fines Citibank for Data Breach

by Sean Sposito
SEP 3, 2013 8:42pm ET

Two years after a data breach that compromised hundreds of thousands of customer accounts, Citibank has agreed to pay a $55,000 settlement to Connecticut.

During the breach, the state said, criminals were able to access multiple bank customers' online information by logging in with a single account number and password and then modifying the URL in the browser to access others' information.

Roughly 360,000 Citibank customers were affected; about 5,066 were in Connecticut.

Citibank discovered the breach in May 2011. It permanently fixed the problem that month. The vulnerability, Connecticut said, may have existed since 2008.

"Citibank represented to its customers that its online system was secured, but ultimately the techniques hackers used to obtain individual account information were relatively simple and unsophisticated," said Connecticut Attorney General George Jepsen in a press release. "This settlement not only ensures that Citibank will be responsive to its customers should this system experience a breach in the future, it also requires the company to review and audit its security protocols."

The issue was discovered by a joint investigation between Jepsen's office and his California counterpart. The settlement is not final until approved by the court.

Lawbot

Law and technology review

Friday, July 29, 2011

Data Breach Fines Racking Up in Massachusetts

Under Mass ePrivacy Law 200 CMR 17.00, Belmont Savings Bank has agreed to pay a $7,500 fine in a settlement announced in July with the Mass State Attorney General's Office. InfoSecurity reports that the Massachusetts based bank lost 13,000 client records after an employee left an unencrypted back-up tape of the records on their company desk overnight. Bank staff theorized that the tape was dropped in the trash by the night cleanup crew, and later incinerated. Belmont Savings is the second firm to settle with the Mass Attorney General's Office after failing to comply with the new electronic privacy regulations.

Also under Mass ePrivacy Law 200 CMR 17.00, the Boston based restaurant chain, The Briar Group, agreed in March to pay a $110,000 fine after malware diverted credit-card data from their dinner guests over an 8-month span. Regulators charged that the chain allowad employees to share common passwords, and the chain continued to accept credit cards even after it knew of the breach. The Briar Group operates Boston's Lenox Hotel, Ned Devine's, Parris, The Anthem Kitchen & Bar, City Bar Waterfront, The Green Briar, and City Table. The chain maintains three locations at the popular Faneuil Hall Market Place on Boston's historic waterfront. *Reported in InfoSecurity.*

Just in case you missad it, back in February, Massachusetts General Hospital was fined $1M by Health and Human Services after it lost records for 192 patients being treated for infectious disease most likely including HIV. The records were left by an employee on the MBTA. And they never returned and they never returned and their fate is still unlearned. They may ride forever beneath the streets of Boston, they're the health records that never returned. *Reported in InfoSecurity*

Posted by Scott Stanley at 12:29 PM

Labels: Belmont Savings, Briar Group, Encryption, InfoSecurity, Lenox Hotel, Mass General, Privacy Law 200 CMR 17.00

No comments:

Post a Comment

Note: Only a member of this blog may post a comment.

Blog Archive

Massachusetts AGO Enters Into Another Settlement For Data Security Violations

By Amy Crafts on January 22nd, 2013

For the fourth time since the Massachusetts data security regulations took effect in March 2010, the Massachusetts Attorney General's Office ("AGO") has settled allegations that Massachusetts-based entities violated the regulations. On January 7, 2013, Suffolk Superior Court approved consent judgments pursuant to which five entities agreed to collectively pay $140,000 to settle allegations that they mishandled and improperly disposed of medical records containing personal information and protected health information. The settlement amount includes civil penalties, attorneys' fees and an allocated amount for a data protection fund to support efforts to improve the security and privacy of sensitive health and financial information in Massachusetts. A copy of the complaint and corresponding consent judgments are attached here.

The medical records contained information relating to more than 67,000 residents, and included names, Social Security numbers, health insurance information and medical diagnoses that were not redacted or destroyed before they were discarded at a local transfer station. The five entities include Goldthwait Associates, which provided medical billing services, in addition to four pathology groups that worked with Massachusetts hospitals and medical centers.

The AGO alleged that Goldthwait Associates mishandled and disposed of medical records containing personal information and protected health information that it received from the pathology groups. In addition, the AGO alleged that the four pathology groups failed to have appropriate safeguards in place to protect the personal information they provided to Goldthwait Associates, and did not take reasonable steps to select and retain a service provider that would maintain appropriate security measures to protect such confidential information. The complaint alleged that Goldthwait Associates violated the Massachusetts Consumer Protection Act, M.G.L. c. 93A; the Massachusetts Data Disposal and Destruction Act, M.G.L. c. 93I; and the Massachusetts Security Breach Act and its corresponding regulations, M.G.L. c. 93H/201 CMR 17.00. In addition, the complaint alleged that the four pathology groups violated the Massachusetts Security Breach Act and its corresponding regulations, M.G.L. c. 93H/201 CMR 17.00; and HIPAA Privacy and Security Rules, 45 C.F.R. §§ 160 to 164.

Unlike the other data security violations prosecuted by the AGO where the settling entity was required to disclose a data breach to the AGO, this matter first became public in 2010 when a *Boston Globe* photographer was discarding his own garbage at the transfer station and noticed a large stack of paper which, upon closer inspection, he discovered to be medical records. It thereafter became apparent that the owners of Goldthwait Associates had recently retired and, in an effort to dispose of their records as cheaply and quickly as possible, had

hired their son to discard the documents at a local transfer station. The complaint stated that Goldthwait's "failure to institute and implement reasonable data security measures to protect the confidentiality of protected health and personal information entrusted to Goldthwait, and instead allow an untrained third-party to dispose of the documents at a dump, resulted in a serious violation of patient privacy and violations of state consumer protection and data security laws."

Since the regulations went into effect in March 2010, the AGO has sent a consistent message of enforcement. In a statement announcing the January 7th settlement, Massachusetts Attorney General Martha Coakley stated: "Personal health information must be safeguarded as it passes from patients to doctors to medical billers and other third party contractors . . . . We believe this data breach put thousands of patients at risk, and it is the obligation of all parties involved to ensure that sensitive information is disposed of properly to prevent this from happening again."

Proskauer Rose LLP
Beijing
Suite 5102, 51/F Beijing Yintai Centre Tower C
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, China
Phone: 86.10.8572.1800
Boca Raton
2255 Glades Road
Suite 421 Atrium
Boca Raton, FL 33431-7360
Phone: 561.241.7400
Boston
One International Place
Boston, MA 02110-2600
Phone: 617.526.9600
Chicago
Three First National Plaza
70 West Madison
Suite 3800
Chicago, IL 60602-4342
Phone: 312.962.3550
Hong Kong
Suites 1701-1705, 17/F
Two Exchange Square
8 Connaught Place
Central, Hong Kong
Phone: 852.3410.8000
London
Ninth Floor
Ten Bishops Square
London E1 6EG
United Kingdom
Phone: 44.20.7539.0600
Los Angeles
2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
Phone: 310.557.2900
Newark
One Newark Center
Newark, NJ 07102-5211

Plus Media Solutions
US Official News

July 24, 2014 Thursday

Massachusetts: Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients

LENGTH: 614 words

DATELINE: Boston

The office of Attorney General, The State of Massachusetts has issued the following news release:

Women & Infants Hospital of Rhode Island (WIH) has agreed to pay $150,000 to resolve allegations that it failed to protect the personal information and protected health information of more than 12,000 patients in Massachusetts, Attorney General Martha Coakley announced today.

The consent judgment, approved yesterday by Suffolk Superior Court Judge Carol Ball, resulted from a data breach reported to the AG's Office in November 2012 that included patients' names, dates of birth, Social Security numbers, dates of exams, physicians' names, and ultrasound images.

"Personal information and protected health information must be properly safeguarded by hospitals and other healthcare entities," AG Coakley said. "This data breach put thousands of Massachusetts consumers at risk, and it is the hospital's responsibility to ensure that this type of event does not happen again."

In April 2012, WIH realized that it was missing 19 unencrypted back-up tapes from two of its Prenatal Diagnostic Centers, one located in Providence, Rhode Island and the other located in New Bedford, Massachusetts. The back-up tapes contained the personal information and protected health information of 12,127 Massachusetts residents.

In the summer of 2011, these back-up tapes were supposed to be sent to a central data center at WIH's parent company, Care New England Health System and then shipped off-site in order to transfer legacy radiology information to a new picture archiving and communications system. However, due to an inadequate inventory and tracking system, WIH allegedly did not discover the tapes were missing until the spring of 2012. Due to deficient employee training and internal policies, the breach was not properly reported under the breach notification statute to the AG's Office and to consumers until the fall of 2012.

Under the terms of the settlement, WIH has agreed to take steps to ensure future compliance with state and federal data security laws and regulations, including maintaining an up-to-date inventory of the locations, custodians, and descriptions of unencrypted electronic media and paper patient charts containing personal

information and protected health information. The hospital also agreed to perform a review and audit of security measures and to take any corrective measures recommended in the review.

According to the settlement, WIH will pay a $110,000 civil penalty, $25,000 for attorney's fees and costs, and a payment of $15,000 to a fund to be used by the Attorney General's Office to promote education concerning the protection of personal information and protected health information and a fund for future data security litigation.

The AG's Office is focused on ensuring that health care practices and their business associates abide by the state's date security laws and federal data privacy requirements under HIPAA and the HITECH Act. Efforts include the $750,000 settlement with South Shore Hospital in May 2012, resolving allegations that it failed to protect the personal information and protected health information of more than 800,000 patients. In 2013, the AG's Office reached a $140,000 settlement with medical billing company Goldthwait Associates and its client pathology groups over allegations that sensitive medical records and confidential billing information for tens of thousands of Massachusetts patients were improperly disposed of at a public dump in Georgetown.

This matter is being handled by Assistant Attorney General Shannon Choy-Seymour of the Health Care Division.

Massachusetts Hospital Agrees to Pay $775,000 for Security Breach

By Amy Crafts on June 1st, 2012

Following a two year investigation by the Massachusetts Attorney General's Office ("AGO"), a local Massachusetts hospital has agreed to pay $775,000 to resolve allegations that it failed to protect the personal and confidential health information of more than 800,000 consumers. The investigation and settlement resulted from a data breach disclosed by South Shore Hospital in 2010, where the information disclosed included individuals' names, Social Security numbers, financial account numbers and medical diagnoses.

In February 2010, South Shore Hospital retained a third-party service provider to erase 473 unencrypted back-up tapes that contained the personal information and protected health information of over 800,000 individuals. While the third-party service provider was retained before the Regulations were implemented, the AGO noted that South Shore Hospital did not notify the third-party service provider that the tapes contained such sensitive information, and also did not verify that the third-party service provider had adequate safeguards in place to protect the sensitive information.

In June 2010, South Shore Hospital learned that only one of the boxes was accounted for, and that two of the boxes were missing. There have been no reports of unauthorized use of the personal information or protected health information to date. An investigation conducted by South Shore Hospital indicated that the back-up tapes were likely disposed of in a secure commercial landfill and were therefore unrecoverable.

In addition to claiming that South Shore Hospital violated the Health Information Technology for Economic and Clinical Health Act ("HITECH" Act), which gives state Attorneys General the authority to bring civil actions on behalf of state residents for violations of the Health Insurance Portability and Accountability Act ("HIPAA"), the action against South Shore Hospital claimed violation of Massachusetts's stringent data security regulations, which went into effect on March 1, 2010. The allegations included failure to implement appropriate safeguards, policies and procedures to protect customers' information; failure to have a Business Associate Agreement in place with the third-party service provider; and failure to train its workforce with respect to health data privacy.

The significant $775,000 fine includes a $250,000 civil penalty and a $225,000 payment for an education fund to be used by the AGO to promote education concerning the protection of personal information and protected health information. In addition to these payments, the consent judgment credits South Shore Hospital $275,000 to reflect security measures it has taken subsequent to the breach.

This is the third enforcement action pursued by the AGO that addresses a breach of security occurring after the

data security regulations went into effect. Thus far, all of the enforcement actions have resulted in settlements. But the payment agreed to by the AGO and South Shore Hospital far exceeds payments agreed to in other settlements.

The AGO appears to be holding up to its promise that it will vigorously enforce the data security regulations. Indeed, Attorney General Coakley stated that "Hospitals and other entities that handle personal and protected health information have an obligation to properly protect this sensitive data, whether it is in paper or electronic form. It is their responsibility to understand and comply with the laws of our Commonwealth and to take the necessary actions to ensure that all affected customers are aware of a data breach."

Proskauer Rose LLP
Beijing
Suite 5102, 51/F Beijing Yintai Centre Tower C
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, China
Phone: 86.10.8572.1800
Boca Raton
2255 Glades Road
Suite 421 Atrium
Boca Raton, FL 33431-7360
Phone: 561.241.7400
Boston
One International Place
Boston, MA 02110-2600
Phone: 617.526.9600
Chicago
Three First National Plaza
70 West Madison
Suite 3800
Chicago, IL 60602-4342
Phone: 312.962.3550
Hong Kong
Suites 1701-1705, 17/F
Two Exchange Square
8 Connaught Place
Central, Hong Kong
Phone: 852.3410.8000
London
Ninth Floor
Ten Bishops Square
London E1 6EG
United Kingdom
Phone: 44.20.7539.0600
Los Angeles
2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
Phone: 310.557.2900
Newark
One Newark Center
Newark, NJ 07102-5211
Phone: 973.274.3200
New Orleans
Poydras Center
650 Poydras Street

Bay State "Brings It": Attorney General Enters Consent Agreement with Restaurant Group for Data Security Failures

By Brendon Tavelli on April 7th, 2011

On March 28, 2011, the Massachusetts Superior Court issued a Final Judgment by Consent between the Commonwealth and Briar Group, LLC that resolves allegations that Briar Group failed to take measures to protect consumer credit and debit card information. The Final Judgment stems from an April 2009 information security breach in which outside hackers used malware to gain access to Briar Group's computer systems and extract payment card information about the company's restaurant and bar customers. Pursuant to the Final Judgment, Briar Group must pay $110,000 to the Commonwealth, establish a written information security program ("WISP"), and implement a number of other information security measures to help protect customer data.

According to the Attorney General, the Final Judgment "works to ensure that steps have been taken to protect consumer information moving forward." Although the Commonwealth's stringent data security regulations (see our post about 201 CMR 17.00 here) did not become effective until after the April 2009 breach, the Attorney General used the regulations as a reference point for identifying deficiencies in the company's approach to information security. In its complaint against Briar Group, the Attorney General alleged, among other things, that the company (i) failed to change default usernames and passwords for its point-of-sale system, (ii) allowed employees to share passwords, (iii) did not appropriately limit the number of employees with administrative access to company systems, and (iv) stored payment card information in clear text on its servers. Taken together, these deficiencies allowed the breach of Briar Group's systems to continue unabated until approximately December 2009.

In her announcement of the Final Judgment, Massachusetts Attorney General Martha Coakley explained that her office "will continue to take action against companies that fail to implement basic security measures on their computer systems to protect the sensitive information entrusted to them by consumers." With this in mind, and 201 CMR 17.00 now firmly entrenched, companies handling personal information about Massachusetts residents should be prepared. *Hint: That means have a WISP and follow it!*

Proskauer Rose LLP
Beijing

NATIONAL ASSOCIATION of REALTORS®

ARTICLES

Property Management Firm Pays $15,000 Fine Following Data Breach

By Melanie Wyne

April 2, 2012

On March 21st the Massachusetts Attorney General announced that a property management firm was fined $15,000 after the theft of a company laptop containing the personal information of over 600 Massachusetts residents.

According to the Massachusetts Attorney General, an employee of the property management company had a laptop containing unencrypted personal information stolen from her car during the night. This incident was found to be in violation of Massachusetts' Data Breach Regulation.

In addition to paying $15,000 in civil penalties the company must:

- Ensure that personal information is not unnecessarily stored on portable devices;
- Ensure that all personal information stored on portable devices is properly encrypted;
- Ensure that all portable devices containing personal information are stored in a secure location; and
- Effectively train employees on the policies and procedures with respect to maintaining the security of personal information

Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

Minnesota A.G. Files Lawsuit Against "Infused" Business Associate for Loss of Patient Data Stored on Laptop; Use of Patient Data Without Full Disclosure

By John Mulhollan on February 6, 2012

In perhaps the first widely publicized action taken against a "business associate" (as defined under the Health Insurance Portability and Accountability Act (HIPAA) and privacy and security regulations thereunder), the Minnesota Attorney General (AG) on January 19 filed a civil lawsuit in federal court against Accretive Health, Inc., for alleged violations of HIPAA, as well as alleged violations of that state's medical privacy law and consumer debt collection practices laws. *Minnesota v. Accretive Health Inc.*, D. Minn., No. 12-145, filed January 19, 2012. The lawsuit arises from the loss by an Accretive employee of a laptop containing several thousand records that included the individually identifiable health information of patients from Accretive's hospital customers. The action is filed under the powers granted to state attorneys general under HITECH provisions that expanded the enforcement powers and civil penalties available for violations of HIPAA.

Accretive Health Inc., the business associate and defendant in the lawsuit, was engaged by two hospitals to perform revenue cycle management services, including a so-called "Quality and Total Cost of Care" service agreement that is alleged to have included intensive management of a hospital's entire revenue cycle process (from patient admissions and registrations, to care coordination, to back office collections of patient receivables), for a fee that included a share of "incentive payments" received by the hospital from payors in return for achieving certain cost savings and quality measures. According to the complaint, management of the hospitals' revenue cycles was performed through so-called "infused employees" of Accretive working on-site in various departments of the hospitals. The patient data was lost when a laptop containing data of approximately 17,000 to 23,000 patients allegedly was stolen from the back seat of a vehicle of an Accretive employee while parked at a local restaurant.

In the lawsuit, the AG alleges that the business associate failed to take adequate security precautions, such as encryption of the data on the lost laptop, to protect the patient information ou the device. The information included patients' names, addresses, phone numbers, Social Security numbers and certain clinical information, including information related to chronic conditions such as mental health and HIV/AIDS conditions. Further, the AG alleges that the business associate violated the Minnesota Health Records Act and various state consumer fraud and deceptive practices acts by, among other things, failing to disclose to the hospital patients its extensive

role in the hospitals' revenue cycle process, its role as a debt collector and its role in the proactive management of patient care, including the incentive payments based on the hospital's cost savings.

While the remedies available to the AG in this case under HIPAA and the HITECH Act are limited to $25,000 per year, compared to the $1.5 million that the federal government could impose for violations, the defendant in this case, if found to have violated the consumer protection and debt collection agency laws, could face significant financial liability and negative effects on its business reputation. This new enforcement action highlights not only the risks inherent in failing to protect patient data that leads to a privacy breach, but also reveals the underlying scrutiny that will be applied to a business associate's business practices as a result of a data breach. Following actions filed against covered entities in Connecticut and Vermont, this case may portend a new trend of enforcement against HIPAA business associates. Stay tuned...

See the AG's complaint.

---

12 of 15 DOCUMENTS

The Burlington Free Press (Vermont)

July 10, 2014 Thursday
1 Edition

Shelburne store fined over credit card breach

BYLINE: By, Free Press Staff

SECTION: A; Pg. 11

LENGTH: 186 words

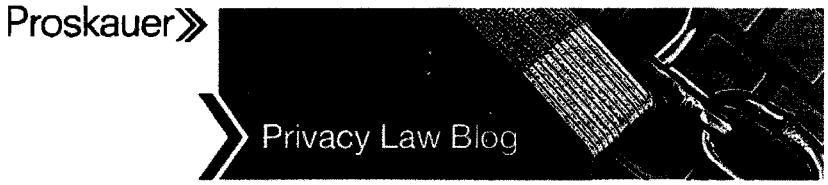
Shelburne Country Store has been fined $3,000 by the state Attorney General's Office for failing to inform 721 online customers that their credit card information had been compromised.

In late 2013, the company's website was hacked and credit card information stolen. Shelburne Country Store quickly fixed the problem with their website when it was informed of the breach in January 2014 but didn't tell customers affected by the breach until contacted by the Attorney General's Office.

"At this stage of the game, having seen widely reported data breaches at big retailers like Target and dozens of others, we will not accept the excuse that a business did not know of its obligations to report a breach," Attorney General William Sorrell said in a statement.

Under Vermont's Security Breach Notice Act, businesses are required to send the Attorney General a confidential notice within 14 days of discovering a breach. The business must also send notice to its affected customers in no later than 45 days.

Any business with questions about the Security Breach Notice Act can call 828-5479, or email data.security@state.vt.us



Glacially Expedient? Vermont Attorney General Settles with HealthNet for Failure to Timely Notify State Residents of Data Breach

By Brendon Tavelli on January 28th, 2011

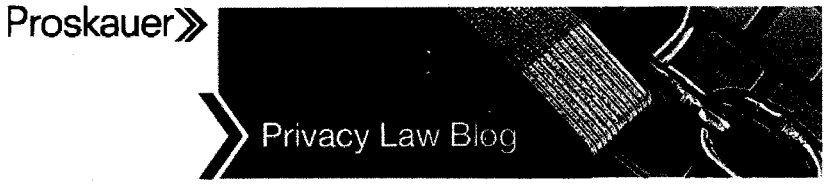
On January 18, 2011, Vermont Attorney General William Sorrell announced a settlement with HealthNet, Inc. and Health Net of the Northeast, Inc. over allegations that the company violated the state's data breach notification law when the company waited over six months to notify state residents of the loss of a portable hard drive that contained their unencrypted personal information. The Attorney General's settlement, the first under Vermont's Security Breach Notice Act, demonstrates that, in the opinion of the Vermont Attorney General, even in the frozen North a six-month gap between the discovery of a breach and notice to individuals cannot be reconciled with the Act's requirement to notify individuals "in the most expedient time possible and without unreasonable delay."

The lengthy delay between discovery of the lost hard drive and individual notifications was not the only thing Sorrell found to be wrong with HealthNet's response to the May 2009 breach, however. Vermont's Attorney General also claimed that HealthNet violated the federal Health Insurance Portability and Accountability Act ("HIPAA") by failing to secure protected health information and the state's Consumer Fraud Act by misrepresenting, in its letters to individuals, the risk posed by the breach. In those letters, HealthNet told individuals that the risk of harm to them was "low" because the files were saved in a format that could not be easily accessed when, in reality, the files were saved in the relatively easily viewable TIF format.

The Vermont Attorney General's settlement with HealthNet, which the U.S. District Court for the District of Vermont approved on January 21, 2011, requires the company to pay $55,000 to the State, submit to a data-security audit, and file reports with the State regarding the company's information security programs for the next two years.

The HealthNet settlement is an important reminder that the unpleasantness of a security breach is only compounded by a poor response. If you have not already done so, the time for establishing a comprehensive breach response plan is now!

Proskauer Rose LLP
Beijing



You, NOT the Newspapers, Should Report a Breach: WellPoint to Pay $100,000 to Indiana AG for Delayed Breach Notification

By Brendon Tavelli on July 11th, 2011

On July 5, 2011, Indiana Attorney General Greg Zoeller announced a settlement with health insurer WellPoint, Inc. The settlement resolves allegations that the company failed to promptly notify the Attorney General's office of a data breach as is required by the Indiana Disclosure of Security Breach Act. As part of the settlement, WellPoint will pay a fine of $100,000 and provide certain identity-theft-prevention assistance to consumers affected by the breach. Interestingly, the settlement includes an admission by WellPoint that the company failed to comply with the law by not notifying Zoeller's office "without unreasonable delay."

The data breach out of which the Attorney General's investigation, lawsuit, and ultimate settlement arose occurred between October 2009 and March 2010. During that time, personal information submitted in connection with applications for individual insurance policies was made publicly accessible via the company's online application tracker website. The exposed information included Social Security numbers, financial account information, and health records. WellPoint immediately secured the application tracker site in early March 2010 after being told by a consumer, a second time, that records containing personal information were potentially accessible on the site.

WellPoint notified affected consumers of the breach beginning in June 2010, but did not also notify the Attorney General's office as required by Indiana law. When Zoeller's office learned of the breach through news reports in late July, it launched an investigation and in October filed suit against the company seeking an injunction and civil penalties for violations of the Indiana Disclosure of Security Breach Act. The parties' recent settlement makes the Attorney General's lawsuit disappear, but not without significant costs to WellPoint. The settlement mandates that WellPoint pay $100,000 into the Attorney General's Consumer Assistance Fund; comply with the Disclosure of Security Breach Act in the future and admit that it failed to do so in this instance; provide affected consumers with up to two years of credit monitoring; and reimburse affected consumers up to $50,000 for any losses that result from identity theft stemming from the breach.

Although WellPoint is currently the public face of improper breach notification in Indiana, it is apparently not alone. Attorney General Zoeller's office has issued warning letters to 47 other companies that delayed issuing appropriate security breach notifications. Perhaps it should go without saying, but according to Zoeller, "[t]he requirement to notify the Attorney General 'without unreasonable delay' is not fulfilled by having me read about

the breach in the newspaper." Sounds simple enough, but are you faster than the reporters? We certainly hope so.

Proskauer Rose LLP
Beijing
Suite 5102, 51/F Beijing Yintai Centre Tower C
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, China
Phone: 86.10.8572.1800
Boca Raton
2255 Glades Road
Suite 421 Atrium
Boca Raton, FL 33431-7360
Phone: 561.241.7400
Boston
One International Place
Boston, MA 02110-2600
Phone: 617.526.9600
Chicago
Three First National Plaza
70 West Madison
Suite 3800
Chicago, IL 60602-4342
Phone: 312.962.3550
Hong Kong
Suites 1701-1705, 17/F
Two Exchange Square
8 Connaught Place
Central, Hong Kong
Phone: 852.3410.8000
London
Ninth Floor
Ten Bishops Square
London E1 6EG
United Kingdom
Phone: 44.20.7539.0600
Los Angeles
2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
Phone: 310.557.2900
Newark
One Newark Center
Newark, NJ 07102-5211
Phone: 973.274.3200
New Orleans
Poydras Center
650 Poydras Street
Suite 1800
New Orleans, LA 70130-6146
Phone: 504.310.4088
New York
Eleven Times Square
New York, NY 10036-8299
Phone: 212.969.3000
Paris
374 rue Saint-Honoré

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Civil Action No. 1:06-cv-0198-JTC
	)	
v.	)	
	)	
CHOICEPOINT, INC., a corporation,	)	
	)	
Defendant.	)	
	)	

SECOND SUPPLEMENTAL STIPULATED ORDER FOR PERMANENT INJUNCTION

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or "Commission"), and Defendant ChoicePoint, Inc. ("Defendant") jointly stipulate to this Second Supplemental Stipulated Order for Permanent Injunction ("Second Supplemental Order"), which modifies the time periods under which the Defendant shall obtain biennial assessments and reports ("Assessments").

NOW THEREFORE IT IS HEREBY ORDERED AS FOLLOWS:

FINDINGS OF FACT AND CONCLUSIONS OF LAW

A. This Court has jurisdiction over the subject matter of this case and over Defendant.

B. Venue in this district is proper under 28 U.S.C. § 1391(b) and (c), and 15 U.S.C. § 53(b).

C. The acts and practices of Defendant are in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

D. The Court finds that entry of this Second Supplemental Order is in the public interest.

E. All provisions of the Final Order and the Supplemental Stipulated Judgment and Order for Permanent Injunction and Monetary Relief remain in full force and effect except as otherwise stated in this Second Supplemental Order.

F. Defendant waives: (a) all rights to seek appellate review or otherwise challenge or contest the validity of this Second Supplemental Order; (b) any claim Defendant may have against the Commission, its employees, representatives, or agents that relate to the matter stated herein; (c) all claims under the Equal Access to Justice Act, 28 U.S.C. § 2412, as amended by Pub. L. 104-121, 110 Stat. 847, 863-64 (1996); and (d) any rights to attorney's fees that may arise under said provision of law.

I. BIENNIAL ASSESSMENT REQUIREMENTS

(Supersedes Paragraph II in the Supplemental Stipulated Judgment and Order for Permanent Injunction and Monetary Relief)

IT IS FURTHER ORDERED that Defendant shall obtain assessments and reports ("Assessments") from a qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession. The Assessments shall cover the following reporting periods:

(1) August 16, 2008 to August 15, 2010;

(2) August 16, 2010 to February 3, 2011;

(3) Every two years from February 4, 2011 to February 3, 2025; and

(4) February 4, 2025 to February 15, 2026;

Provided however, that the Commission, at its sole discretion, may require Defendant to obtain up to two additional Assessments covering the two two-year periods following the final Assessment period ending February 15, 2026, if the FTC provides the Defendant with written

notice between February 15, 2024 and August 15, 2025, stating that the first such additional Assessment will be required, and/or written notice, between February 15, 2026 and August 15, 2027 that the second additional Assessment will be required.

Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that Defendant has implemented and maintained during the reporting period to comply with Paragraph III of the Final Order;

B. Explain how such safeguards are appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, and the sensitivity of the personal information collected from or about consumers;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph III of the Final Order; and

D. Certify that Defendant's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected, and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Within fifteen (15) days after each Assessment is prepared and completed, Defendant

shall notify the Commission that the Assessment has been prepared and completed and provide: (1) the name, address, phone number, and credentials of the third-party professional who conducted the Assessment; (2) an overview of the administrative, technical, and physical safeguards the third-party professional evaluated for the Assessment; and (3) proof of certification from the third-party professional as required under Paragraph I.D of this Second Supplemental Order. Defendant shall deliver all notifications to the Commission pursuant to Paragraph IV.D of the Supplemental Order.

All Assessments shall be retained by Defendant until three (3) years after completion of the final Assessment and provided to the Associate Director for Enforcement upon request within ten (10) business days after Defendant receives such request.

II. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Second Supplemental Order.

III. COSTS AND ATTORNEY'S FEES

IT IS FURTHER ORDERED that each party shall bear its own costs and attorney's fees incurred in connection with this action.

//

//

//

//

//

//

IV. NOTICE OF ENTRY OF SUPPLEMENTAL ORDER

IT IS FURTHER ORDERED that entry in the docket of this Second Supplemental Order by the Clerk of Court shall constitute notice to Defendant of the terms and conditions of this Second Supplemental Order, and that Defendant waives all rights to contest in any future proceeding whether Defendant was properly served with this Second Supplemental Order.

IT IS SO ORDERED:

Dated this 3RD day of SEPTEMBER 2010.

Hon. Jack T. Camp
United States District Judge

//

//

//

//

//

//

//

//

//

//

//

FOR THE FEDERAL TRADE COMMISSION:

JAMES A. KOHM
Associate Director for Enforcement
ROBERT S. KAYE
Assistant Director for Enforcement

Robin Rosen Spector, Attorney
Jock Chung, Attorney
Federal Trade Commission
Division of Enforcement
600 Pennsylvania Avenue, NW
Suite M-8102B
Washington, D.C. 20580
(202) 326-3740 (Spector)
(202) 326-2984 (Chung)
(202) 326-2558 (fax)

WILLARD K. TOM
General Counsel

FOR THE DEFENDANT:

ChoicePoint, Inc.
By: James Peck
Chief Executive Officer

Reviewed by Legal

Robert R. Belair, Esq.
Kevin L. Coy, Esq.
Oldaker, Belair, & Wittie L.L.P.
818 Connecticut Avenue, N.W.
Suite 1100
Washington, D.C. 20006

Counsel for Defendant

Christopher Wolf, Esq.
Hogan & Hartson LLP
Columbia Square
555 Thirteenth Street N.W.
Washington, D.C. 20004

Counsel for Defendant

//

//

//

//

//

FOR THE PLAINTIFF, THE UNITED STATES OF AMERICA:

SALLY QUILLIAN YATES
United States Attorney

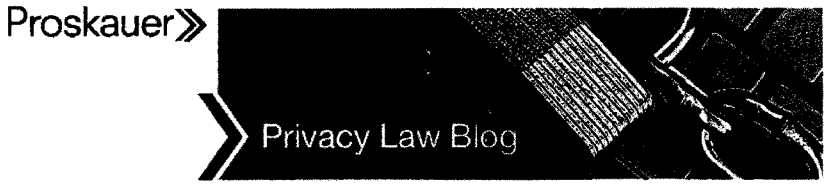
DANIEL A. CALDWELL
Assistant United States Attorney
Georgia Bar No. 102510
600 Richard B. Russell Building
75 Spring Street, SW
Atlanta, Georgia 30303
Telephone: (404) 581-6224
Facsimile: (404) 581-6181
E-mail: Dan.Caldwell@usdoj.gov

EUGENE M. THIROLF
Director
Office of Consumer Litigation

KENNETH L. JOST
Deputy Director
Office of Consumer Litigation

ALAN J. PHELPS
Trial Attorney
Office of Consumer Litigation
PO Box 386
Washington, D.C. 20044
Telephone: (202) 307-6154
Facsimile: (202) 514-8742
E-mail: Alan.Phelps@usdoj.gov

Attorneys for Plaintiff
United States of America



A $1.2 Million Photocopier Mistake: Health Plan Settles with HHS in HIPAA Breach Case

By Ryan Blaney on August 20th, 2013

We have heard the well-publicized stories of stolen laptops and resulting violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and we generally recognize the inherent security risks and potential for breach of unsecured electronic protected health information posed by computer hard drives. We remember to "wipe" the personal data off of our phones or computers before they are disposed, donated, or recycled.

A recent HIPAA settlement offers a costly reminder that other types of office equipment we use regularly have similar hard drives capable of storing confidential personal information.

On August 14, 2013, HHS announced a $1,215,780 settlement with the not-for-profit managed care plan Affinity Health Plan, Inc., stemming from an investigation of potential violations of the HIPAA Privacy and Security Rules relating to an April 15, 2010 breach report filed by Affinity with the HHS Office for Civil Rights (OCR). Affinity's breach report and OCR's subsequent investigation revealed that Affinity had impermissibly disclosed the protected health information of up to 344,579 individuals when it returned multiple photocopiers to leasing agents without erasing the photocopier hard drives. Affinity learned of the breach when a representative from CBS Evening News informed the New York health plan that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity and had found confidential medical information on the photocopier's hard drive. OCR's investigation indicated that Affinity had failed to assess the potential security risks and implement policies for the disposal of protected health information stored on the photocopier hard drives.

In addition to the financial settlement, the Resolution Agreement includes a corrective action plan (CAP) requiring Affinity to use its "best efforts to retrieve all photocopier hard drives that were contained in photocopiers previously leased by [Affinity] that remain in the possession of [the leasing agent]." The CAP also requires Affinity to conduct a comprehensive risk analysis and implement safeguards to protect electronic protected health information on all of its electronic equipment and systems.

For more than ten years, digital copiers have been capable of storing images of documents. This settlement should serve as a warning to entities and individuals who handle electronic personal health information: any and all equipment capable of storing trace amounts of digital information should be accounted for in risk assessments conducted under the HIPAA Security Rule. All HIPAA Privacy and Security Policies and Procedures Manuals

should be updated to include guidelines for safeguarding protected health information retained on digital copiers, scanners, fax machines and other devices whose primary function may not be data storage.

By Ryan Blaney and Kelly Carroll

Proskauer Rose LLP
Beijing
Suite 5102, 51/F Beijing Yintai Centre Tower C
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, China
Phone: 86.10.8572.1800
Boca Raton
2255 Glades Road
Suite 421 Atrium
Boca Raton, FL 33431-7360
Phone: 561.241.7400
Boston
One International Place
Boston, MA 02110-2600
Phone: 617.526.9600
Chicago
Three First National Plaza
70 West Madison
Suite 3800
Chicago, IL 60602-4342
Phone: 312.962.3550
Hong Kong
Suites 1701-1705, 17/F
Two Exchange Square
8 Connaught Place
Central, Hong Kong
Phone: 852.3410.8000
London
Ninth Floor
Ten Bishops Square
London E1 6EG
United Kingdom
Phone: 44.20.7539.0600
Los Angeles
2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
Phone: 310.557.2900
Newark
One Newark Center
Newark, NJ 07102-5211
Phone: 973.274.3200
New Orleans
Poydras Center
650 Poydras Street
Suite 1800
New Orleans, LA 70130-6146
Phone: 504.310.4088
New York
Eleven Times Square
New York, NY 10036-8299

Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

Proposed $6.8M Fine Related to Puerto Rico Breach Incident

By Lynn Sessions and Kimberly M. Wong on March 7, 2014

Triple-S Salud, Inc. ("Triple-S"), a Puerto Rico Health Insurance Administration ("PRHIA") contractor, filed a Form 8-K indicating that the PRHIA intended to impose a civil monetary penalty of $6,768,000 and other administrative sanctions stemming from a breach incident affecting 13,336 Dual Eligible Medicare beneficiaries. The breach incident occurred in September 2013 when Triple-S mailed to approximately 70,000 Medicare beneficiaries a pamphlet that inadvertently displayed the receiving beneficiary's Medicare Health Insurance Claim Number. In addition to the proposed fine, the Form 8-K indicates that sanctions include: suspending enrollment of dual-eligible beneficiaries; notification to all affected individuals of their right to end their enrollment; and implementation of a corrective action plan from PHRIA to prevent future breach incidents.

In an El Nuevo Dia article, PHRIA Executive Director Ricardo A. Rivera Cardona explained that the fine results from how Triple-S incorrectly handled sensitive information protected by HIPAA. The PHRIA and Triple-S contract imposes fines for HIPAA violations. Of the total fine, $100,000 is due to incomplete information provided by Triple-S to PHRIA in their investigation. Triple-S has 30 days to request an administrative hearing regarding the fine.

As to breaches affecting 500 or more patients, in addition to the September 2013 incident, Triple-S has reported two other incidents to the Department of Health and Human Services Office for Civil Rights. In September 2010, Triple-S reported a theft affecting the PHI of 398,000 individuals. In October of 2008, Triple-S reported a theft and unauthorized access/disclosure affecting the PHI of 8,000 individuals.

PHRIA's proposed civil monetary penalty falls well outside the settlement amounts and civil monetary penalty ("CMP") previously issued by OCR. Settlement amounts with OCR have ranged between $35,000 to $2.5 million. The only CMP issued by OCR pertained to Cignet Health in the amount of $4.3 million in 2011. The CMP pertained to allegations that Cignet Health blocked 41 patients from accessing their medical records between September 2008 and October 2009. The largest portion of the CMP ($3 million) was due to Cignet Health's refusal to cooperate in OCR's investigation.

Breach incidents continue to result in regulatory investigations and financial penalties. Enforcement activity is likely to continue to increase given OIG's November 2013 report regarding OCR oversight and enforcement of the HIPAA Security Rule. From the enforcement activity covered in 2013 blog posts, covered entities are learning that breach response does not stop at notification.

Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

HHS OCR Settles Post-Data Breach Investigation for Record $4.8M

By Kimberly M. Wong on May 12, 2014

On May 7, 2014, HHS OCR announced a pair of resolution agreements with New York Presbyterian Hospital (NYP) and Columbia University (CU) totaling $4.8 million dollars—the highest settlement amount to date. These resolution agreements make it clear that organizations must be able to propose steps to analyze security risks for ePHI as specified by HIPAA and plan strategies to manage identified risks.

Pursuant to 45 C.F.R. §§ 164.308(a)(1)(i)(ii)(A) and (B), an organization must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

> (i) ensure the confidentiality, integrity, and availability of ePHI created, received, maintained, and/or transmitted;
> (ii) protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
> (iii) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required;
> (iv) ensure compliance by its workforce.

By way of background, NYP and CU are separate covered entities participating in a joint arrangement in which CU faculty members serve as attending physicians at NYP under the affiliation name "New York Presbyterian Hospital/Columbia University Medical Center". The two entities operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network allows access to NYP patient information systems containing ePHI.

The NYP and CU resolution agreements with HHS OCR stem from a joint breach report submitted by the entities on September 27, 2010 regarding the disclosure of the ePHI of 6,800 individuals. The breach occurred when a CU employed physician, who developed applications for both NYP and CU, attempted to deactivate a personally-owned computer server on to the network containing NYP ePHI. This resulted in the availability of patient information on Internet search engines. NYP and CU learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former NYP patient, on the Internet. Patient information affected included patient status, vital signs, medications, and laboratory results.

HHS OCR's investigation of NYP and CU began on November 5, 2010 and indicated:

- NYP impermissibly disclosed the ePHI of 6,800 patients to Google and other Internet search engines when a computer server that had access to NYP ePHI information systems was errantly reconfigured;
- NYP and CU failed to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI;
- NYP and CU failed to implement process for accessing and monitoring all IT equipment, applications, and data systems that were linked to NYP patient databases prior to the breach incident, and failed to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level; and
- NYP failed to implement appropriate policies and procedures for authorizing access to its NYP patient database, and it failed to comply with its own policies on information access management.

In addition to payments from NYP ($3.3 million dollars) and CU ($1.5 million dollars), both entities must comply with a corrective action plan (CAP). As to corrective action:

- NYP shall modify its existing risk analysis process, as well as develop and implement a risk management plan;
- NYP shall develop an enhanced privacy and security awareness program;
- CU shall conduct a thorough risk analysis, as well as develop and implement a risk management plan;
- CU shall review and revise internal policies and procedures on Information Access Management;
- CU shall develop a privacy and security awareness training program;
- NYP and CU shall review and revise its respective policies and procedures on device and media controls; and
- NYP and CU shall each implement a process for evaluating any environmental or opcrational changes that affect the security of their respective ePHI

The CAP for each entity is for a 3-year time period. Both entities must submit the documentation required under its obligations for review and approval by HHS OCR before implementation. In addition, each entity must submit a report to HHS OCR regarding reportable events, implementation status, and compliance with the CAP.

HHS OCR's recent HIPAA enforcement history demonstrates that it intends to enforce the HIPAA risk analysis and mitigation requirements under the Security Rule. Following data breach reports to HHS OCR, organizations are often asked to provide a copy of their most recent risk analysis and mitigation plan related specifically to the facts of the incident, or their most recent analysis and plan in their entirety. In addition, there has been additional attention paid to risk analysis with the Office of the National Coordinator for Health Information Technology (ONC) release of its Security Risk Assessment Tool in March of 2014 (blogged about here). OCR also recently announced its preparation for the next round of HIPAA audits, which likely will focus on HIPAA requirements covered entities are most "unaware" of, including the risk analysis requirement (blogged about here).

Timely and thorough security risk analysis and mitigation is an OCR hot button. Entities must review their current risk analysis and mitigation plan to determine whether potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI is assessed and mitigated.

Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

HHS Settles HIPAA Violations Related to a Breach for $1.5M

By Theodore J. Kobus III on March 15, 2012

BlueCross BlueShield of Tennessee (BCBST) was the victim of a theft in 2009 when an intruder stole 57 hard drives which contained protected health information (PHI) of more than 1 million customers. The information on the hard drives included names, Social Security Numbers, diagnosis codes, dates of birth, and health plan identification numbers. Reports suggest that the information would be very difficult to extract from the hard drives and BlueCross BlueShield of Tennessee undertook great efforts and significant expense to identify their customers. Indeed, over 800 people may have worked on the efforts to identify the customers. After the incident, BCBST undertook efforts to encrypt all data at rest.

Still, BCBST entered into a resolution agreement (.pdf) on March 13, 2011, by which it agreed to pay $1.5M. BCBST also entered into a corrective action plan (CAP) which sets out a period of compliance obligations and has a term of 450 days. The CAP requires:

- BCBST implement policies and procedures (to be reviewed by HHS) which require:
  - A risk assessment be performed to identify potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI when it is created, received, maintained, used, or transmitted on or off-site
  - A risk management plan he implemented to respond to the risks identified in the risk assessment;
  - Use of facility access controls and a facility security plan to limit access to areas where ePHI is located;
  - Physical safeguards governing the storage of electronic storage media containing ePHI;
- Training on policies and procedures;
- Random monitoring by BCBST's Chief Privacy Officer for compliance with the policies;
- Biannual reports to HHS over the CAP period describing compliance with policies and procedures, training efforts, and reportable events that occurred.

When dealing with regulators, such as OCR, keep these principles in mind:

- Regulators expect transparency.
- Your investigation should be prompt, thorough, and well documented. If certain investigations are privileged, make certain that you assert that privilege.
- A good attitude and cooperation send a message that the organization is committed to compliance and safeguarding PII, PHI, and ePHI.
- Notification concerning a breach should be appropriate and prompt.
- Know the root cause of the breach and address it through staff training, awareness programs, technical safeguards, and new policies/procedures/physical safeguards.
- Provide customers with the appropriate level of mitigation or remediation measures. Credit monitoring does not always address the risk to the customer. Sometimes, it can be as simple as advising a patient to monitor its Explanation of Benefits (EOB) statements or telling a customer to file a report with a credit card company that his or her credit card number has potentiall been exposed.

Leon Rodriguez, director of the HHS Office for Civil Rights (OCR) said, "This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program." The safeguard and training requirements of the CAP are very similar to requests for information we see from OCR following a reportable breach. If a healthcare organization does not currently have the above risk management plans and safeguards in place, the warning sent as a result of this settlement is clear—make these compliance issues a priority before you have a reportable breach.

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
June 23, 2014

Contact: HHS Press Office
202-690-6343

$800,000 HIPAA settlement in medical records dumping case

Parkview Health System, Inc. has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule with the U.S. Department of Health and Human Services Office for Civil Rights (OCR). Parkview will pay $800,000 and adopt a corrective action plan to address deficiencies in its HIPAA compliance program. Parkview is a nonprofit health care system that provides community-based health care services to individuals in northeast Indiana and northwest Ohio.

OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA Privacy Rule. In September 2008, Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician's practice. On June 4, 2009, Parkview employees, with notice that the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.

As a covered entity under the HIPAA Privacy Rule, Parkview must appropriately and reasonably safeguard all protected health information in its possession, from the time it is acquired through its disposition.

"All too often we receive complaints of records being discarded or transferred in a manner that puts patient information at risk," said Christina Heide, acting deputy director of health information privacy at OCR. "It is imperative that HIPAA covered entities and their business associates protect patient information during its transfer and disposal."

Parkview cooperated with OCR throughout its investigation. In addition to the $800,000 resolution amount, the settlement includes a corrective action plan requiring Parkview to revise their policies and procedures, train staff, and provide an implementation report to OCR.

OCR offers helpful FAQs concerning HIPAA and the disposal of protected health information: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights, and privacy rights in health care and human service settings, and to find information on filing a

complaint, visit us at http://www.hhs.gov/ocr/office.

The Resolution Agreement can be found on the OCR website at:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/parkview.html

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: June 23, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
May 7, 2014

Contact: HHS Press Office
(202) 690-6343

Data breach results in $4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

"When entities participate in joint compliance arrangements, they share the burden of addressing the risks to protected health information," said Christina Heide, Acting Deputy Director of Health Information Privacy for OCR. "Our cases against NYP and CU should remind health care organizations of the need to make data security central to how they manage their information systems."

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

For information about the basics of HIPAA Security Risk Analysis and Risk Management, as well as other compliance tips, visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training

The New York and Presbyterian Hospital Resolution Agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf

The Columbia University Resolution Agreement may be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/columbia-university-resolution-agreement.pdf

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.HHS.gov/OCR

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: May 8, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
April 22, 2014

Contact: HHS Press Office
202-690-6343

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

"Covered entities and business associates must understand that mobile device security is their obligation," said Susan McAndrew, OCR's deputy director of health information privacy. "Our message to these organizations is simple: encryption is your best defense against these incidents."

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

OCR received a breach notice in February 2012 from QCA Health Plan, Inc. of Arkansas reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car. While QCA encrypted their devices following discovery of the breach, OCR's investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and is required to provide HHS with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI. QCA is also required to retrain its workforce and document its ongoing compliance efforts.

OCR has six educational programs for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules. Each of these programs is available with free Continuing Medical Education credits for physicians and Continuing Education credits for health care professionals, with one module focusing specifically on mobile device security: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training

The Resolution Agreements can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.HHS.gov/OCR

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: April 22, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
March 7, 2014

Contact: HHS Press Office
(202) 690-6343

County Government Settles Potential HIPAA Violations

Skagit County, Washington, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the Department of Health and Human Services (HHS) to correct deficiencies in its HIPAA compliance program. Skagit County is located in Northwest Washington, and is home to approximately 118,000 residents. The Skagit County Public Health Department provides essential services to many individuals who would otherwise not be able to afford health care.

"This case marks the first settlement with a county government and sends a strong message about the importance of HIPAA compliance to local and county governments, regardless of size," said Susan McAndrew, deputy director of health information privacy at the HHS Office for Civil Rights (OCR). "These agencies need to adopt a meaningful compliance program to ensure the privacy and security of patients' information."

OCR opened an investigation of Skagit County upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County. OCR's investigation revealed a broader exposure of protected health information involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases. OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.

Skagit County continues to cooperate with OCR through a corrective action plan to ensure it has in place written policies and procedures, documentation requirements, training, and other measures to comply with the HIPAA Rules. This corrective action plan also requires Skagit County to provide regular status reports to OCR.

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at http://www.hhs.gov/ocr/office/index.html.

The Resolution Agreement can be found on the OCR website at:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/skagit-agreement.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: March 7, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
December 26, 2013

Contact: HHS Press Office
(202) 690-6343

Dermatology practice settles potential HIPAA violations

Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services, agreeing to a $150,000 payment. APDerm will also be required to implement a corrective action plan to correct deficiencies in its HIPAA compliance program. APDerm is a private practice that delivers dermatology services in four locations in Massachusetts and two in New Hampshire. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The HHS Office for Civil Rights (OCR) opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and train workforce members.

"As we say in health care, an ounce of prevention is worth a pound of cure," said OCR Director Leon Rodriguez. "That is what a good risk management process is all about – identifying and mitigating the risk before a bad thing happens. Covered entities of all sizes need to give priority to securing electronic protected health information."

In addition to a $150,000 resolution amount, the settlement includes a corrective action plan requiring AP Derm to develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.

To learn more about nondiscrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.HHS.gov/OCR.

The resolution agreement can be found on the OCR website at

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-agreement.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: December 27, 2013

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
August 14, 2013

Contact: Office of Civil Rights
(202) 619-0403

HHS settles with health plan in photocopier breach case

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules for $1,215,780. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

Affinity filed a breach report with the HHS Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information. Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

"This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent," said OCR Director Leon Rodriguez. "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."

In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.

For more information on safeguarding sensitive data stored in the hard drives of digital copiers: http://business.ftc.gov/documents/bus43-copier-data-security. The National Institute of Standards and Technology has issued guidance on media sanitation: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf. OCR offers free training on compliance with the HIPAA Privacy and Security Rules for continuing medical education credit at http://www.medscape.org/sites/advances/patients-rights.

The HHS Resolution Agreement and CAP can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news.*

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: August 14, 2013

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
July 11, 2013

Contact: HHS Press Office
(202) 690-6343

WellPoint pays HHS $1.7 million for leaving information accessible over Internet

The managed care company WellPoint Inc. has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.7 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by WellPoint as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

The report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.

OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule.

The investigation indicated WellPoint did not:

- adequately implement policies and procedures for authorizing access to the on-line application database
- perform an appropriate technical evaluation in response to a software upgrade to its information systems
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

As a result, beginning on Oct. 23, 2009, until Mar. 7, 2010, the investigation indicated that WellPoint impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information.

Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

Beginning Sept. 23, 2013, liability for many of HIPAA's requirements will extend directly to business associates that receive or store protected health information, such as contractors and subcontractors.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The Resolution Agreement can be found on the OCR website at:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: August 5, 2013

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

HHS requires California medical center to protect patients' right to privacy

FOR IMMEDIATE RELEASE
Thursday, June 13, 2013

HHS Press Office
(202) 690-6343

News Release

Shasta Regional Medical Center (SRMC) has agreed to a comprehensive corrective action plan to settle a U.S. Department of Health and Human Services (HHS) investigation concerning potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

The HHS Office for Civil Rights (OCR) opened a compliance review of SRMC following a Los Angeles Times article which indicated two SRMC senior leaders had met with media to discuss medical services provided to a patient. OCR's investigation indicated that SRMC failed to safeguard the patient's protected health information (PHI) from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions, without a valid written authorization. OCR's review indicated that senior management at SRMC impermissibly shared details about the patient's medical condition, diagnosis and treatment in an email to the entire workforce. In addition, SRMC failed to sanction its workforce members for impermissibly disclosing the patient's records pursuant to its internal sanctions policy.

"When senior level executives intentionally and repeatedly violate HIPAA by disclosing identifiable patient information, OCR will respond quickly and decisively to stop such behavior," said OCR Director Leon Rodriguez. "Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected."

In addition to a $275,000 monetary settlement, a corrective action plan (CAP) requires SRMC to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members. The CAP also requires fifteen other hospitals or medical centers under the same ownership or operational control as SRMC to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

The Resolution Agreement can be found on the OCR website at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/shasta-agreement.pdf

# # #

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Idaho State University Settles HIPAA Security Case for $400,000

FOR IMMEDIATE RELEASE
Tuesday, May 21, 2013

HHS Press Office
(202) 690-6343

News Release

Idaho State University (ISU) has agreed to pay $400,000 to the U.S. Department of Health Human Services (HHS) to settle alleged violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The settlement involves the breach of unsecured electronic protected health information (ePHI) of approximately 17,500 patients at ISU's Pocatello Family Medicine Clinic.

ISU operates 29 outpatient clinics and is responsible for providing health information technology systems security at those clinics. Between four and eight of those ISU clinics are subject to the HIPAA Privacy and Security Rules, including the clinic where the breach occurred.

The HHS Office for Civil Rights (OCR) opened an investigation after ISU notified HHS of the breach in which the ePHI of approximately 17,500 patients was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU. OCR's investigation indicated that ISU's risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU also failed to assess the likelihood of potential risks occurring.

OCR concluded that ISU did not apply proper security measures and policies to address risks to ePHI and did not have procedures for routine review of their information system in place, which could have detected the firewall breach much sooner.

"Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program," said OCR Director Leon Rodriguez. "Proper security measures and policies help mitigate potential risk to patient information."

ISU has agreed to a comprehensive corrective action plan to address the issues uncovered by the investigation and its failure to ensure uniform implementation of required HIPAA Security Rule protections at each of its covered clinics.

The Resolution Agreement can be found on the OCR website at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.html

# # #

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
January 2, 2013

Contact: HHS Press Office
(202) 690-6343

HHS announces first HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho settles HIPAA security case for $50,000

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." said OCR Director Leon Rodriguez. "Encryption is an easy method for making lost information unusable, unreadable and undecipherable."

The Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a "breach," of 500 individuals or more to the Secretary of HHS and the media within 60 days after the discovery of the breach. Smaller breaches affecting less than 500 individuals must be reported to the Secretary on an annual basis.

A new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*, has been launched by OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC) that offers health care providers and organizations practical tips on ways to protect their patients' health information when using mobile devices such as laptops, tablets, and smartphones. For more information, visit www.HealthIT.gov/mobiledevices.

The Resolution Agreement can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: August 5, 2013

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
September 17, 2012

Contact: HHS Press Office
(202) 690-6343

Massachusetts provider settles HIPAA case for $1.5 million

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services (HHS) $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. MEEI also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information.

The investigation by the HHS Office for Civil Rights (OCR) followed a breach report submitted by MEEI, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification Rule, reporting the theft of an unencrypted personal laptop containing the electronic protected health information (ePHI) of MEEI patients and research subjects. The information contained on the laptop included patient prescriptions and clinical information.

OCR's investigation indicated that MEEI failed to take necessary steps to comply with certain requirements of the Security Rule, such as conducting a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices, implementing security measures sufficient to ensure the confidentiality of ePHI that MEEI created, maintained, and transmitted using portable devices, adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices, and adopting and implementing policies and procedures to address security incident identification, reporting, and response. OCR's investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule.

"In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices," said OCR Director Leon Rodriguez. "This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom."

In addition to the $1.5 million settlement, the agreement requires MEEI to adhere to a corrective

action plan, which includes reviewing, revising, and maintaining policies and procedures to ensure compliance with the Security Rule. An independent monitor will conduct assessments of MEEI's compliance with the corrective action plan and render semi-annual reports to HHS for a 3-year period.

HHS OCR enforces the HIPAA Privacy and Security Rules, as well as the HITECH Breach Notification Rule. The Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The Security Rule protects health information in electronic form by requiring entities covered by HIPAA to adopt and implement physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure. The HITECH Breach Notification Rule requires covered entities to report a breach of unsecured protected health information to affected individuals, the Secretary, and, in certain circumstances, to the media.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights, or committed another violation of the HIPAA Privacy or Security Rules, may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found on the OCR website at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html.

Additional information about OCR's enforcement activities can be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: April 4, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
June 26, 2012

Contact: News Division
202-690-6343

Alaska settles HIPAA security case for $1,700,000

The Alaska Department of Health and Social Services (DHSS) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $1,700,000 to settle possible violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. Alaska DHSS has also agreed to take corrective action to properly safeguard the electronic protected health information (ePHI) of their Medicaid beneficiaries.

The HHS Office for Civil Rights (OCR) began its investigation following a breach report submitted by Alaska DHSS as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHSS employee. Over the course of the investigation, OCR found evidence that DHSS did not have adequate policies and procedures in place to safeguard ePHI. Further, the evidence indicated that DHSS had not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.

In addition to the $1,700,000 settlement, the agreement includes a corrective action plan that requires Alaska DHSS to review, revise, and maintain policies and procedures to ensure compliance with the HIPAA Security Rule. A monitor will report back to OCR regularly on the state's ongoing compliance efforts.

"Covered entities must perform a full and comprehensive risk assessment and have in place meaningful access controls to safeguard hardware and portable devices," said OCR Director Leon Rodriguez. "This is OCR's first HIPAA enforcement action against a state agency and we expect organizations to comply with their obligations under these rules regardless of whether they are private or public entities."

OCR enforces the HIPAA Privacy and Security Rules. The Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The Security Rule protects health information in electronic form by requiring entities covered by HIPAA to use physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure.

The HITECH Breach Notification Rule requires covered entities to report an impermissible use or

disclosure of protected health information, or a "breach," of 500 individuals or more to the HHS Secretary Sebelius and the media. Smaller breaches affecting less than 500 individuals must be reported to the secretary on an annual basis.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: April 4, 2014

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
April 17, 2012

Contact: HHS Press Office
(202) 690-6343

HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards

Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona, has agreed to pay the U.S. Department of Health and Human Services (HHS) a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients.

The settlement with the physician practice follows an extensive investigation by the HHS Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The incident giving rise to OCR's investigation was a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible. On further investigation, OCR found that Phoenix Cardiac Surgery had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules, and had limited safeguards in place to protect patients' electronic protected health information (ePHI).

"This case is significant because it highlights a multi-year, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules," said Leon Rodriguez, director of OCR. "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity."

OCR's investigation also revealed the following issues:

- Phoenix Cardiac Surgery failed to implement adequate policies and procedures to appropriately safeguard patient information;
- Phoenix Cardiac Surgery failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules;
- Phoenix Cardiac Surgery failed to identify a security official and conduct a risk analysis; and
- Phoenix Cardiac Surgery failed to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.

Under the HHS resolution agreement, Phoenix Cardiac Surgery has agreed to pay a $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: April 4, 2014 .

HHS.gov U.S. Department of Health & Human Services

News

FOR IMMEDIATE RELEASE
March 13, 2012

Contact: HHS Press Office
(202) 690-6343

HHS settles HIPAA case with BCBST for $1.5 million

First enforcement action resulting from HITECH Breach Notification Rule

Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced today. BCBST has also agreed to a corrective action plan to address gaps in its HIPAA compliance program. The enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule.

The investigation followed a notice submitted by BCBST to HHS reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR's investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

"This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program," said OCR Director Leon Rodriguez. "The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients' right to private and secure health information."

In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform monitor reviews to ensure BCBST compliance with the corrective action plan.

HHS Office for Civil Rights enforces the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The HIPAA Security Rule protects health

information in electronic form by requiring entities covered by HIPAA to use physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure.

The HITECH Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a "breach," of 500 individuals or more to HHS and the media. Smaller breaches affecting less than 500 individuals must be reported to the secretary on an annual basis.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pdf.

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Last revised: April 4, 2014

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Resolution Agreement

UCLA Health System Settle Potential Violations of the HIPAA Privacy and Security Rules

Following an investigation by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the University of California at Los Angeles Health System (UCLAHS) has agreed to settle potential violations of the HIPAA Privacy and Security Rules for $865,500 and has committed to a corrective action plan aimed at remedying gaps in its compliance with the rules.

The resolution agreement resolves two separate complaints filed with OCR on behalf of two celebrity patients who received care at UCLAHS. The complaints alleged that UCLAHS employees repeatedly and without permissible reason looked at the electronic protected health information of these patients.

OCR's investigation into the complaints revealed that from 2005-2008, unauthorized employees repeatedly looked at the electronic protected health information of numerous other UCLAHS patients. Through policies and procedures, entities covered under HIPAA must reasonably restrict access to patient information to only those employees with a valid reason to view the information and must sanction any employee who is found to have violated these policies.

"Covered entities are responsible for the actions of their employees. This is why it is vital that trainings and meaningful policies and procedures, including audit trails, become part of the every day operations of any health care provider," said OCR Director Georgina Verdugo. "Employees must clearly understand that casual review for personal interest of patients' protected health information is unacceptable and against the law."

The corrective action plan requires UCLAHS to implement Privacy and Security policies and procedures approved by OCR, to conduct regular and robust trainings for all UCLAHS employees who use protected health information, to sanction offending employees, and to designate an independent monitor who will assess UCLAHS compliance with the plan over 3 years.

"Covered entities need to realize that HIPAA privacy protections are real and OCR vigorously enforces those protections. Entities will be held accountable for employees who access protected health information to satisfy their own personal curiosity," said Director Verdugo.

Additional Information

- Read the Resolution Agreement and CAP
- Read the HHS Press Release

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Resolution Agreement

Massachusetts General Hospital Settles Potential HIPAA Violations

The General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass General) has agreed to pay the U.S. government $1,000,000 to settle potential violations of the HIPAA Privacy Rule.

Mass General, one of the nation's oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. The settlement follows an extensive investigation by OCR.

"We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information," said OCR Director Georgina Verdugo.

The incident giving rise to the agreement involved the loss of protected health information (PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.

This impermissible disclosure involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train. The documents were never recovered.

"To avoid enforcement penalties, covered entities must ensure they are always in compliance with the HIPAA Privacy and Security Rules," said Verdugo. "A robust compliance program includes employee training, vigilant implementation of policies and procedures, regular internal audits, and a prompt action plan to respond to incidents."

Additional Information

- Read the Resolution Agreement and CAP
- Read the HHS Press Release

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Civil Money Penalty

Cignet Health Fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations

The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) has issued a Notice of Final Determination finding that a covered entity, Cignet Health of Prince George's County, MD (Cignet), violated the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS has imposed a civil money penalty (CMP) of $4.3 million for the violations, representing the first CMP issued by the Department for violations of the HIPAA Privacy Rule. The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

"Today the message is loud and clear: HHS is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule and ensuring provider cooperation with our enforcement efforts," said OCR Director Georgina Verdugo.

In a Notice of Proposed Determination issued October 20, 2010 (NPD), OCR found that Cignet violated 41 patients' rights by denying them access to their medical records. These patients, each of whom made a request to obtain their record between September 2008 and October 2009, individually filed complaints with OCR initiating investigations of each complaint. The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The CMP for these violations is $1.3 million.

During the investigations, Cignet refused to respond to OCR's repeated demands to produce the records. Additionally, Cignet failed to cooperate with OCR's investigations of the complaints, including failure to produce the records in response to OCR's subpoena. OCR filed a petition to enforce its subpoena in United States District Court and obtained default judgment against Cignet on March 30, 2010. On April 7, 2010, Cignet produced the medical records to OCR, but otherwise made no efforts to resolve the complaints through informal means.

Covered entities are required under law to cooperate with the Department's investigations. OCR found that Cignet's failure to cooperate with OCR's investigations was due to willful neglect. The CMP for these violations is $3 million.

"Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records, and seriously consider their compliance with all of HIPAA's requirements," said Director Verdugo. "The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules."

Additional Information

- Read the Notice of Final Determination
- Read the Notice of Proposed Determination
- Read the HHS Press Release

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Resolution Agreement

On December 13, 2010, the U.S. Department of Health & Human Services (HHS) entered into a Resolution Agreement with Management Services Organization Washington, Inc. (MSO), to settle potential violations of the Health Information Portability and Accountability Act Privacy and Security Rules. This settlement arose from and was made in coordination with the HHS Office of the Inspector General and the U.S. Department of Justice, which had been investigating MSO for violations of the Federal False Claims Act.

In the agreement, MSO agrees to pay $35,000 and implement a detailed Corrective Action Plan (CAP) to ensure that it will appropriately safeguard identifiable electronic patient information against impermissible use or disclosure. The CAP includes requirements for MSO to develop, maintain, and revise its policies and procedures and to appropriately train its workforce on these policies and procedures. HHS will monitor MSO's compliance with the terms of the CAP and the Privacy and Security Rules for two years.

The Resolution Agreement and CAP relate to MSO's disclosure of electronic protected health information to Washington Practice Management, LLC, owned by MSO, which used the information for marketing purposes. An HHS investigation showed that MSO intentionally did not have in place or implement appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the protected health information.

Read the Resolution Agreement and Corrective Action Plan

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case

Rite Aid Corporation and its 40 affiliated entities have agreed to pay $1 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services (HHS) announced today. In a coordinated action, Rite Aid also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act.

Rite Aid, one of the nation's largest drug store chains, has also agreed to take corrective action to improve policies and procedures to safeguard the privacy of its customers when disposing of identifying information on pill bottle labels and other health information. The settlements apply to all of Rite Aid's nearly 4,800 retail pharmacies and follow an extensive joint investigation by the HHS Office for Civil Rights (OCR) and the FTC.

OCR, which enforces the HIPAA Privacy and Security Rules, opened its investigation of Rite Aid after television media videotaped incidents in which pharmacies were shown to have disposed of prescriptions and labeled pill bottles containing individuals' identifiable information in industrial trash containers that were accessible to the public. These incidents were reported as occurring in a variety of cities across the United States. Rite Aid pharmacy stores in several of the cities were highlighted in media reports.

Disposing of individuals' health information in an industrial trash container accessible to unauthorized persons is not compliant with several requirements of the HIPAA Privacy Rule and exposes the individuals' information to the risk of identity theft and other crimes. This is the second joint investigation and settlement conducted by OCR and FTC. OCR and FTC settled a similar case involving another national drug store chain in February 2009.

The HIPAA Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities), including most pharmacies, to safeguard the privacy of patient information, including such information during its disposal.

Among other issues, the reviews by OCR and the FTC indicated that:

- Rite Aid failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process;
- Rite Aid failed to adequately train employees on how to dispose of such information properly; and
- Rite Aid did not maintain a sanctions policy for members of its workforce who failed to properly dispose of patient information.

Under the HHS resolution agreement, Rite Aid agreed to pay a $1 million resolution amount to HHS and must implement a strong corrective action program that includes:

- Revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;
- Training workforce members on these new requirements;
- Conducting internal monitoring; and
- Engaging a qualified, independent third-party assessor to conduct compliance reviews and render reports to HHS.

Rite Aid has also agreed to external independent assessments of its pharmacy stores' compliance with the FTC consent order. The HHS corrective action plan will be in place for three years; the FTC order will be in place for 20 years.

Additional information:

- Read the Resolution Agreement
- Read the Press Release
- More information about the FTC Consent Order agreement
- Frequently Asked Questions on the Disposal of Protected Health Information

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Resolution Agreement

CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case

In a case that involves the privacy of millions of health care consumers, on January 16, 2009, the U.S. Department of Health & Human Services (HHS) reached agreement with CVS Pharmacy, Inc. to settle potential violations of the HIPAA Privacy Rule. To resolve the Department's investigation of its privacy practices, CVS agreed to pay $2.25 million and implement a detailed Corrective Action Plan to ensure that it will appropriately dispose of protected health information such as labels from prescription bottles and old prescriptions. The new practices will apply to all CVS retail pharmacies, over 6,300 stores. In a coordinated action, CVS Caremark Corporation, the parent company of the pharmacy chain, also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act.

CVS is the largest pharmacy chain in the country. OCR opened its investigation of CVS pharmacy compliance with the Privacy Rule after media reports alleged that protected health information maintained by several retail pharmacy chains was being disposed of in dumpsters that were not secure and could be accessed by the public. At the same time, the FTC opened its investigation of CVS. OCR and the FTC conducted their investigations collaboratively. This is the first instance in which OCR has coordinated investigation and resolution of a matter with the FTC.

The Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities), including pharmacies, to safeguard the privacy of protected health information, including such information during its disposal.

Among other issues, the OCR review indicated that:

- CVS failed to implement adequate policies and procedures to reasonably an d appropriately safeguard protected health information during the disposal process;
- CVS failed to adequately train employees on how to dispose of such information properly; and
- CVS did not maintain and implement a sanctions policy for members of its workforce who failed to comply with its disposal policies and procedures.

Under the Resolution Agreement, CVS agreed to pay a $2,250,000 resolution amount and implement a strong Corrective Action Plan that requires:

1. revising and distributing its policies and procedures regarding disposal of protected health information;
2. sanctioning workers who do not follow them;
3. training workforce members on these new requirements;
4. conducting internal monitoring;
5. engaging a qualified, independent third-party assessor to conduct assessments of CVS compliance with the requirements of the Corrective Action Plan and render reports to HHS;
6. new internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
7. submitting compliance reports to HHS for a period of three years.

Both HHS and FTC require CVS to actively monitor its compliance with the Resolution Agreement and Consent Order. More information about the FTC Consent Order agreement.

Read the Resolution Agreement.

Read the Press Release.

For more information about the HIPAA Privacy Rule requirements for disposal of protected health information, please view our Frequently Asked Questions on the Disposal of Protected Health Information developed to coincide with this enforcement action.

Additional information

- Read the Resolution Agreement
- Read the Press Release
- More information about the FTC Consent Order agreement
- Frequently Asked Questions on the Disposal of Protected Health Information

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

Resolution Agreement

Additional information

- Read the Resolution Agreement
- Read the Press Release

HHS, Providence Health & Services Agree on Corrective Action Plan to Protect Health Information

On July 16, 2008, the U.S. Department of Health & Human Services (HHS) entered into a Resolution Agreement with Seattle-based Providence Health & Services (Providence) to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

In the agreement, Providence agrees to pay $100,000 and implement a detailed Corrective Action Plan to ensure that it will appropriately safeguard identifiable electronic patient information against theft or loss. The Resolution Agreement relates to Providence's loss of electronic backup media and laptop computers containing individually identifiable health information in 2005 and 2006.

A Resolution Agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS for a period of years, typically three years. During the period, HHS monitors the compliance of the covered entity with the obligations it has agreed to perform.

With respect to the HIPAA Privacy and Security Rules, this is the first time HHS has required a Resolution Agreement from a covered entity. Providence's cooperation with OCR and CMS allowed HHS to resolve this case without the need to impose a civil money penalty.

The incidents giving rise to the agreement involved two entities within the Providence health system, Providence Home and Community Services and Providence Hospice and Home Care. On several occasions between September 2005 and March 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the Providence premises and were left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients. HHS received over 30 complaints about the stolen tapes and disks, submitted after Providence, pursuant to state notification laws, alerted patients to the theft. Providence also reported the stolen media to HHS. OCR and CMS together focused their investigations on Providence's failure to implement policies and procedures to safeguard this information.

As a result, Providence agrees to pay a $100,000 resolution amount to HHS and implement a robust Corrective Action Plan that requires: revising its policies and procedures regarding physical and technical safeguards (e.g., encryption) governing off-site transport and storage of electronic media containing patient information, subject to HHS approval; training workforce members on the safeguards; conducting audits and site visits of facilities; and submitting compliance reports to HHS for a period of three years.

Back to Top

Message

From: Tavenner, Marilyn (CMS/OA) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MARILYN.TAVENNER.CMS]
Sent: 10/5/2013 6:08:03 PM
To: Bataille, Julie (CMS/OC) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Julie.GreenBataille.CMS]
CC: Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana .Khalid .CMS]
Subject: Fw: And I should be perfectly clear

Please delete this email-but please see if we can work on call script. [redacted]

----- Original Message -----
From: Lambrew, Jeanne [mailto[redacted]
Sent: Saturday, October 05, 2013 01:55 PM
To: Tavenner, Marilyn (CMS/OA); Jennings, Christopher <[redacted] Hash, Michael (HHS/OHR); Palm, Andrea (HHS/IOS); Park, Todd [redacted]
Cc: Khalid, Aryana C. (CMS/OA)
Subject: RE: And I should be perfectly clear

There may be a problem with the CSR training or script: I tried again. I was told that they could take my information, depending on how complicated my circumstances are and whether they could verification information, it could take 20-30 minutes. When I pushed and asked: I could I enroll without going to the website, I was told no, at some point I would have to create an account on HealthCare.gov.

We are regrouping over here on a process recommendation for discussion to ensure that we are all working off of the same understanding of how things work (like this) and what is going on to prevent confusion, lots of emails and phone calls.

More later.

-----Original Message-----
From: Tavenner, Marilyn (CMS/OA) [redacted]
Sent: Saturday, October 05, 2013 1:28 PM
To: Jennings, Christopher; Lambrew, Jeanne; Hash, Michael (HHS/OHR); Palm, Andrea (HHS/IOS); Park, Todd
Cc: Khalid, Aryana C. (CMS/OA)
Subject: And I should be perfectly clear

There are three things going on here. Those applications we took in a PDF file the first 3 days. 25,000 approx which for all practical purposes look and act like a paper application. They will have to be worked by SERCO and we are doing. Paper applications that are now starting to come in will be worked by SERCO. Website is clear to everyone I believe. It is a matter of the identity proofing and then go all the way through. So let me explain what happened yesterday. We went to on line assistance with folks. Which means that instead of a PDF we can now take their info on line-we can take them all the way through shopping and help them pick a plan. Everyone is doing this but it has been less than one day. We did about 4000 this way. Should these folks want to have this tool on line themselves-then they would create an acct/be identity proofed and then their account would be there for them. Hope this answers your questions and I am available anytime on [redacted]

Cc: Chris Lunt [Redacted]
To: Bryan Sivak [Redacted]
From: Zac Jiwa
Sent: Mon 3/18/2013 1:44:45 PM
Subject: It kept me up last night

I feel like we are not making the "ask". As I work on the script for tomorrow, I don't feel like we are taking the opportunity to express our need. We are telling her that "this is what we are doing", but we are not telling her that there are obstacles to making it happen. Namely, a lack of support by OIS to make it happen or the cloud of vagueness that surrounds their action. At the end of the day, OIS, through its contracts with CGI and QSSI, will have to carry the torch to make this project successful. Chris nor I can do it alone and unless they have "marching orders", I don't see them putting the necessary resources behind it. I grow weary of the bullshit passive/aggressiveness of Henry, or rather his lack of engagement to the point that we can only speculate that it is passive/aggressiveness.

I feel like we should have an "ask", but I don't know whether it is a "do you support and believe that this is the right direction" or if it is a "can you please advise CMS/OIS to make this a priority"? I doubt that she gets into the minutia of the latter, but it feels like there needs to be an absolute directive so that it is crystal clear where we go from here. This needs to go from a pet project of CMCS to a priority component of execution.

The big problem that I see in making our case, though, is that we don't have even a rough estimate of costs for building "MAGI in a Box" because the contractors will not engage in the dialog and we have no idea if the contractors can perform the necessary dev in time. According to "off the record" discussions with QSSI, I don't think the timeline is a major concern.

The other way to do this is through a complete covert ops mission to unseat the CGI FFE rules engine by working with some of the contractors that Chris has been in discussions with to replace the Drools implementation. As much as I like that idea (only because I think CGI/OIS has way over engineered this project), I think we have little chance of pulling off a coup and we do not want to bite off more than we can chew (MAGI is only a piece of the whole). The other idea that we have discussed (I think I shared with you), is to give us $1M to run a developer challenge for an open source "MAGI in a box".

I have digressed...What are you thoughts regarding our "ask" of the Secretary?

Zac

Sent from my mobile device. Expect brevity.

United States Government Accountability Office

Report to Congressional Requesters

September 2014

HEALTHCARE.GOV

Actions Needed to Address Weaknesses in Information Security and Privacy Controls

GAO-14-730

GAO Highlights

Highlights of GAO-14-730, a report to congressional requesters

Why GAO Did This Study

PPACA required the establishment of health insurance marketplaces to assist individuals in obtaining private health insurance coverage. The Department of Health and Human Services' CMS is responsible for overseeing the establishment of these marketplaces, including creating the website for obtaining coverage. The marketplaces became operational on October 1, 2013. As requested, this report examines the security and privacy of the Healthcare.gov website.

GAO (1) describes the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assesses the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov. GAO compared the implementation of controls over Healthcare.gov's supporting systems with privacy and security requirements and guidelines. This is a public version of a limited official use only report that GAO issued in September 2014. Certain information on technical issues has been omitted from this version.

What GAO Recommends

GAO is making six recommendations to implement security and privacy management controls to help ensure that the systems and information related to Healthcare.gov are protected. HHS concurred but disagreed in part with GAO's assessment of the facts for three recommendations. However, GAO continues to believe its recommendations are valid, as discussed in the report.

View GAO-14-730. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

September 2014

HEALTHCARE.GOV

Actions Needed to Address Weaknesses in Information Security and Privacy Controls

What GAO Found

Many systems and entities exchange information to carry out functions that support individuals' ability to use Healthcare.gov to compare, select, and enroll in private health insurance plans participating in the federal marketplaces, as required by the Patient Protection and Affordable Care Act (PPACA). The Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key federal systems supporting Healthcare.gov, including the Federally Facilitated Marketplace (FFM) system, which contains several modules that perform key functions related to health plan enrollment, and the Federal Data Services Hub (data hub), which provides connectivity between the FFM and other state and federal systems. CMS is also responsible for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other federal agencies, including the Department of Defense, Department of Homeland Security, Internal Revenue Service, Office of Personnel Management, Peace Corps, Social Security Administration, and the Department of Veterans Affairs also play key roles in maintaining systems that connect with CMS systems to perform eligibility-checking functions. Finally, a number of commercial entities, including CMS contractors, participating issuers of qualified health plans, agents, and others also connect to the network of systems that support enrollment in Healthcare.gov.

While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain both in the processes used for managing information security and privacy as well as the technical implementation of IT security controls. CMS took many steps to protect security and privacy, including developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. However, Healthcare.gov had weaknesses when it was first deployed, including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions. While CMS has taken steps to address some of these weaknesses, it has not yet fully mitigated all of them. In addition, GAO identified weaknesses in the technical controls protecting the confidentiality, integrity, and availability of the FFM. Specifically, CMS had not: always required or enforced strong password controls, adequately restricted access to the Internet, consistently implemented software patches, and properly configured an administrative network. An important reason that all of these weaknesses occurred and some remain is that CMS did not and has not yet ensured a shared understanding of how security was implemented for the FFM among all entities involved in its development. Until these weaknesses are fully addressed, increased and unnecessary risks remain of unauthorized access, disclosure, or modification of the information collected and maintained by Healthcare.gov and related systems, and the disruption of service provided by the systems.

Contents

Abbreviations

CCIIO	Center for Consumer Information and Insurance Oversight
CHIP	State Children's Health Insurance Program
CMS	Centers for Medicare & Medicaid Services
data hub	Federal Data Services Hub
DHS	Department of Homeland Security
DOD	Department of Defense
FFM	Federally Facilitated Marketplace
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IT	information technology
MIDAS	Multidimensional Insurance Data Analytics System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	privacy impact assessment
PII	personally identifiable information
PPACA	Patient Protection and Affordable Care Act
SSA	Social Security Administration
VA	Department of Veterans Affairs

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 16, 2014

Congressional Requesters

The Patient Protection and Affordable Care Act (PPACA),[1] signed into law on March 23, 2010, is intended to reform aspects of the private health insurance market and expand the availability and affordability of health care coverage. It requires the establishment of a health insurance marketplace[2] in each state[3] to assist consumers and small businesses in comparing, selecting, and enrolling in health plans offered by participating private issuers of qualified health plans. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) is responsible for overseeing the establishment of these marketplaces, including creating a federally facilitated marketplace in states not establishing their own. CMS staff have worked with a variety of contractors to develop, test, and maintain information technology (IT) systems to support the federally facilitated marketplace. Healthcare.gov is the website that provides a consumer portal to these marketplaces and the related data systems supporting eligibility and enrollment.

The security and privacy of personally identifiable information (PII)[4] that is collected and processed by the Healthcare.gov website and supporting IT systems are critically important. Large numbers of individuals submit extensive amounts of sensitive information, such as employment and wage information, portions of which may be accessed by multiple organizations including CMS, other federal agencies, issuers of qualified health plans, and state agencies. Healthcare.gov and other state-based

[1]Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152,124 Stat.1029 (Mar. 30, 2010). In this report, references to PPACA include all amendments made by the Health Care and Education Reconciliation Act.

[2]PPACA requires the establishment of health insurance exchanges—marketplaces where eligible individuals can compare and select among insurance plans offered by participating issuers of health coverage. In this report, we use the term marketplace.

[3]In this report, the term "state" includes the District of Columbia.

[4]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

marketplaces began facilitating enrollment on October 1, 2013. CMS has reported that over 8 million individuals applied for healthcare coverage through a state-based marketplace or the federally facilitated marketplace between October 1, 2013 and March 31, 2014.[5] The Congressional Budget Office has estimated that about 25 million people will enroll by 2022.[6]

Given the high degree of Congressional interest in examining the development, launch, and other issues associated with accessing the federal marketplace through Healthcare.gov, GAO is conducting a body of work in order to assist Congress with its oversight responsibilities. Several GAO reviews are currently underway. You requested that we examine the security and privacy of the Healthcare.gov website and its supporting systems at CMS. Our specific objectives were to (1) describe the planned exchanges of information between the Healthcare.gov website, supporting IT systems, and the federal, state, and other organizations that are providing or accessing the information, including special arrangements for handling tax information in compliance with legal requirements and (2) assess the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov.

This is a public version of a limited official use only report we issued in September 2014. Certain information has been omitted. Although the information provided in this report is more limited in scope, it addresses the same objectives as the limited official use only report. Also, the overall methodology used for both reports is the same.

To describe the planned exchanges of information between Healthcare.gov and federal and state organizations, we reviewed PPACA and other relevant laws to identify the responsibilities of CMS and other federal agencies for establishing and participating in health insurance marketplaces. We reviewed and analyzed CMS system and security documentation, including interagency security agreements, with each

[5]This number includes individuals who enrolled during the special enrollment period through April 19, 2014.

[6]Congressional Budget Office, *Updated Estimates of the Effects of the Insurance Coverage Provisions of the Affordable Care Act, April 2014* (Washington, D.C.: April 2014).

federal partner in order to identify interconnections between Healthcare.gov and other external partners that are providing or accessing information to support implementation of Healthcare.gov. Further, we obtained documentation and interviewed officials at the following federal agencies that are responsible for supporting implementation of Healthcare.gov: the Department of Defense (DOD), the Department of Homeland Security (DHS), the Internal Revenue Service (IRS), the Office of Personnel Management (OPM), the Peace Corps, the Social Security Administration (SSA), and the Department of Veterans Affairs (VA). We also obtained information and interviewed officials at Experian Information Solutions, which provides services to CMS to support Healthcare.gov. Based on an analysis of the information we received, we described the major types of data connections that are currently in place or planned between systems maintained by CMS to support Healthcare.gov and other internal and external systems. We also reviewed requirements in the Internal Revenue Code and PPACA regarding the disclosure of tax return information to carry out marketplace eligibility determinations to describe how IRS and CMS policies and procedures for sharing tax data adhere to legal requirements.

To assess the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov, we compared the CMS's documented policies, procedures, and practices to the provisions and requirements contained in relevant privacy and information security laws and additional security management criteria, specifically National Institute of Standards and Technology (NIST) standards and guidelines. We also assessed the implementation of controls over Healthcare.gov's supporting systems and interconnections by examining risk assessments, security plans, security control assessments, contingency plans, and remedial action plans. Specifically, we observed controls over the Federally Facilitated Marketplace (FFM) system, including its supporting software, the operating systems, network and computing infrastructure provided by the supporting platform as a service, and infrastructure as a service systems. We performed our work at CMS headquarters in Baltimore, Maryland; and at contractor facilities in Dallas, Texas; and Reston and Chantilly, Virginia.

We conducted this performance audit from December 2013 to September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings

and conclusions based on our audit objectives. A full description of our objectives, scope, and methodology can be found in appendix I.

Background

PPACA directed each state to establish a state-based health insurance marketplace by January 1, 2014.[7] These marketplaces were intended to provide a seamless, single point-of-access for individuals to enroll in private health plans, apply for income-based financial assistance established under the law, and, as applicable, obtain an eligibility determination for other health coverage programs, such as Medicaid or the State Children's Health Insurance Program (CHIP).[8]

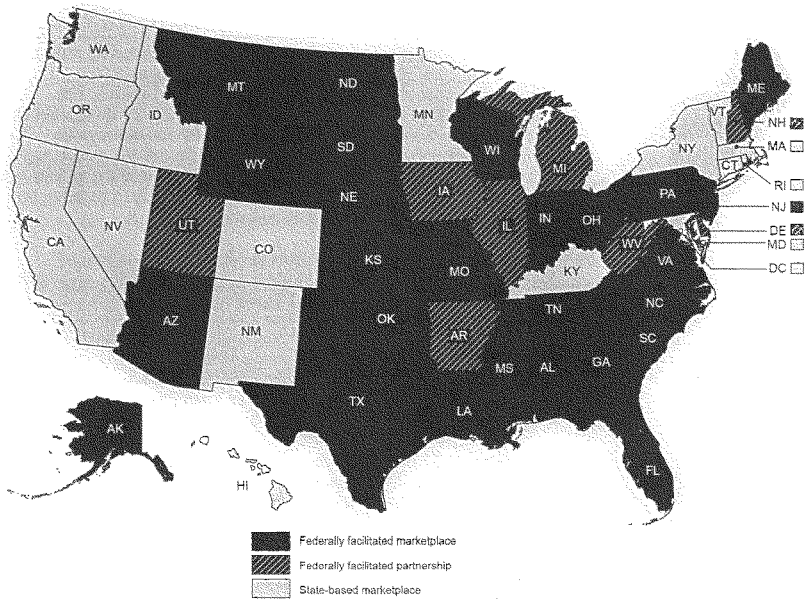
In states electing not to establish and operate a marketplace, PPACA required the federal government to establish and operate a marketplace in that state, referred to as the federally-facilitated marketplace. Thus, the federal government's role for any given state—whether it established a marketplace or oversees a state-based marketplace—was dependent on a state decision. For plan year 2014, 17 states elected to establish their own marketplace, while CMS operated a federally-facilitated marketplace or partnership marketplace[9] for 34 states. Figure 1 shows the states and the types of marketplaces they use.

[7]PPACA, § 1311(b)(1), 124 Stat. at 173.

[8]Medicaid is a joint federal-state program that finances health care coverage for certain low-income individuals. CHIP is a federal-state program that provides health care coverage to children 19 years of age and younger living in low-income families whose incomes exceed the eligibility requirements for Medicaid.

[9]A partnership exchange is a variation of a federally facilitated marketplace. HHS establishes and operates this type of exchange with states assisting HHS in carrying out certain functions of that marketplace.

Figure 1: Type of Health Insurance Marketplace Used by States for Plan Year 2014



Sources: GAO analysis of CMS data; Map Resources (map). | GAO-14-730

PPACA required state and federal marketplaces to be operational on or before January 1, 2014. Healthcare.gov, the public interface for the federally facilitated marketplace, began facilitating enrollments on October 1, 2013, at the beginning of the first annual open enrollment period established by CMS. This open enrollment period closed on March 31, 2014; however the government granted short extensions on an individual basis to those who had begun, but not completed, their application. According to CMS, the extension was granted due to the

volume of applicants. No applications for the initial enrollment period were accepted after April 15, 2014.[10]

Laws and Regulations Set Requirements for Ensuring the Security and Privacy of Personally Identifiable Information

Federal laws and guidance specify requirements for protecting federal systems and data. This includes systems used or operated by a contractor or other organization on behalf of a federal agency. The Federal Information Security Management Act of 2002 (FISMA) requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or another organization on behalf of an agency.

FISMA assigns certain responsibilities to NIST, which is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

Accordingly, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing information security programs. Relevant publications include:

- Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*,[11] requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values

[10]Most state-based marketplaces followed the federal guidelines regarding individuals who started the process before March 30, 2014 but could not finish, allowing applicants to complete the application and select a plan by April 15, 2014. Other states, including Colorado, Nevada, Oregon, and Maryland allowed consumers additional time beyond April 15, 2014, to complete the enrollment process and obtain coverage in 2014.

[11]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: Feb. 2004).

assigned to the respective security objectives are the highest values from among the security categories that the agency identifies for each type of information resident on those information systems.

- Federal Information Processing Standard 200, *Minimum Security Requirements for Federal Information and Information Systems*,[12] specifies minimum security requirements for federal agency information and information systems and a risk-based process for selecting the security controls necessary to satisfy these minimum security requirements.

- Federal Information Processing Standard 140-2, Security *Requirements for Cryptographic Modules*,[13] requires agencies to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. This standard specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments.

- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*,[14] provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The guidance includes privacy controls to be used in conjunction with the specified security controls to achieve comprehensive security and privacy protection.

- NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security*

[12]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[13]NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May, 2001).

[14]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md.: April 2013).

Life Cycle Approach, explains how to apply a risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

- NIST Special Publication 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems* (draft),[15] recommends steps to help develop a more defensible and survivable IT infrastructure—including the component products, systems, and services that compose the infrastructure. While agencies are not yet required to follow these draft guidelines, they establish a benchmark for effectively coordinating security efforts across complex interconnected systems, such as those that support Healthcare.gov.

While agencies are required to use a risk-based approach to ensure that all of their IT systems and information are appropriately secured, they also must adopt specific measures to protect PII and must establish programs to protect the privacy of individuals whose PII they collect and maintain. Agencies that collect or maintain health information also must comply with additional requirements. In addition to FISMA, major laws and regulations[16] establishing requirements for information security and privacy in the federal government include:

- **The Privacy Act of 1974**[17] places limitations on agencies' collection, access, use, and disclosure of personal information maintained in systems of records. The act defines a "record" as any item, collection,

[15]NIST, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, SP 800-160, draft, (Gaithersburg, Md.: May, 2014).

[16]Regulations also establish security and privacy requirements that are applicable to the marketplaces or Healthcare.gov-related contracts. For example, in March 2012, CMS issued a Final Rule regarding implementation of the exchanges (marketplaces) under PPACA and it promulgated a regulation regarding privacy and security standards that marketplaces must establish and follow. See 77 Fed. Reg. 18310, 18444 (March 27, 2012), 45 C.F.R. § 155.260. To ensure that federal contractor-operated systems meet federal information security and privacy requirements, the Federal Acquisition Regulation requires that agency acquisition planning for IT comply with the information technology security requirements in FISMA and addresses application of the Privacy Act to contractors. 48 C.F.R. § 7.103(w), and Subpart 24.1.

[17]5 U.S.C. 552a.

or grouping of information about an individual that is maintained by an agency and contains his or her name or another individual identifier. It defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or other individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice in the Federal Register that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and contest its content.[18]

- **The Computer Matching Act** is a set of amendments to the Privacy Act[19] requiring agencies to follow specific procedures before engaging in programs involving the computerized comparison of records for the purpose of establishing or verifying eligibility or recouping payments for a federal benefit program or relating to federal personnel management. The goal of the amendments was to prevent data "fishing expeditions" that could reduce or terminate benefits without verifying the information and notifying affected individuals of the matching program.

  Under these amendments, referred to as the Computer Matching Act, agencies must establish computer matching agreements with participating agencies that specify, among other things, the purpose and legal authority of the program and a justification for the program, including a specific estimate of any savings. A computer matching agreement ensures that there is procedural uniformity in carrying out computer matches and includes due process rights for individuals whose benefits may be affected.

- **The E-Government Act of 2002**[20] strives to enhance protection for personal information in government information systems by requiring

[18]Under the Privacy Act, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[19]Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (Oct. 18, 1988), as amended by Pub. L. No. 101-56, 103 Stat. 149 (July 19, 1989), and Pub. L. No. 101-508, § 7201, 104 Stat. 1388 (Nov. 5, 1990).

[20]Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (Dec. 17, 2002).

that agencies conduct, where applicable, a privacy impact assessment for each system. This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to the Office of Management and Budget (OMB) guidance, [21] a privacy impact assessment is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. Agencies must conduct a privacy impact assessment before developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form or before initiating any new data collections involving identifiable information that will be collected, maintained, or disseminated using IT if the same questions or reporting requirements are imposed on ten or more people.

- **The Health Insurance Portability and Accountability Act of 1996**[22] establishes national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers, and provides for the establishment of privacy and security standards for handling health information. The act calls for the Secretary of HHS to adopt standards for the electronic exchange, privacy, and security of health information, which were codified in the Security and Privacy Rules.[23] The Security Rule specifies a series of administrative, technical, and physical security practices for "covered

[21]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

[22]Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (Aug. 21, 1996) (codified at 42 U.S.C. §§ 1320d–1320d-9). Additional privacy and security protections, and amendments to the HIPAA Privacy and Security Rules, were established by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, Div. A, Title XIII, 123 Stat. 115, 226-279 and Div. B, Title IV, 123 Stat. 467-496 (Feb. 17, 2009).

[23]The Health Insurance Portability and Accountability Act of 1996 Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164 and were updated at 78 Fed. Reg. 5566 (Jan. 25, 2013) and 79 Fed. Reg. 7290 (Feb. 6, 2014).

entities"[24] and their business associates to implement to ensure the confidentiality of electronic health information. The Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information, such as limiting uses and disclosures to intended purposes, notification of privacy practices, allowing individuals to access their protected health information, securing information from improper use or disclosure, and allowing individuals to request changes to inaccurate or incomplete information. The Privacy Rule establishes a category of health information, called "protected health information," which may be used or disclosed to other parties by "covered entities" or their business associates only under specified circumstances or conditions, and generally requires that a covered entity or business associate make reasonable efforts to use, disclose, or request only the minimum necessary protected health information to accomplish the intended purpose.

- **The Internal Revenue Code (IRC)** provides that tax returns and return information are confidential and may not be disclosed by IRS, other federal employees, state employees, and others having access to the information except as provided in Section 6103.[25] IRC Section 6103 allows IRS to disclose taxpayer information to federal agencies and authorized employees of those agencies for certain specified purposes. It specifies which agencies (or other entities) may have access to tax return information, the type of information they may access, for what purposes such access may be granted, and under what conditions the information will be received. For example, there are provisions in IRC section 6103 that will allow the use of tax information in the determination of eligibility for state, local or federal benefit programs administered by either SSA or various departments of human services or for loan programs under the jurisdiction of the Department of Education. Because the confidentiality of tax data is considered crucial to voluntary compliance, if agencies want to establish new uses of tax information, besides ensuring that executive branch policy requiring a business case to be developed for sharing

[24]"Covered entities" are defined in regulations implementing the Health Insurance Portability and Accountability Act of 1996 as health plans that provide or pay for the medical care of individuals, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations. 45 C.F.R. § 160.103.

[25]26 U.S.C. § 6103.

tax data, Congress must enact enabling legislation to allow the IRS to disclose the information necessary to meet the agency's needs.

- **IRS Publication 1075** establishes tax information security guidelines for safeguarding federal tax return information used by federal, state and local agencies. This publication provides guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS. The guide details security controls, reporting, record keeping and access control requirements that are aligned with IRS standard practices to meet the requirements of IRC Section 6103.

HHS has Established Responsibilities for Overseeing Implementation of PPACA and Ensuring the Security and Privacy of Health Insurance Marketplaces

Under FISMA, the Secretary of HHS has the overall responsibility for implementing an agencywide information security program to ensure compliance with all governmentwide legal and policy requirements. That responsibility has been delegated to the HHS Chief Information Officer, who is responsible for ensuring the development and maintenance of a departmentwide IT security and privacy program to include the development and implementation of policies, standards, procedures, and IT security controls resulting in adequate security for all organizational information systems and environments of operation for those systems, including Healthcare.gov. The HHS Chief Information Officer is also responsible for establishing, implementing, and enforcing a departmentwide framework to facilitate an incident response program and the development of privacy impact assessments for all department systems.

The CMS Center for Consumer Information and Insurance Oversight (CCIIO) has overall responsibility for the federal systems supporting the establishment and operation of the federally-facilitated marketplace as well as for overseeing state marketplaces.[26] More specifically, CCIIO develops and implements policies and rules governing state-based marketplaces, oversees the implementation and operations of state-based marketplaces, and administers federally-facilitated marketplaces for states that elect not to establish their own.

[26]HHS established the Office of Consumer Information and Insurance Oversight in April 2010 as part of the HHS Office of the Secretary. In January 2011, the office moved to CMS and became CCIIO.

Security and privacy responsibilities for Healthcare.gov and its supporting systems are shared among several offices within CMS. The CMS Chief Information Officer is responsible for implementing and administrating the CMS information security program, which covers the systems developed by CMS to satisfy PPACA requirements. The Chief Information Officer is the designated approving authority for all CMS information systems and develops and implements CMS-specific policies and procedures that implement requirements in FISMA as well as HHS and other governmentwide security directives.

The CMS Chief Information Security Officer is responsible for ensuring the assessment and authorization of all systems, and the completion of periodic risk assessments, including annual security testing and security self-assessments. In addition, the Chief Information Security Officer is responsible for disseminating information on potential security threats and recommended safeguards and for establishing, documenting, and enforcing security requirements and processes for granting and terminating administrative privileges for servers, security domains, local workstations, and other information assets. Furthermore, Chief Information Security Officer responsibilities include supporting the CMS Senior Official for Privacy in documenting and managing privacy implementation in CMS IT systems, and collaborating with the CMS Chief Information Officer to help make security-related risk determinations.

Within component organizations of CMS, individual Information Systems Security Officers have been established to oversee security issues that arise in the development and implementation of specific systems. The Information Systems Security Officer within the CMS Office of e-Health Standards Privacy Policy and Compliance serves as the principal advisor to CCIIO on matters involving the security of information systems developed by CMS in support of Healthcare.gov. Information Systems Security Officer responsibilities include serving as a focal point for information security and privacy incident reporting and resolution, ensuring that standard information security requirements are included in contracts, ensuring that information security notices and advisories are distributed to appropriate CMS and contractor personnel, and ensuring that vendor-issued security patches are expeditiously installed.

The CMS Senior Official for Privacy is responsible for coordinating as the lead, in collaboration with the CMS Chief Information Security Officer, in developing and supporting integration of department privacy program initiatives into CMS information security practices. This includes establishing a CMS policy framework to facilitate the development and

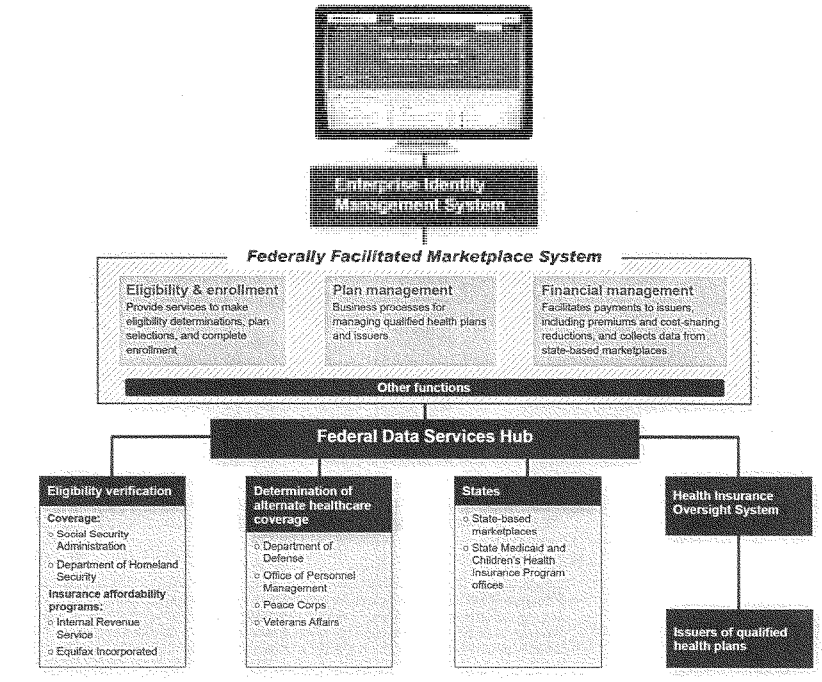
maintenance of privacy impact assessments for all systems, reviewing completed assessments, and attesting that they have been completed adequately and accurately.

The CMS Office of e-Health Standards Privacy Policy and Compliance is the principal authority for the management and oversight of CMS' Privacy Act duties. The CMS Privacy Officer's responsibilities include developing policy, providing program oversight, reviewing new and existing CMS policies, procedures, program memoranda, interagency agreements, and other written arrangements that may have an impact on the personal privacy of an individual, advising and assisting with the development and coordination of computer matching agreements between CMS components and other federal or state agencies, and reviewing and coordinating Privacy Act system of records notices and computer matching agreements.

CMS Exchanges Data with Many Interconnected Systems and External Partners to Facilitate Marketplace Enrollment

PPACA requires that CMS and the states establish automated systems to facilitate the enrollment of eligible individuals in appropriate healthcare coverage. Many systems and entities exchange or plan to exchange information to carry out this requirement. CCIIO has overall responsibility for the federal systems supporting Healthcare.gov and for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other federal agencies also play a role in maintaining systems that connect with the CMS systems to perform eligibility-checking functions. Finally, a number of private entities, including CMS contractors, participating issuers of qualified health plans, agents, and others also connect to the network of systems that support enrollment in Healthcare.gov. Figure 2 shows the major entities that exchange data in support of marketplace enrollment in qualified health plans and how they are connected.

Figure 2: Overview of Healthcare.gov and its Supporting Systems



Source: GAO analysis of CMS data. | GAO-14-730

PPACA directed the creation of exchanges, commonly referred to as "marketplaces," which are intended to facilitate a seamless eligibility and enrollment process through which a consumer submits a single application and receives an eligibility determination for enrollment into private marketplace insurance plans, known as qualified health plans, and

income-based financial subsidies to defray the cost of qualified health plan coverage,[27] and, if applicable, coverage under Medicaid, and CHIP.

PPACA required that marketplaces be operational in each state by January 1, 2014. States could choose to establish and operate their own state-based marketplace or have their residents use the federally-facilitated marketplace.[28] Regardless of whether a state established and operated its own marketplace or used the federally-facilitated marketplace, all marketplaces had to be equipped to carry out two key functions: eligibility and enrollment functions to assess and determine an individual's eligibility for enrollment and enroll eligible individuals in coverage and plan management processes to certify private health insurance plans for participation in the marketplace. Further, the federally-facilitated marketplace is equipped to handle financial management processes to facilitate payments to health insurers. In addition, each marketplace was to provide assistance to consumers in completing an application, obtaining eligibility determinations, comparing coverage options, and enrolling in coverage.

Several Major CMS Systems Support Enrollment-related Activities

The FFM system contains several modules that perform key functions related to obtaining healthcare coverage. In addition to the FFM, CMS operates a system known as the Federal Data Services Hub (data hub), which provides connectivity between the FFM and other state and federal systems. Within CMS, the Office of Information Services/Consumer Information and Insurance Systems Group is tasked with technical oversight of the development and implementation of the FFM and the data hub. Several other CMS systems also play a specific role in the

[27]Insurance affordability programs include the advance premium tax credit and cost-sharing reductions. The advance premium tax credit is available on an advance basis, and advance payment of the premium tax credit is reconciled on a tax filer's tax return. The credit is generally available to eligible tax filers and their dependents that are (1) enrolled in one or more qualified health plan through a marketplace and (2) not eligible for other health insurance coverage that meets certain standards. Cost sharing generally refers to costs that an individual must pay when using services that are covered under the health plan that the person is enrolled in. Common forms of cost sharing include copayments and deductibles.

[28]Through subsequent guidance, HHS identified options for states to partner with HHS when HHS establishes and operates an exchange. Specifically, under this model, states may assist HHS in carrying out certain functions of the exchanges, namely plan management and consumer assistance.

enrollment process, including the Enterprise Identity Management System, the Multidimensional Insurance Data Analysis System, the Health Insurance Oversight System, and the Health Insurance General Ledger. These systems are discussed in further detail later in this report.

Healthcare.gov Website

Healthcare.gov is the federal website that serves as the user interface for obtaining coverage through the FFM. Individuals can use the website to obtain information about health coverage, set up a user account, select a health plan, and apply for coverage. The site supports two major functions: providing information about PPACA health insurance reforms and health insurance options (the "Learn" web page) and facilitating enrollment in coverage (the "Get Insurance" web page). The "Learn" page provides basic information on how the marketplace works, how to apply for coverage, and available health plans. It also contains information on plan costs, ways to reduce out-of-pocket costs, and how consumers can protect themselves from fraud. Individuals do not have to provide PII to access this section of the website. In contrast to the information-oriented "Learn" page, the "Get Insurance" page allows a consumer to take steps to apply for health insurance and other associated benefits. In order to do so, a consumer must obtain a login account and prove his or her identity.

Enterprise Identity Management System

Before an individual can apply for health coverage or other benefits, CMS must verify his or her identity to help prevent unauthorized disclosure of PII. The process of verifying an applicant's identity and establishing a login account is facilitated by CMS' Enterprise Identity Management System. The system is intended to provide identity and access management services to protect CMS data while ensuring that users are identity-proofed and only authorized users are allowed and capable of accessing CMS resources.

To create a login account, the applicant provides a name and e-mail address and creates a password. Once an account has been created, the identity is confirmed using additional information, which may include Social Security number, current address, phone number, and date of birth. This information is transferred to Experian Information Solutions, Inc., a CMS contractor, which matches the information against its records.

In order to verify an applicant's identity, Experian must pull the applicant's credit profile to generate questions for the applicant. Experian's authority to receive PII and access the applicant's credit profile is stated in the terms of use of the Marketplace, and is granted by the applicant before the application process begins. The PII involved includes the applicant's

name, Social Security number (when provided), current address, phone number, and date of birth.

Experian's Remote Identity Proofing service verifies the applicant's identity using an application that interacts directly with the Enterprise Identity Management System. During the applicant registration process, the Enterprise Identity Management System sends the applicant's information to the Remote Identity Proofing service to match the information against Experian's records. A series of questions are then generated based on the applicant's information on file at Experian, and the applicant's responses are used to establish the identity of the person requesting the account. If an applicant fails the identity proofing process online, they must contact Experian's call center to take further steps to confirm their identity. If the applicant's identity cannot be confirmed via the call center, a manual review of documentation proving the applicant's identity is to be conducted by a separate contractor.

The Enterprise Identity Management System was developed by Quality Software Services, Inc. and made available for use on October 1, 2013, to support the 2014 health coverage enrollment season, which extended from October 1, 2013, through March 31, 2014.[29]

Federally Facilitated Marketplace System

The core of the FFM is a transactional database that was originally developed by CGI Federal, Inc., and since January 2014 has been further developed and maintained by Accenture, Inc. The FFM is intended to facilitate the eligibility verification process, enrollment process, plan management, financial management services, and other functions, such as quality control and oversight. It consists of three major modules: eligibility and enrollment, plan management, and financial management.

- **Eligibility and enrollment module**. Residents of states that operate their own state-based marketplaces enroll in healthcare plans via those marketplaces, which will be discussed subsequently. All others use the eligibility and enrollment module of the FFM system, which is intended to guide applicants through a step-by-step process to determine his or her eligibility for coverage and financial assistance, after which he or she is shown applicable coverage options and has the opportunity to enroll.

[29]The Enterprise Identity Management System is a CMS enterprisewide system that was not developed solely to support the FFM.

For the eligibility determination process, an applicant is asked questions on citizenship or immigration status, income, residency, and incarceration status. In each case, the applicant is asked a series of questions tailored to the responses he or she provides. PII asked of applicants generally includes:

- First, middle, and last name
- Date of birth
- Social Security number
- Ethnicity (optional)
- Home address (including city, state, county, and zip code)
- Phone number
- Citizenship or immigration status
- Employer name and address

Applicants requesting financial assistance answer additional questions regarding income to determine eligibility for advance payments of the premium tax credit and cost-sharing reductions, and assess or determine for potential eligibility for Medicaid and CHIP programs. This information includes:

- Wage and other income amounts
- Tax deduction amounts
- Information on existing health coverage enrollment

Throughout the eligibility and enrollment process, the applicant's information is collected and stored in the FFM's database and compared with records maintained by other federal agencies and other private entities to determine whether an applicant is eligible to enroll in a qualified health plan and, if so, to receive advance payments of the premium tax credit and cost-sharing reductions to defray the cost of this coverage. As part of this process, the system performs checks with other federal agencies to determine whether an applicant is eligible for coverage or benefits through other federal programs or agencies, such as the Federal Employee Health Benefits program or the VA.

Once a complete eligibility determination has been made, the FFM allows an applicant to view, compare, select, and enroll in a qualified health plan. Options are displayed to the applicant on the Healthcare.gov webpage, and applicants can use the "Plan Compare" function to view and compare plan details. The applicant can customize and filter the plans by plan type, premium amount, maximum out-of-pocket expenses, deductible, availability of cost-

sharing reductions, or insurance company. Once an applicant has signed up for a qualified health plan on Healthcare.gov, the FFM relays information about the enrollment to the chosen health plan.

The eligibility and enrollment module was developed and made available for public use beginning October 1, 2013, to support the 2014 health coverage enrollment season.

- **Plan management module**. While the eligibility and enrollment module supports individual applicants, the plan management module is intended to interact primarily with state agencies and issuers of qualified health plans. Specifically, the plan management module is intended to provide a suite of services for submitting, certifying, monitoring, and renewing qualified health plans, as well as managing their withdrawal. This module allows states and issuers to submit "bids" detailing proposed health plans to be offered on Healthcare.gov, including rate and benefits information. CMS personnel use the system to review, monitor, and certify or decertify the bids submitted by issuers. Once a bid has been approved, it is made available on Healthcare.gov. Like the eligibility and enrollment module, the plan management module uses a MarkLogic database.

  The plan management module was not operational during the initial 2014 enrollment period that began October 1, 2013. According to CMS officials, development and implementation of the module has occurred in incremental updates, and basic functionality, such as the ability to submit information about a proposed health plan for review by CMS, was intended to become available in the second quarter of 2014 for use during the 2015 enrollment period that begins November 15, 2014.

- **Financial management module**. Like plan management, the financial management module interacts primarily with issuers of qualified health plans. The module is intended to facilitate payments to health insurers through transactions based on the Electronic Data Interchange protocol.[30] Additional services include payment calculation for reinsurance, risk adjustment analysis, and the data

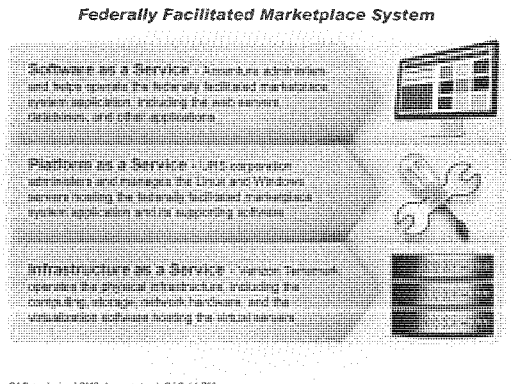
[30]The Electronic Data Interchange protocol establishes uniform data requirements and content that support standards such as the American National Standards Institute standard ASC X12, Benefit Enrollment and Maintenance (834), which is used to transfer enrollment information from a qualified health plan issuer to an applicant.

collection required to support these services. Transactions to be supported by the module include payments of premiums and cost-sharing reductions for individual enrollments, reinsurance, and risk adjustments.

Like the plan management module, the financial management module was not operational during the 2014 enrollment period. According to CMS officials, development and implementation of the module is occurring in incremental updates scheduled to be implemented throughout 2014. Functionality to support payments to insurers covering cost-sharing reductions and the advance premium tax credit was scheduled for the second quarter of 2014.

From a technical perspective, the FFM leverages data processing and storage resources that are available from private sector vendors over the Internet, a type of capability known as cloud-based services. The functionality provided by the system exists in several "layers" of services, including infrastructure as a service, platform as a service, and software as a service. Figure 3 depicts how the FFM is deployed across cloud service layers.

Figure 3: High-level Architecture of FFM System and Supporting Infrastructure



Source: GAO analysis of CMS documents. | GAO-14-730

- **Infrastructure as a service** — the service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment upon which a platform (i.e., operating system and programming tools and services) to develop and execute applications can be developed by the customer. Verizon Terremark provides this service for CMS, which includes helping CMS operate the data center, managing the physical computing and network hardware, and administering the virtualization software, on top of which run the operating systems.

- **Platform as a service** — the service provider delivers and manages the underlying infrastructure (i.e., servers, software, storage, and network equipment), as well as the platform (i.e., operating system, and programming tools and services) upon which the customer can create applications using programming tools supported by the service provider or other sources. URS Corporation, a subcontractor to Verizon Terremark, provides this service for CMS, acting as the Windows and Linux administrators for the virtual servers on top of which the FFM application runs.

- **Software as a service** — runs on a software platform and infrastructure managed by other vendors and delivers a complete application, such as the Healthcare.gov website, that individuals interact with when applying for healthcare coverage. CGI Federal originally designed, developed, and assisted with the operation of the FFM for CMS, but in January 2014 Accenture took over as the system's operator. Accenture's responsibilities include administering the web servers, databases, and applications running on top of the application operating system, as well as operating some security appliances that provide security controls for the FFM applications.

Federal Data Services Hub

The data hub is a CMS system that acts as a single portal for exchanging information between the FFM and CMS's external partners, including other federal agencies, state-based marketplaces, other state agencies, other CMS systems, and issuers of qualified health plans. The data hub was developed under contract by Quality Software Services, Inc., and made available for use on October 1, 2013, to support the 2014 health coverage enrollment season, which extended from October 1, 2013,

through March 31, 2014. The data hub was designed as a "private cloud" service[31] supporting the following primary functions:

- **Real-time eligibility queries**. The FFM, state-based marketplaces, and Medicaid/CHIP agencies transmit queries to various external entities, including other federal agencies, state agencies, and commercial verification services to verify information provided by applicants, such as immigration and citizenship data, income data, individual coverage data, and incarceration data.
- **Transfer of application information**. The FFM or a state-based marketplace transfers application information to state Medicaid/CHIP agencies. Conversely, state agencies also use the data hub to transfer application information to the FFM.
- **Transfer of taxpayer information**. The IRS transmits taxpayer information to the FFM or a state-based marketplace to support the verification of household income and family size when determining eligibility for advance payments of the premium tax credit and cost-sharing reductions
- **Exchange of enrollment information with issuers of qualified health plans**. The FFM sends enrollment information to appropriate issuers of qualified health plans, which respond with confirmation messages back to CMS when they have effectuated enrollment. State-based marketplaces also send enrollment confirmations, which CMS uses to administer the advance premium tax credit and cost-sharing reductions and to track overall marketplace enrollment.
- **Monitoring of enrollment information**. CMS, issuers of qualified health plans, and state-based marketplaces exchange enrollment information on a monthly basis to reconcile enrollment records.
- **Submission of health plan applications**. Issuers of qualified health plans submit "bids" for health plan offerings for validation by CMS.

[31]Although exact definitions vary, cloud computing can, at a high level, be described as a form of computing where users have access to scalable, on-demand IT capabilities that are provided through Internet-based technologies. A private cloud is operated solely for a single organization and the technologies may be on or off the premises.

To support these functions, each entity establishes Web services[32] that are used by the data hub for exchanging data with them. The data hub determines which entity has the data needed to answer a request from the FFM or a state-based marketplace during the application process. The data hub may connect with multiple data sources to provide a single answer to a request, which it provides in real-time, in a standard format.

Connections between external entities and the data hub are made through an Internet protocol that establishes an encrypted system-to-system web browser connection. Encryption of the data transfer between the two entities is designed to meet NIST standards, including Federal Information Processing Standard 140-2.[33] This type of connection is intended to ensure that only authorized systems can access the data exchange, thus safeguarding against cyber attacks attempting to intercept the data.

The data hub is designed to not retain any of the data that it transmits in permanent storage devices, such as hard disks. According to CMS officials, data is stored only momentarily in the data hub's active memory. The entities that transmit the data are responsible for maintaining copies of their transmissions in case the data needs to be re-transmitted. As a result, CMS does not consider the data hub to be a repository of personally identifiable information.[34]

Other CMS Systems

Several other CMS systems also support Healthcare.gov-related activities, including:

[32]Web services are client and server applications that communicate over the World Wide Web's HyperText Transfer Protocol. Web services provide a standard means of interoperating between software applications running on a variety of platforms and frameworks.

[33]Agencies are required to encrypt agency data, where appropriate, using NIST-certified cryptographic modules. FIPS 140-2 specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) and provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md: May, 2001).

[34]In terms of the Privacy Act of 1974, CMS has determined that the data hub is not a system of records subject to the act's provisions.

- **Multidimensional Insurance Data Analytics System (MIDAS)**. This is a data warehouse system that is intended to provide reporting and performance metrics related to the FFM and other Healthcare.gov-related systems. The system offers several pre-defined reports, which are generated upon request and contain aggregated information about enrollments. According to CMS officials, the MIDAS system has been operational since before the beginning of the first enrollment period in October 2013.

- **Health Insurance Oversight System**. The system is intended to provide an interface for issuers of qualified health plans to submit information about qualified health plans. This information is to be transmitted to the plan management module of the FFM once that module is operational. According to CMS officials, the system serves a security function by keeping issuers of qualified health plans from having to connect directly with the FFM.

- **Health Insurance General Ledger**. The system is a longstanding internal CMS accounting system that handles payments and financial collections, including payments associated with the advance premium tax credit and cost-sharing reductions.

Many External Partner Entities Connect with the FFM and Data Hub

CMS relies on a variety of federal, state, and private-sector entities to support its Healthcare.gov-related activities, including other federal agencies, state-based marketplaces and supporting systems, issuers of qualified health plans, and agents and brokers.

Federal agencies and private entities assisting in making determinations for eligibility and financial assistance

Several federal agencies and one commercial verification service connect with the FFM and data hub to obtain and compare applicant data with their records to help CMS determine applicants' eligibility for coverage in a qualified health plan and for insurance affordability programs.[35] These entities include SSA, DHS, IRS, and Equifax, Inc.

- **Social Security Administration**. SSA's primary role is to assist CMS in confirming applicant-supplied information by comparing it with citizenship, Social Security number, death records, and incarceration

[35]To be eligible to enroll in a qualified health plan offered through a marketplace, an individual must be a U.S. citizen or national, or otherwise lawfully present in the United States, reside in the marketplace service area, and not be incarcerated (unless jailed while awaiting final disposition).

status maintained by SSA. This information is used to determine eligibility for enrollment in marketplace coverage. In addition to confirming citizenship data, death records, and incarceration status, SSA confirms disability benefits information to assist CMS in determining an applicant's qualification for insurance affordability programs, such as the advance premium tax credit, cost-sharing reductions, Medicaid, CHIP, and exemptions from the individual responsibility requirement. [36]

In order to assist CMS in confirming citizenship and whether identification information provided by an applicant corresponds to a deceased individual, SSA matches and validates data provided by applicants, including Social Security number, name, and date of birth with its internal systems, including the Master Files of Social Security Number Holders and Social Security Applications, which contains name, date of birth, place of birth, parents' names, citizenship status, date of death (if applicable) and associated Social Security number. The result is then sent to CMS to assist in making a determination of eligibility.

When requested by CMS, SSA provides incarceration status from its Prisoner Update Processing System. Incarceration status is verified for applicants who have attested that they are not currently incarcerated. Verification may occur for applicants to Medicaid and CHIP programs as well as qualified health plans under PPACA. The PII involved includes the applicant's Social Security number, name, and date of birth. If a positive incarceration status is identified, SSA transmits the relevant prisoner identification number, date of confinement, facility type, and contact information to CMS for use in determining eligibility.

Further, when requested by CMS, SSA provides monthly and annual Social Security Act benefit information and Social Security Act disability information from its Master Beneficiary Record database to CMS for determination or assessment of an applicant's eligibility to participate in insurance affordability programs. The information provided includes a disability indicator, current benefit status, and

[36]PPACA requires individuals to maintain health coverage that meets certain minimum requirements and imposes penalties on those who do not do so unless they have been granted an exemption from the requirement.

quarters of coverage. SSA may also provide information to CMS on monthly or annual benefits received by the applicant.

- **Department of Homeland Security**. DHS verifies the naturalized, acquired, or derived citizenship or immigration status of applicants as needed by CMS. DHS generally undertakes this verification only if CMS is unable to verify an applicant's status with SSA using a Social Security number or if the applicant indicates he or she is not a U.S. citizen on the application. In addition, DHS verifies the status of non-citizens who are lawfully present in the U.S. and seeking eligibility to enroll in a qualified health plan or participate in Medicaid, CHIP, or a state-based health plan as well as current beneficiaries who have had a change in immigration status or whose status may have expired. Within DHS, U.S. Citizenship and Immigration Services is responsible for verifying immigration status based on immigration status-related information provided by CMS, where appropriate, to assist CMS with its eligibility determination. Verification can be performed at any point during the benefit year and involves an initial electronic query and potentially two additional verification steps, if needed.

  The Systematic Alien Verification for Entitlements program accesses immigrant, non-immigrant, and derived and naturalized citizen status information from federal immigration databases through the Verification Information System. Initially, DHS attempts to verify status based on an applicant's immigration identification number, name, date of birth, and immigration document type using an automated verification process. If DHS cannot verify the status with this information alone, then it will prompt CMS to request additional information, at which time DHS will manually research the case. If DHS is still unable to verify the status, it will prompt CMS to submit copies of the applicant's immigration documents and a completed DHS Document Verification Request form to DHS for a final attempt to verify status. The verified immigration status or naturalized, acquired, or derived citizenship information is then transmitted through the data hub to the FFM to support eligibility and enrollment determination.

- **Internal Revenue Service**. IRS's role is to provide federal tax information to be used by CMS to determine or assess income and determine an applicant's eligibility for insurance affordability programs, including the advance premium tax credit, cost-sharing reductions, Medicaid, and CHIP. The IRS also provides an optional service for CMS to use in calculating the maximum amount of advance payments of the premium tax credit, which an eligible

applicant can elect to receive for assistance in paying monthly premiums.

In order to perform these functions, the IRS matches the applicant's Social Security number with tax return information and provides CMS with the applicant's Social Security number, family size, filing status, modified adjusted gross income, taxable year, and any other items authorized pursuant to the Internal Revenue Code. CMS may initiate this process by either an individual request or a bulk request.

The IRS Customer Account Data Engine supports this process. The data engine maintains records of tax returns, return transactions, and authorized taxpayer representatives. This system extracts and transmits tax return data to the CMS FFM, which then gives the applicant an opportunity to resolve any inconsistencies between the attestation and the matched IRS tax return information.

The IRS Advance Premium Tax Credit Computation Engine is then used by CMS to calculate the maximum allowable amount of the advance payments of the premium tax credit and also to calculate the remainder of the household contribution.[37] In order to calculate these amounts, the computation engine uses information about household income, the corresponding federal poverty level, family size, state of residency, and the cost to the applicant of subscribing to a qualified health plan. The IRS does not retain information about the applicant once it has sent the results to the FFM. IRS and CMS are to retain the raw data they exchange only to provide calculation results and perform IT integrity checks. CMS also retains a record of the amount of the advance payment of the premium tax credit that the applicant chooses to accept.

- **Equifax, Inc.** Equifax's role is to verify information about an applicant's current income and employment to assist CMS in making a determination about an applicant's qualification for insurance affordability programs, such as the advance premium tax credit and cost-sharing reductions. Specifically, according to CMS, the FFM sends an applicant's name, Social Security number, and date of birth

[37]Treasury Inspector General for Tax Administration, *Affordable Care Act: Improvements Are Needed to Strengthen Systems Development Controls for the Premium Tax Credit Project*, 2013-23-119 (Washington, D.C.: Sept. 27, 2013).

through the data hub to the Equifax Workforce Solutions Data Center, using an Equifax web service interface.

When it receives a request, Equifax searches for an exact match of the Social Security number supplied in the request and calculates a confidence score based upon additional information (name and date of birth) in the request. If the confidence score is above a threshold agreed upon with CMS and all required data elements are present, Equifax returns income and employment verification information (including employee and employer identification, employment status, base compensation, annual compensation, and pay period information) through the data hub to be used by CMS in determining eligibility for insurance affordability programs.

Federal agencies determining whether alternate healthcare coverage is available

Several additional federal agencies connect with the FFM and data hub to support CMS in determining whether a potential applicant has alternative means for obtaining minimum essential coverage[38] and therefore may not be eligible to receive the advance premium tax credit and cost-sharing reductions. For example, applicants could have minimum essential coverage if they are enrolled in a government program, such as Medicare or Medicaid, or certain employer-sponsored programs, such as the Federal Employees Health Benefits program. Those agencies responsible for determining if an applicant has minimum essential coverage include the following:

- **Department of Defense**. DOD's role is to verify the applicant's eligibility for TRICARE, the department's health care system for active duty military personnel and their families. DOD maintains TRICARE coverage information for all enrollees and beneficiaries within DOD. This information is matched by CMS to determine if an individual has minimum essential coverage.

  The Defense Manpower Data Center provides data used to determine TRICARE eligibility, enrollment, and medical claims payments via the Defense Enrollment Eligibility Reporting System. DOD initiates the verification process in the system once it receives a request from CMS with applicant data, including Social Security number, name,

[38]Minimum essential coverage includes health plans such as individual market health plans, eligible employer-sponsored health plans (if they meet affordability and quality standards), or government-sponsored health coverage such as Medicare, Medicaid, and the Children's Health Insurance Program. See 26 U.S.C. § 5000A(f).

date of birth, gender, and requested qualified health plan effective coverage start and end date. DOD determines if the individual is a beneficiary and if so, it responds to the verification request with the insurance end date (if TRICARE coverage has lapsed), Social Security number ID, and response code to verify the status of an individual's TRICARE coverage.

- **Office of Personnel Management**. OPM's role is to provide health insurance coverage data to CMS for federal employees so that CMS can determine if an individual has minimum essential coverage.

  CMS performs the matching function itself, using a data file provided periodically by OPM. OPM transmits this data file to CMS on a monthly basis that contains coverage information of all employees who receive health benefits through the federal government. In addition to the personnel data file, OPM also sends an annual premium index file that contains information on the costs of health plans available to federal employees.

  OPM's Enterprise Human Resources Integration office relies on its Statistical Data Mart to support this function. The Statistical Data Mart transmits a file via a secure private link to the CMS Data Center, which then routes the file through the data hub to the FFM. The file contains Social Security number, name, gender, date of birth, employment data, and health plan coverage information for all federal employees who have employer-sponsored coverage.

- **Peace Corps**. The Peace Corps' role is similar to OPM's. It provides CMS with information on active Peace Corps volunteers to facilitate verification of an applicant's coverage under the Peace Corps' volunteer health benefits program. The Peace Corps is responsible for providing medical care to all Peace Corps volunteers throughout their service, and such medical care is considered minimum essential coverage.

  The Peace Corps sends a data file to CMS containing information on all current volunteers five times per week. The information is based on the agency's Volunteer Applicant and Service Records system, which includes records of current and former Peace Corps volunteers, trainees, and applicants for volunteer service, including Peace Corps United Nations volunteers. The file includes all volunteers and trainees who have received health benefits in the previous three calendar months. Although the volunteer's Social Security number and eligibility start date are the only PII required to verify coverage,

the Peace Corps sends additional data elements, including name, gender, date of birth, eligibility end date for those who are no longer in service, and projected end date for those still in service, in case that information is needed to handle specific CMS queries.

- **Department of Veterans Affairs**. VA's role is to validate the existing coverage of VA health beneficiaries so CMS can determine if an individual has minimum essential coverage. The Veterans Health Administration within VA is responsible for this process.

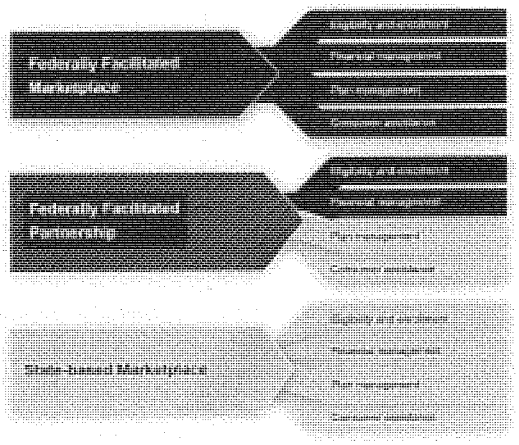
  In order to verify existing coverage, VA matches applicant information to Veterans Health Administration's Health Care Program beneficiary records. CMS requests data from VA's records only when it is necessary to determine if an individual has minimum essential coverage. The PII matched includes: Social Security number, name, gender, date of birth, requested qualified health plan effective coverage date, and requested qualified health plan end date.

  VA relies on records from the Veterans Information & Eligibility Reporting Services system, which gathers and catalogs data from various sources, applications, and databases across VA and DOD. Once an applicant's identity has been matched, the system retrieves coverage information from VA's supporting systems. Based on the applicant's enrollment status, VA's Virtual Lifetime Electronic Record Data Access Service passes back a response to CMS that includes the verified Social Security number and the relevant VA health coverage start date and end date, if applicable.

State-based marketplaces and other state systems

In most states, multiple government entities may need to connect to the FFM and data hub to carry out a variety of functions related to healthcare enrollment. State-based marketplaces generally perform the same functions that the FFM performs for states that do not maintain their own marketplace. However, in certain cases, known as partnership marketplaces, states may elect to perform one or both of the plan management and consumer assistance functions while the FFM performs the rest. The specific functions performed by each partner vary from state to state. Figure 4 shows what functions are performed by each type of marketplace.

Figure 4: Functions Performed by the Various Types of Marketplaces



Source: GAO analysis of CMS data. | GAO-14-730

Regardless of whether a state operates its own marketplace, most states need to connect their state Medicaid and CHIP agencies to either their state-based marketplace or the FFM to exchange data about enrollment in these programs. Such data exchanges are generally routed through the CMS data hub. In addition, states may need to connect with the IRS (also through the data hub) in order to verify an applicant's income and family size for the purpose of determining eligibility for or the amount of the advance premium tax credit and cost-sharing reductions. Finally, state-based marketplaces are to send enrollment confirmations to the FFM so that CMS can administer advance payments of the premium tax credit and cost-sharing payments and track overall marketplace enrollment.

Issuers of Qualified Health Plans	Issuers of qualified health plans access the FFM separately from individual applicants, using CMS's Health Insurance Oversight System. The primary data transfer to issuers is the passing of enrollment information from the FFM when an individual completes the application process. In this case, the FFM transmits the enrollment information to the data hub, which forwards it to the cognizant issuer of qualified health plans in a standardized Electronic Data Interchange format. The issuer then replies with a confirmation message that is also formatted according to the standard. According to CMS, there were 219 issuers of qualified health plans that participated during the 2014 plan year. Apart from enrollment, issuers of qualified health plans are to interact with the FFM through the Plan Management and Financial Management modules, as previously described. CMS established procedures to help ensure the security of data transmissions between the FFM and issuers of qualified health plans. Specifically, each issuer is required to digitally sign all transmissions with an encryption key that can be used by the FFM (and vice versa) to ensure that the transmissions are authentic. According to CMS officials, as transactions are readied for transmission, the CMS MIDAS system checks the data to ensure that it is being routed to the right provider. Subsequent to the transmission, MIDAS takes additional steps to confirm that the transmission was executed correctly. Issuers of qualified health plans also sign trading partner agreements with CMS requiring that the Electronic Data Interchange transactions they conduct be in accordance with CMS security and privacy policies.
Agents and brokers	In addition to applicants themselves, agents and brokers may access the Healthcare.gov website to perform enrollment-related activities on behalf of applicants. It is up to individual states to determine whether to allow agents and brokers to carry out these activities, which can include enrolling in healthcare plans and applying for the advance premium tax credit and cost-sharing reductions. To perform these functions, agents and brokers need to first, be licensed by their state. They are then required to complete registration requirements, which include participating in a training course in using the FFM and electronically signing an agreement on the use of the system that includes adherence to FFM security and privacy policies. FFM user accounts are created for these individuals after they are authenticated through the Enterprise Identity Management System. According to CMS,

71,103 agents and brokers have completed the registration process for plan year 2014.

Offline functions

Individuals can also use a paper application when applying for health insurance under PPACA. CMS awarded a contract for eligibility support services to Serco Inc. for the intake, routing, review, and troubleshooting of paper applications submitted for enrollment into a qualified health plan and for insurance affordability programs including, but not limited to, the advance premium tax credit, cost-sharing reductions, Medicaid, and CHIP. Serco Inc. is also expected to provide records management and verification support.

CMS and IRS Took Steps to Protect Taxpayer Information

IRS and CMS have taken steps to establish policies and procedures for complying with requirements for protecting taxpayer information, including the Internal Revenue Code, which provides that tax returns and return information are confidential and may not be disclosed by IRS except for certain purposes specified in section 6103 of the Internal Revenue Code.[39] PPACA amended section 6103(l) (21) of the Internal Revenue Code to authorize the IRS, upon written request from the Secretary of HHS, to disclose certain taxpayer PII, in order to assist in carrying out eligibility determinations for financial assistance through the data hub and FFM.

Additionally, IRS Publication 1075 establishes guidelines for safeguarding federal tax return information used by federal, state, and local agencies. This publication details security controls, reporting, record keeping, and access control requirements that are aligned with IRS standard practices to meet the requirements of section 6103 of the code.

In order to document the safeguards in place to protect taxpayer information received during the Healthcare.gov enrollment process, IRS required CMS to complete and submit a Safeguard Procedures Report outlining the security configurations and controls it intended to implement. For example, in order to address Internal Revenue Code section 6103 (p)(4)(C), which requires any entity or person receiving a return or return information to restrict access to the return or return information only to persons whose duties or responsibilities require access and to whom

[39]26 U.S.C.§ 6103.

disclosure may be made, CMS reported that it restricts access to taxpayer data only to individuals who require the data to perform their official duties and as authorized under the code through separation of duties, role-based security for all employees and contractors, and minimum required access for duties. In September 2013, IRS's Director of the Office of Privacy, Governmental Liaison and Disclosure informed CMS that IRS accepted its report as certification that the confidentiality of federal tax information disclosed to CMS would be adequately protected.

Information Security and Privacy Weaknesses Place Healthcare.gov Data at Risk

While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain in both the processes used for managing security and privacy as well as the technical implementation of IT security controls. CMS took steps to protect security and privacy, including developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. However, CMS has not fully addressed security and privacy management weaknesses, including having incomplete security plans and privacy documentation, conducting incomplete security tests, and not establishing an alternate processing site to avoid major service disruptions. In addition, we identified weaknesses in the technical controls protecting the confidentiality, integrity, and availability of the data maintained in the FFM. An important reason for these security and privacy weaknesses is that CMS did not ensure a shared understanding of how security was implemented for the FFM among all entities involved in its development. Until these weaknesses are addressed, increased and unnecessary risks remain of unauthorized access, disclosure, or modification of the information collected and maintained by Healthcare.gov and related systems or the disruption of service provided by the systems.

CMS Established a Security and Privacy Program for Healthcare.gov and Related Systems

FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout an information system's life cycle; and a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices.

In addition, OMB Circular A-130, Appendix III, requires federal agencies to establish interconnection security agreements before connecting their IT systems to other IT systems, based on an acceptable level of risk. The authorization should define the rules of behavior and controls that must be maintained for the system interconnection. Further, NIST guidance states that the interconnection agreement should document the requirements for connecting the IT systems and describe the security controls that will be used to protect the systems and data.[40]

As previously discussed, the Privacy Act requires agencies that establish or make changes to a system of records, to develop a system of records notice that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and contest its content.[41] Further, the E-Government Act of 2002 requires agencies to conduct a privacy impact assessment. This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system.

In addition, NIST issued guidance in 2013 on establishing privacy protections as part of an overall information security program.[42] The guidance is intended to serve as a road map for identifying and implementing privacy controls based on the need to protect the PII of individuals collected and maintained by an organization's information systems and programs. For example, NIST states that organizations should administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII and ensure that personnel certify acceptance of responsibilities for privacy requirements. In addition, NIST requires organizations to develop and implement a privacy incident response plan and provide an organized and effective response to privacy incidents in accordance with the plan. The plan should include, among other things:

[40]NIST, *Security Guide for Interconnecting Information Technology Systems (Gaithersburg, Md.,* August 2002).

[41]Under the Privacy Act, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[42]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53 Revision 4 (Gaithersburg, Md., April 2013).

- the establishment of a cross-functional privacy incident response team that reviews, approves, and participates in the execution of the plan;
- a privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks; and
- a process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly.

CMS developed security-related policies and procedures

CMS took steps to establish protections for Healthcare.gov and related systems as part of its information security program. It assigned overall responsibility for securing the agency's information and systems to appropriate officials, including the agency Chief Information Officer and Chief Information Security Officer, and designated information system security officers to assist in certifying information systems of particular CMS components. Additionally, CMS business owners are responsible for ensuring CMS systems they are responsible for are developed in accordance with, and comply with, CMS information security policies.

CMS also documented information security policies and procedures to safeguard the agency's information and systems and to reduce the risk of and minimize the effects of security incidents. For example, *CMS's Policy for the Information Security Program*[43] established its overall information security program and set ground rules under which the agency is to operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents. This policy establishes preventive measures and controls designed to detect any incidents that occur. It also addresses the recovery of information resources in the event of a disaster.

Further, CMS has also developed a process for planning, implementing, evaluating, and documenting remedial actions to address identified deficiencies in information security policies, procedures, and practices. The process specifies that plans of action and milestones are to be developed within 30 days of the final results of any external assessment or review, and that remedial actions are to be tracked monthly until the deficiency has been resolved, as determined by a security controls assessment, continuous monitoring, or security impact analysis. CMS has

[43]CMS, *CMS Policy For the Information Security Program* (Baltimore, Md., August 2010).

established a tracking system, called the CMS FISMA Controls Tracking System, which it uses to track plans of action and milestones for addressing identified deficiencies. In addition, according to CMS officials, a dedicated team has been established to monitor the security of Healthcare.gov and related systems on a continuous basis.

CMS established interconnection security agreements with federal partners

CMS established interconnection security agreements with the federal agencies it exchanges information with, including DHS, DOD, IRS, SSA, and VA. These agreements identify the requirements for the connection, the roles and responsibilities for each party, the security controls protecting the connection, the sensitivity of the data to be exchanged, and the training requirements and background checks required for personnel with access to the connection.

CMS took steps to protect the privacy of Healthcare.gov applicants' information

To address Privacy Act requirements, CMS published and updated a system-of-records notice for Healthcare.gov that addresses all required information. The notice includes, among other things, a description of the types of individuals that will have their PII contained in the system, the type of information that will be maintained in the system, and external entities who may receive such information without the explicit consent of affected individuals.

CMS has developed basic privacy training for all staff and role-based training for staff who need it, such as individuals who have access to PII while executing their routine duties. The Director of CMS's Privacy Policy and Compliance Group stated that all personnel, including contractor staff, working with databases or IT systems were required to attend privacy training based on their responsibilities related to Healthcare.gov. Contractors are required to submit evidence that this training has taken place.

Further, CMS has also established an incident handling and breach response plan and an incident response team to help manage response efforts for privacy incidents, to identify trends, and make recommendations to HHS to reduce the risks to PII. The plan outlines CMS's processes to detect a potential security incident, report it, and limit the scope and magnitude of an incident. The plan outlines the factors that CMS will consider when assessing the likely risk of harm caused by an

incident and specifies policies and procedures for notifying individuals affected by a breach of PII.[44]

CMS Accepted Increased Security Risks When Healthcare.gov Was Deployed in October 2013

In granting the FFM system an "authority to operate" in September 2013 and allowing states to connect to the data hub that had not fulfilled all security requirements, CMS accepted increased security risks. However, accepting such risks meant that the overall risk was heightened that a compromise could occur to the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. CMS subsequently took steps to mitigate the risks identified at the time of the interim authority to operate and the interim state interconnection authorizations.

CMS accepted risks in authorizing states to connect to the data hub

CMS is responsible for the overall security of the data hub, which includes ensuring that the states connecting to it have complied with CMS's security review process.[45] Any state seeking to gain an "authority to

[44]In 2013, we reported that CMS had developed, but inconsistently implemented, policies and procedures for responding to a data breach involving PII that addressed key practices specified by the OMB and NIST. We recommended that the Secretary of Health and Human Services direct the Administrator for the Centers for Medicare & Medicaid Services to: (1) require documentation of the risk assessment performed for breaches involving PII, including the reasoning behind risk determinations; (2) document the number of affected individuals associated with each incident involving PII; and (3) require an evaluation of the agency's response to data breaches involving PII to identify lessons learned that could be incorporated into agency security and privacy policies and practices. For more information, see GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34, (Washington, D.C.: Dec. 9, 2013).

[45]CMS developed a document, called the *Minimum Acceptable Risk Standards for Exchanges*, which defines a set of minimum standards for acceptable security risk that the marketplaces must address and is based on NIST standards and the IRS Safeguards Program.

connect" to the data hub was required to submit documentation that it had properly secured its planned connection.[46]

However, not all states seeking to connect to the FFM through the data hub had satisfactorily completed all the CMS requirements prior to the start of the open enrollment season on October 1, 2013. According to the Information Systems Security Officer within the Consumer Information and Insurance Systems Group, four states (Mississippi, Oklahoma, Utah, and West Virginia) did not resolve issues identified in CMS's review of their documentation prior to October 1, 2013. Rather than deny these states the ability to connect, CMS accepted the security risks and gave the states an interim 60-day authorization. (In contrast, the 38 states that fully met requirements were granted a 3-year authorization.) The same official stated that examples of issues that led to an interim authorization were (1) high-risk findings remaining open from security testing, (2) a large number of lower risk findings remaining open from testing, or (3) the lack of a third-party independent security assessment. According to this official, no states seeking to connect to the data hub at the beginning of open season were denied the ability to do so because CMS officials deemed it critically important that all states be able to connect to Healthcare.gov if they sought to do so.

In cases where CMS granted an interim authorization, officials told us the CMS Chief Information Officer sent a letter to the state specifying the tasks that had to be completed before a full 3-year authorization would be granted. As CMS officials pointed out, their decision to allow these states to connect on an interim basis was in accordance with NIST standards, which state that "interim approval may be granted if the planned interconnection does not meet the requirements stated in the interconnection security agreement, but mission criticality requires that

[46]The documentation required by CMS includes: (1) a system security plan describing the design of the system and the process for identifying and mitigating security risks, (2) a report documenting an assessment of the security risks for the system conducted either internally or through a third party, (3) a plan of action and milestones and corrective action plan for mitigating any risks identified by the security risk assessment, (4) a signed information exchange agreement documenting roles and responsibilities for protecting data, and (5) an interconnection security agreement specifying the interconnection arrangements and responsibilities for all parties, the security controls implemented by the state, the technical and operational security requirements that the state follows, and attesting that the state IT system is designed, managed, and operated in compliance with the CMS standards.

the interconnection must be established and cannot be delayed.[47] According to CMS, no compromises of data resulted from its acceptance of these risks and each of these states subsequently addressed the deficiencies in its original submission and received a 3-year authorization.

CMS accepted significant risks in initially authorizing the FFM to operate

In addition to allowing four states to connect without fulfilling all security requirements, CMS also authorized the FFM to operate in September 2013 though testing for several support systems had not been completed and high-risk findings had been identified in the testing that was completed. NIST guidelines state that the authorizing official is to determine whether the risks to organizational operations, organizational assets, individuals, and other organizations, are acceptable.[48] Further, *CMS's Information Security Authorization to Operate Guide* states that a system should be denied an authorization to operate if there are open high-risk findings; the authorization to operate package is missing the system security plan, risk assessment, or security assessment; or a known vulnerability has been exploited.

The FFM was initially granted authorization to operate on September 3, 2013, even though high-risk weaknesses existed. This authorization was for a limited configuration of the system that included only modules for qualified health plans and for dental coverage. For this configuration, the CMS Chief Information Officer deemed the existing risks to the system as acceptable, despite the fact that two high-risk findings remained open because an action plan had been developed for addressing the risks and the approval was predicated on completion of those actions. In addition, four other findings had not been addressed. According to CMS officials, a subsequent decision was made to take offline the modules of the FFM that had been authorized on September 3, 2013, because the high-risk findings associated with them could not be mitigated before the beginning of open enrollment on October 1.

An additional decision memorandum, dated September 27, 2013, addressed other modules of the FFM. It noted that CMS's security

[47]NIST, *Security Guide for Interconnecting Information Technology Systems*, SP 800-47 (Gaithersburg, Md., August 2002).

[48]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md., February 2010).

contractor had not been able to test all of the security controls for the FFM in one complete version of the system. The memorandum granted an authority to operate for six months and stipulated that a full security controls assessment be conducted on the FFM, including all three of its major modules, within 60 to 90 days of October 1.

A complete security controls assessment of the FFM's eligibility and enrollment module was conducted in December 2013, in keeping with the time frames established in the September 27, 2013, memo. However, the other two major modules of the FFM—plan management and financial management—were not tested. These modules had not yet been fully developed and were not made available online on October 1.

CMS Has Not Fully Implemented Security and Privacy Management Controls Associated With Healthcare.gov

Though CMS developed and documented security policies and procedures, it did not fully implement actions required by NIST before Healthcare.gov began collecting and maintaining PII from individual applicants. Specifically, NIST guidelines[49] require that system security plans include a description of the components comprising the system—called an authorization boundary—and a listing of other information systems that interconnect with the system, among other elements. The plans should also identify the individuals responsible for the system and its security, include descriptions of how security controls are implemented, and, in the case of controls recommended by NIST but not implemented, a justification for why the control was deemed not necessary for that system. To the extent that a system relies on controls established for another system (known as inherited controls) or for multiple systems (referred to as common controls), NIST guidelines call for describing those controls as well, noting that organizations should assess how effective they are for the new system being planned and identify compensating or supplementary controls as needed.

CMS did not document key controls in system security plans

CMS developed system security plans for the systems supporting Healthcare.gov that document the planned implementation of the controls designed to protect the confidentiality, integrity, and availability of the systems and the information they contain. While the system security plans for the FFM and data hub incorporate most of the elements

[49]NIST, *Guide for Developing Security Plans for Federal Information Systems*, Special Publication 800-118 Revision 1 (Gaithersburg, Md., February, 2006).

specified by NIST, each is missing or has not completed one or more relevant elements. For example, the security plan for the FFM does not define the system's authorization boundary, or explain why agency officials determined that four of the controls listed in NIST's guidance were not applicable. Additionally, for 125 inherited controls and control enhancements out of the 312 controls and enhancements in the plan, the plan contains no details other than identifying the system from which they are inherited. Similarly, the data hub security plan does not list the systems with which it has interconnection security agreements, though it connects with systems from many federal agencies, states, and the District of Columbia.[50] CMS officials told us that they believed their security plans were complete. However, the plans they provided did not contain these important elements.

Without complete system security plans, it will be difficult for agency officials to make a fully informed judgment regarding the risks involved in operating those systems, increasing the risk that the confidentiality, integrity, or availability of the system could be compromised.

CMS has not finalized an interconnection security agreement with Equifax

CMS has not completed security documentation governing its interconnection with Equifax Inc., a private company that performs income verification services that CMS uses to determine eligibility for income-based subsidies. In order to perform the verification, CMS transmits PII to Equifax, which responds with information about the applicant's current employer and compensation. As previously discussed, OMB requires agencies to establish interconnection security agreements before connecting their IT systems to other IT systems. CMS officials said they are relying on a draft data use agreement for this exchange of data, because the agreement has not yet been fully approved within CMS.

CMS did not fully assess privacy risks in PIAs

CMS privacy documentation was also incomplete. OMB requires agencies to assess privacy risks as part of the process of developing a privacy impact assessment (PIA).[51] These risk assessments are intended to help program managers and system owners determine appropriate privacy protection policies and techniques to implement those policies.

[50]Currently, 47 states, including the District of Columbia have a connection to the data hub.

[51]OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

According to OMB, an analysis of privacy risks should be performed to determine the nature of privacy risks and the resulting impact if corrective actions are not in place to mitigate those risks as well as an assessment of alternative processes for handling information to mitigate potential privacy risks.

CMS developed and documented PIAs for the FFM and the data hub. Both PIAs describe, among other things, the purpose of the system; the type of information it will collect, maintain, or share; and whether the system handles PII. The PIA for the data hub states that the system does not collect, maintain, use, or share PII, although it processes and transmits data, including PII, in support of Healthcare.gov and its supporting systems. Both PIAs were approved by the CMS Senior Official for Privacy and the HHS Senior Agency Official for Privacy.

However, in completing these PIAs, CMS did not assess the risks associated with the handling of PII or identify mitigating controls to address such risks. Both PIAs provided only general information about the systems, such as the type of information that the system would collect, the intended uses for the PII that was to be collected, and the external entities with whom the PII would be shared. They did not include an analysis of privacy risks associated with this broad collection of personal information or what steps were taken to mitigate those risks. For example, the data hub PIA did not include an analysis justifying the agency's conclusion that the system does not collect, maintain, use, or share PII. Nor did the FFM PIA include an assessment of alternative processes for handling information to mitigate potential privacy risks associated with the extensive amount of PII collected and maintained by the system.

The Director of CMS's Privacy Policy & Compliance Group stated that discussions about the risks associated with the handling of PII within Healthcare.gov-related systems were conducted during the system's security development process because CMS considered this a security issue. She also stated that CMS's PIAs were intended primarily to look at data flows and authorities to collect the data. However, according to OMB guidance, a PIA should also include an analysis of privacy risks. Without such an analysis, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems.

Likewise, the draft PIA for MIDAS, a data warehouse system that provides reporting and performance metrics related to the FFM and other

supporting systems, does not include an analysis of privacy risks consistent with OMB guidance. According to CMS officials, MIDAS generates reports that aggregate data, including PII collected during the plan enrollment process, to create summary reports. The Director of CMS's Privacy Policy & Compliance Group stated that MIDAS did not contain PII when it first became operational and that a draft PIA was developed after the system's functions were changed to include processing of PII. She also stated that the draft had not yet been finalized but did not indicate whether the final version would include an analysis of privacy risks. Without an approved PIA that includes a thorough analysis of privacy risks, it will be difficult for CMS to demonstrate that it has assessed the potential for PII to be displayed to users, among other risks, and taken steps to ensure that the privacy of that data is protected.

CMS did not establish computer matching agreements with two agencies

CMS did not establish a computer matching agreement with all of the federal agencies with which it exchanges data for the purposes of verifying eligibility for healthcare coverage and the advance premium tax credit, as required by the Computer Matching Act. Specifically, CMS has a computer matching agreement in place with SSA, DHS, IRS, DOD, and VA. These agreements include all required information, including the purpose and legal authority for the exchange, a justification for the exchange, and a description of the records that will be matched.

However, CMS did not develop such an agreement with OPM or the Peace Corps. According to OPM and Peace Corps officials, they determined that a computer matching agreement was not required because they transmitted information to CMS in a batch file format on an intermittent basis rather than establishing a real-time comparison process. Further, they considered their transmission of information to CMS to be a one-way transaction, rather than a direct matching of information in two or more systems. However, the Computer Matching Act neither specifies the connectivity between two automated systems of records nor that the requirement for an agreement applies only to certain types of transfers.[52] Accordingly, since the exchange of data between

[52]The Computer Matching amendments to the Privacy Act require a matching agreement when a record is disclosed by an agency to a recipient agency for use in a computer matching program. 5 U.S.C. § 552a(o). The Privacy Act defines "matching program" as any computerized comparison of two or more automated systems of records for the purpose of [among other purposes] establishing or verifying the eligibility of applicants for, or recipients or beneficiaries of, payments under federal benefit programs. 5 U.S.C. § 552a(a)(8).

CMS and OPM and the Peace Corps appears to be a computerized comparison of data from two automated systems of records for purposes of determining eligibility for federal benefits,[53] as described in the act, a computer matching agreement would be required.[54]

Without conducting a complete PIA for systems collecting and maintaining PII and establishing computer matching agreements with all agencies exchanging PII for eligibility determination purposes, increased risk exists that proper protections have not been implemented for the PII being exchanged.

CMS did not conduct complete security testing

FISMA requires agencies to periodically test and evaluate information security controls on information systems to ensure they are being implemented effectively. In addition, NIST and CMS guidance make clear that the security of complex systems such as the FFM and interconnected systems needs to be tested in a comprehensive fashion that takes into consideration how the systems are interconnected and how security controls are managed across all interconnected systems. For example, NIST has developed a risk management framework that, among other things, emphasizes that agencies should test the implementation of security controls to determine the extent to which they are implemented correctly, are operating as intended, and meet security requirements.[55] NIST also notes that security assessments should assess the controls implemented by a system and those inherited from other systems. Draft NIST guidance on security engineering also makes clear that security validation should take place at multiple levels of a system, ranging from individual components and service, up through systems of systems. The framework states that security assessments or testing should be completed before a system is granted an "authority to connect" to other agency systems.

[53] PPACA requires individuals to maintain health coverage that meets certain minimum requirements and imposes penalties on those who do not do so. OPM and Peace Corps, among other government agencies, provide health insurance coverage data to CMS for purposes of determining if an individual has minimum essential coverage.

[54]We recently issued a report on computer matching agreements, including the need for additional OMB guidance. See GAO, *Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation*, GAO-14-44 (Jan. 13, 2014).

[55]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37 Revision 1* (Gaithersburg, Md. February 2010).

CMS's system security plan procedures state that a completed system security plan package must contain technical information about the system, its security requirements, and the controls implemented to provide protection against vulnerabilities. CMS procedures also note that for a comprehensive assessment, the assessor is expected to assess all controls, including those that are inherited, and limitations on testing inherited controls should be clearly identified. In addition, CMS policy states that an understanding of all relevant controls and how they are inherited throughout the system is required to evaluate the effectiveness of security controls.

CMS has undertaken, through its contractors and at the agency and state levels, a series of security-related testing activities that began in 2012. Table 1 summarizes these activities through June 2014.

Table 1: Security Testing of the Federally Facilitated Marketplace (FFM) System, Data Hub, and Connections with Federal Partners

Date	Test Performed	Scope
September 2012	Infrastructure as a service security control assessment	Physical environment and hardware in data center.
October 2012	Platform as a service security control assessment	Security controls of the platform as a service general support system.
March-April 2013	First FFM security control assessment	Partial application assessment of the FFM Qualified Health Plans module.
	Data hub testing with Department of Defense begins	Tests performed include functional tests, connectivity tests, and performance tests.
May 2013	Data hub testing with Social Security Administration begins	Tests performed include penetration tests, connectivity tests and performance tests.
	Data hub testing with Department of Homeland Security begins	Tests performed include security assessment, and interface tests.
July 2013	Data hub connection testing with Internal Revenue Service	Tests performed include controls assessments, compliance and vulnerability scanning.
August - September 2013	Second FFM security control assessment	Partial application testing of the deployed FFM eligibility and enrollment module, but with testing hampered by significant functionality issues identified by the tester. Assessment did not including operating systems or network hardware.
	Data hub connection testing with Department of Veterans Affairs	Tests performed include connectivity tests and performance tests.
	Data hub security control assessment	Application testing of the data hub, including operating systems and network hardware.
December 2013	Third FFM security control assessment	Partial application testing of the deployed FFM eligibility and enrollment module, but not including operating systems or network hardware.

Date	Test Performed	Scope
March 2014	Fourth FFM security control assessment	Application testing of the deployed FFM eligibility and enrollment and plan management modules, but not including operating systems or network hardware.
June 2014	Fifth FFM security control assessment	Testing of specific system-level components supporting the FFM, including system configuration settings and network vulnerability testing.

Source: GAO Analysis of Agency documents| GAO-14-730

However, these controls assessments did not effectively identify and test all relevant security controls prior to deploying the IT systems supporting Healthcare.gov.

The security control assessments for the FFM did not include tests of the full suite of security controls specified by NIST and CMS. The contractor that conducted these assessments reviewed only the security controls that CMS selected. This testing did not include agency policy and procedures, incident response controls, many of the controls specified for physical and environmental protection, and CMS security program management controls.

CMS could not demonstrate that it had tested all the security controls specified in the October 2013 system security plan for protecting the FFM. Neither the test plan nor the final report of the September 2013 security control assessment states specifically which controls were tested at that time. CMS did not test all of the FFM's components before deployment and did not test them all on an integrated system. Because the eligibility and enrollment module was the only one that was to become operational on October 1, 2013, it was the only FFM module that the contractors tested. Because extensive software development activities were still underway, CMS allowed only very limited independent testing by its contractors. Testing of all deployed eligibility and enrollment modules and plan management modules did not take place until March 2014.

FFM testing remained incomplete as of June 2014. While CMS took steps to address security at specific layers and in specific segments, it had not ensured that controls worked effectively for the entire system. For example, CMS had not yet adequately considered the role of "inherited" controls on the security of the FFM. In tests in August, September, and December of 2013, and March 2014, CMS declared operating system and network infrastructure controls—inherited from the underlying cloud-based services system—as being out of scope for security controls

assessments, or explicitly assumed they were adequate. However, the effectiveness of these inherited controls for the FFM and other Healthcare.gov supporting systems was not confirmed in the FFM testing.

Without comprehensive testing, CMS does not have reasonable assurance that its security controls for the FFM are working as intended, increasing the risk that attackers could compromise the confidentiality, integrity, or availability of the system.

CMS did not establish an alternate processing site to protect against major disruptions

FISMA requires agencies to develop plans and procedures to ensure continuity of operations for IT systems that support their operations and assets. A continuity of operations plan helps ensure that an organization's mission-essential functions can continue during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. If normal operations are interrupted, network managers must be able to detect, mitigate, and recover from the disruption while preserving access to vital information.

NIST has issued guidance that provides agencies with detailed instructions on implementing the provisions of FISMA. For Healthcare.gov and its related systems, which CMS has rated at the "moderate" risk level, NIST guidance requires that a contingency plan be prepared, alternative processing and storage sites established, and information system backup, recovery, and reconstitution procedures implemented to ensure that operations can continue in the event of a disruption.[55] According to NIST guidance, the contingency plan should include a strategy to recover and perform system operations at an alternate facility for an extended period to ensure continuity of operations. Moreover, operations at the alternate site should be governed by an agreement that details the agency's specific needs, including disaster declaration, site availability, information system requirements, security requirements, records management, and service-level management. These alternate facilities must at least have adequate space and infrastructure to support recovery activities, and may contain some or all of the necessary system hardware, software, telecommunications, and power sources.

[55]NIST, *Contingency Planning Guide for Federal Information Systems*, SP 800-34 Revision 1 (Gaithersburg, Md., May 2010).

CMS developed and documented contingency plans for the FFM and data hub. In these plans, CMS identified the activities, resources, responsibilities, and procedures needed to carry out operations during prolonged interruptions of the systems and outlined coordination with other stakeholders participating in contingency activities. It also established system recovery priorities, a line of succession based on the type of disaster, and specific procedures on how to restore both systems and their associated applications after a disaster situation. In these plans, CMS designated a facility as its "warm" disaster recovery site,[57] to hold mirrored databases, servers, and daily replicated enterprise data of its critical IT systems.

However, as noted in the FFM and data hub contingency plans, as of March 2014, the warm disaster recovery site had not yet been established. According to CMS, the data supporting the FFM are being backed up to the designated site, but backup systems are not otherwise supported there, limiting that facility's ability to support disaster recovery efforts. CMS officials stated that the agency is working with a new contractor to establish an alternate recovery site for all Healthcare.gov-related systems, which they said is expected to be operational in the fall of 2014. However they did not provide documentation confirming these plans. Until a designated alternate site is in place and fully operational, CMS remains unprepared to mitigate and recover from a disaster that threatens the availability of vital information.

Control Weaknesses Continue to Threaten Information and Systems Supporting Healthcare.gov

A basic management objective for any organization is to protect confidentiality, integrity, and availability of the information and systems that support its critical operations and assets. Organizations accomplish this by designing and implementing access and other controls that are intended to protect information and systems from unauthorized disclosure, modification, and loss. Specific controls include, among other things, those related to identification and authentication of users, authorization restrictions, and configuration management.

[57] According to NIST 800-34, warm disaster recovery sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources for operational readiness in the event of a disaster. However, the equipment is not loaded with the software or data required to operate the system. Recovery to a warm site can take several hours to several days, depending on system complexity and the amount of data to be restored.

CMS did not effectively implement or securely configure key security tools and devices on the systems supporting HealthCare.gov to sufficiently protect the users and information on the system from threats to confidentiality, integrity and availability. For example:

- CMS did not always require or enforce strong password controls on systems supporting the FFM. NIST Special Publication 800-53 recommends and CMS policy sets standards for minimum password length and complexity. Without strong password controls, an attacker attempting to compromise the FFM would have a greater chance of being able to compromise user credentials and access the system.

- CMS did not restrict systems supporting the FFM from accessing the Internet. NIST Special Publication 800-53 recommends that information systems be configured to only provide essential capabilities and functions. However, systems supporting the FFM that we reviewed were able to access the public Internet. Allowing these systems to access the Internet may allow for unauthorized users to access data from the FFM network, increasing the risk that an attacker with access to the FFM could send data to an outside system, or that malware could communicate with a command and control server.

- CMS did not consistently implement patches for several FFM systems. NIST Special Publication 800-53 recommends that organizations test and install newly-released security patches, service packs, and hot fixes. However, CMS did not consistently apply patches to critical systems or applications in a timely manner. Also, several critical systems had not been patched or were no longer supported by their vendors. By not keeping current with security patches, CMS faces an increased risk that servers supporting the FFM could be compromised through exploitation of known vulnerabilities.

- CMS's contractor had not securely configured its administrative network properly. NIST Special Publication 800-53 recommends how such a network should be configured. Without adhering to NIST recommendations, CMS may face an increased risk of unauthorized access to the FFM network.

In addition to the above weaknesses, we identified other security weaknesses in controls related to boundary protection, identification and authentication, authorization, and software updates that limit the effectiveness of the security controls on the systems supporting

HealthCare.gov and unnecessarily place sensitive information at risk of unauthorized disclosure, modification or exfiltration. CMS officials stated that it was difficult to ensure that a system as large and complex as the FFM had no vulnerabilities and that performing assessments to identify vulnerabilities as we did was useful. The control weaknesses we identified during this review are described in a separate report with limited distribution.

Security and Privacy Weaknesses Resulted from CMS Not Establishing a Shared Understanding of How Security Was Implemented for Healthcare.gov-related Systems

One cause of the previously discussed weaknesses is that CMS did not ensure that the multiple entities contributing to the development of the FFM all shared the same understanding of how security controls were implemented. For a complex system of systems like Healthcare.gov, it is important that all participants in the development of the system—both agency officials and contractor staff—share the same understanding of the system's security architecture.[58] Such an understanding is important to ensuring that security controls function effectively as a cohesive whole. Without it, vulnerabilities can exist in the system that may escape the notice of individual system developers. Many of the vulnerabilities identified during our technical controls assessment may be due to the fact that different contractors working on the system had conflicting views on how security controls for Healthcare.gov were to work.

NIST guidelines note that, for complex information systems, knowledge of the security properties of individual subsystems does not necessarily provide complete knowledge of the security properties of the entire system. Controls that are effective within one subsystem may be less adequate when interconnections with other subsystems are taken into account, and an individual subsystem may depend on security controls that are inherited from other systems or the infrastructure the subsystem is built on to provide adequate protection. Accordingly, NIST states that, to be effective, security controls must be mutually supporting, employed with realistic expectations for effectiveness, and implemented as part of an explicit, information system-level security architecture. NIST also notes that, when applying controls, agencies should consider any implementation issues related to the integration or interfaces between

[58]A security architecture describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. [NIST, *Managing Information Security Risk*, SP 800-39 (Gaithersburg, Md.: March 2011)].

common, hybrid, and system-specific controls. It recommends that an agency ensure that there are effective communications among the entities providing security capabilities to and receiving security capabilities from others.

CMS and contractor staff did not always agree on how security controls for the FFM were to be implemented or who was responsible for ensuring they were functioning properly. Although responsibility for implementing security controls for the FFM is spread across multiple systems and parties, CMS officials stated that no one individual was responsible for ensuring consistency of the security controls across the entire system. The Consumer Information and Insurance Systems Group Information System Security Officer stated that the agency generally relied on its contractor security control assessors to have an integrated awareness of the system's overall security posture. However, these assessors had only limited access to the FFM at any given point in time and tested elements of the system only incrementally.

Further, CMS and its contractors did not agree on security responsibilities. For example, although CMS identified one subcontractor as being responsible for managing firewall rules, that responsibility was not included in the subcontractor's statement of work, and staff for the subcontractor indicated it was the responsibility of a different contractor. In another instance, the contractor responsible for managing database accounts said they were unable to do so properly due to large numbers of accounts held by other contractors or users at CMS, and a lack of communication from those entities regarding which accounts were still needed and which could be terminated.

Without ensuring that all parties responsible for the FFM's security controls agree on security roles and responsibilities and share the same understanding of how controls are implemented, the controls may not function as intended, increasing the risk that attackers could compromise the confidentiality or integrity of the system and the data it contains.

Conclusions

Healthcare.gov and its related systems represent a complex system of systems that interconnect a broad range of federal agency systems, state agencies and systems, and other entities, such as contractors and issuers of qualified health plans.

In developing Healthcare.gov and its supporting systems and establishing connections with federal and state partners, CMS took important steps to

help ensure that the site and the PII it maintains are protected from unauthorized access or misuse. However, a system with this degree of complexity and involving such a sizeable number of interconnections can pose many security and privacy risks. CMS did not take all reasonable steps to limit those risks. Security and privacy plans were missing relevant elements, and security testing was incomplete. A number of control weaknesses pose unnecessary and increased security risks to the FFM, interconnected systems, and information. Until it addresses shortcomings in both the technical security controls and its information security program, CMS is exposing Healthcare.gov-related data and its supporting systems to significant risks of unauthorized access, use, disclosure, modification, and disruption.

Recommendations for Executive Action

To fully implement its information security program and ensure that PII contained in its systems is being properly protected from potential privacy threats, we recommend that the Secretary of Health and Human Services direct the Administrator of the Centers for Medicare & Medicaid Services to implement the following six recommendations:

1. Ensure that the system security plans for the FFM and data hub contain all the information recommended by NIST.
2. Ensure that all privacy risks associated with Healthcare.gov are analyzed and documented in their privacy impact assessments.
3. Develop separate computer matching agreements with OPM and the Peace Corps to govern the data that is being compared with CMS data for the purposes of verifying eligibility for the advance premium tax credit and cost-sharing reductions.
4. Perform a comprehensive security assessment of the FFM, including the infrastructure, platform and all deployed software elements.
5. Ensure that the planned alternate processing site for the systems supporting Healthcare.gov is established and made operational in a timely fashion.
6. Establish detailed security roles and responsibilities for contractors, including participation in security controls reviews, to better ensure that communications between individuals and entities with responsibility for the security of the FFM and its supporting infrastructure are effective.

In a separate report with limited distribution, we are also making 22 recommendations to resolve technical information security weaknesses

related to access controls, configuration management, and contingency planning.

Agency Comments and Our Evaluation

We sent draft copies of this report to the eight agencies covered by our review, as well as Experian Information Solutions. We received written responses from the Departments of Health and Human Services (HHS) and Veterans Affairs. HHS fully or partially concurred with all of GAO's recommendations. Further, the Department of Veterans Affairs stated that it generally concurred with our conclusions. These comments are reprinted in appendices II and III.

In addition, on August 27, 2014, we received technical comments via e-mail from the following: (1) the Senior Advisor to Director within the Internal Revenue Service's Office of Governmental Liaison, Disclosure & Safeguards; (2) the Social Security Administration's Chief of Staff; and (3) a program manager within Experian Information Solutions' Cybersecurity Solutions Operations office. Further, on August 28, 2014, a program analyst from the GAO-OIG Liaison Office within the Department of Homeland Security also provided us with technical comments in an e-mail. Finally, on August 29, 2014, a program analyst within the Office of Personnel Management's Merit System Accountability and Compliance - Internal Oversight & Compliance office also provided us with technical comments in an e-mail. All of the technical comments received were incorporated into the draft as appropriate.

Further, on August 25, 2014 and August 29, 2014, respectively, an official from the Peace Corps' Office of Congressional Relations and from the Department of Defense's Office of Inspector General indicated via e-mail that both agencies had no comments on the report.

In its written comments, HHS noted that the Centers for Medicare & Medicaid Services (CMS) developed the Healthcare.gov related systems consistent with federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. Further, HHS stated that CMS did not concur with our draft finding that it accepted significant security risks when it granted the FFM and the data hub an Authority to Operate in September 2013 and allowed states to connect to the data hub. The basis for CMS' view was that (1) independent security testing had been completed on the data hub and the pieces of the FFM that went live on October 1, 2013, with no open high findings, and (2) every state that connected to the data hub had adhered to CMS security procedures. However, we disagree that

these facts justify the conclusion that CMS accepted no significant risks in authorizing the systems to operate in September 2013. The fact that CMS's security contractor had not been able to test all of the security controls for the FFM in one complete version of the system meant that there was an increased risk that undetected security control deficiencies could lead to a compromise that jeopardizes the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. Also, four of the states that were granted an authority to operate were given only interim authorizations because of issues such as: (1) high-risk findings remaining open from security testing, (2) a large number of lower risk findings remaining open from testing, or (3) the lack of a third-party independent security assessment. We believe such shortcomings also posed an increased risk that a compromise could occur to the confidentiality, availability, and integrity of Healthcare.gov and the data it maintained. Thus we continue to believe that CMS accepted significant risks in approving Healthcare.gov operations in September 2013.

In response to our 28 recommendations, HHS concurred with three of the six recommendations to fully implement its information security program and all 22 of the recommendations to improve the effectiveness of its information security controls. It also provided information regarding specific actions the agency has taken or plans on taking to address these recommendations. We also received technical comments from HHS, which have been incorporated into the final report as appropriate.

HHS partially concurred with our three remaining information security program-related recommendations. Specifically, regarding our recommendation to ensure that the system security plans for the FFM and Hub contain all the information recommended by NIST, HHS noted that CMS has a master security plan that identifies all of its agency-level controls but acknowledged that the system security plans for the FFM and data hub did not adequately document inherited agency-level controls. We continue to believe that it is important for the system security plans to include all information recommended by NIST, including the system's authorization boundary and explanations for why controls listed in NIST's guidance are not being implemented, elements that were missing from the FFM security plan. CMS stated that it would update its plans to include inherited security controls.

Regarding our recommendation to ensure that all privacy risks associated with HealthCare.gov are analyzed and documented in privacy impact assessments (PIA), CMS partially concurred, stating that the PIAs for the FFM and the data hub were created using the HHS PIA template, which

go beyond the requirements set by the Office of Management and Budget guidance on PIAs. However, OMB guidance for implementing the privacy provisions of the E-Government Act of 2002 (OMB Memorandum M-03-22) requires PIAs to include an analysis of privacy risks, and the CMS PIAs did not include such an analysis. Without it, CMS cannot demonstrate that it thoroughly considered and addressed options for mitigating privacy risks associated with these systems. We continue to believe the PIAs should include an analysis of all privacy risks associated with HealthCare.gov operations.

Regarding our recommendation to perform a comprehensive security assessment of the FFM, including the infrastructure, platform, and all deployed software elements, CMS concurred that comprehensive security assessments are important, but disagreed that the infrastructure, platform, or software elements had not been tested. It noted that a security control assessment was completed separately for the infrastructure as a service and platform as a service that host FFM systems, and authorities to operate were granted, on November 23, 2012, and January 25, 2013, respectively. HHS also noted that FFM security controls were tested again in June 2014. We have updated the report to include the tests to which CMS referred. However, we continue to believe that while CMS took steps to address security at specific layers, it did not ensure that controls worked effectively for the entire system and did not adequately document the role of inherited controls in the security of the FFM. NIST guidelines on managing information security risk (Special Publication 800-39) note that security controls that are effective within one subsystem may be less adequate when interconnections with other subsystems are taken into account and that such controls must be mutually supporting and employed with realistic expectations for effectiveness. Thus we continue to believe that a comprehensive assessment of the security of the FFM is warranted to ensure that the security controls for the FFM are adequate.

We are sending copies of this report to the Departments of Defense, Health and Human Services, Homeland Security, Treasury, and Veterans Affairs, as well as the Office of Personnel Management, the Peace Corps, and the Social Security Administration.

Should you or your staffs have questions on matters discussed in this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Contact points for our

Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Gregory C. Wilshusen
Director, Information Security Issues

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

List of Congressional Requesters

The Honorable Ron Wyden
Chairman
The Honorable Orrin Hatch
Ranking Member
Committee on Finance
United States Senate

The Honorable Thomas R. Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Lamar Alexander
Ranking Member
Committee on Health, Education, Labor and Pensions
United States Senate

The Honorable Jon Tester
Chairman
Subcommittee on Efficiency and Effectiveness of Federal
Programs and the Federal Workforce
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Claire McCaskill
Chairman
Subcommittee on Financial and Contracting Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Darrell Issa
Chairman
The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Dave Camp
Chairman
The Honorable Sander M. Levin
Ranking Member
Committee on Ways and Means
House of Representatives

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Mike Coffman
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

The Honorable Charles Boustany, Jr.
Chairman
The Honorable John Lewis
Ranking Member
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

The Honorable Mark Begich
United States Senate

The Honorable Michael Bennet
United States Senate

The Honorable Richard Blumenthal
United States Senate

The Honorable Robert P. Casey, Jr.
United States Senate

The Honorable Al Franken
United States Senate

The Honorable Kay R. Hagan
United States Senate

The Honorable Tim Kaine
United States Senate

The Honorable Amy Klobuchar
United States Senate

The Honorable Mary Landrieu
United States Senate

The Honorable Joe Manchin III
United States Senate

The Honorable Jeffrey A. Merkley
United States Senate

The Honorable Bill Nelson
United States Senate

The Honorable Mark Pryor
United States Senate

The Honorable Jeanne Shaheen
United States Senate

The Honorable John Thune
United States Senate

The Honorable Mark Udall
United States Senate

The Honorable Mark R. Warner
United States Senate

The Honorable Ron Barber
House of Representatives

The Honorable John Barrow
House of Representatives

The Honorable Tulsi Gabbard
House of Representatives

The Honorable Pete P. Gallego
House of Representatives

The Honorable Duncan Hunter
House of Representatives

The Honorable Mike Kelly
House of Representatives

The Honorable Ann McLane Kuster
House of Representatives

The Honorable Daniel W. Lipinski
House of Representatives

The Honorable Patrick E. Murphy
House of Representatives

The Honorable Scott Peters
House of Representatives

The Honorable Kyrsten Sinema
House of Representatives

The Honorable Filemon Vela
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the planned exchanges of information between the Healthcare.gov website, supporting information technology (IT) systems, and the federal, state, and other organizations that are providing or accessing the information, including special arrangements for handling tax information in compliance with legal requirements and (2) assess the effectiveness of the programs and controls implemented by the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS) to protect the security and privacy of the information and the major IT systems used to support Healthcare.gov.

To address our first objective, we reviewed the Patient Protection and Affordable Care Act (PPACA) and other relevant laws to identify the responsibilities of CMS and other federal agencies for establishing and participating in healthcare coverage marketplaces. We reviewed and analyzed system and security documentation, including interagency agreements, with each partnering entity in order to identify interconnections between Healthcare.gov and other external partners that are providing or accessing information to support enrollment processes for Healthcare.gov. Further, we obtained documentation and interviewed officials at the following federal agencies that directly support implementation of Healthcare.gov: the Department of Defense (DOD), Homeland Security (DHS), and Veterans Affairs (VA), as well as CMS, Experian Information Solutions, the Internal Revenue Service (IRS), the Office of Personnel Management (OPM), the Peace Corps, and the Social Security Administration (SSA). We also received a demonstration of the online Healthcare.gov system, which we used to corroborate the information flow described to us by agency officials and in official documentation. Based on an analysis of the information we received, we described the major types of data connections that are currently in place or planned between systems maintained by CMS to support Healthcare.gov and other internal and external systems. We also reviewed requirements set forth in the Internal Revenue Code, PPACA, and implementing guidance regarding the handling of taxpayer data to describe how IRS and CMS policies and procedures for sharing tax data adhere to legal requirements.

To address our second objective, we reviewed relevant information security and privacy laws, guidance, and National Institute of Standards and Technology (NIST) standards and guidance to identify federal security and privacy control requirements. We compared CMS's security and privacy policies and procedures to determine their adherence to federal requirements. We then assessed the implementation of controls over Healthcare.gov and its supporting systems and interconnections by

reviewing risk assessments, security plans, system control assessments, contingency plans, and remedial action plans. To determine the effectiveness of the information security controls for the Federally Facilitated Marketplace (FFM), we analyzed the overall network control environment, identified interconnectivity and control points, and reviewed controls for the network and servers supporting the FFM. Specifically, we reviewed controls over the FFM application and its supporting software, the operating systems, network and computing infrastructure provided by the supporting platform as a service, and infrastructure as a service systems.

To evaluate CMS's controls over its information systems supporting Healthcare.gov, we used our Federal Information System Controls Audit Manual, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information; NIST standards and guidelines; National Security Agency guidance; Center for Information Security guidance; and agency policies, procedures, practices, and standards.

Specifically, we

- reviewed network access paths to determine if boundaries had been adequately protected;
- reviewed the complexity and expiration of password settings to determine if password management was being enforced;
- analyzed users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observed configurations for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- reviewed software security settings to determine if modifications of sensitive or critical system resources had been monitored and logged;
- examined configuration settings and access controls for routers, network management servers, switches, and firewalls; and
- inspected the operating system and application software on key servers and workstations to determine if critical patches had been installed and/or were up-to-date.
- Aspects of our review of controls on the infrastructure supporting Healthcare.gov were limited because they involved shared system elements in a cloud environment. Regarding the CMS infrastructure as a service contract with its contractor, we only reviewed those elements of the environment that were dedicated to CMS's use. Consequently, it is possible our review may either have not identified

certain controls that would compensate for the weaknesses we identified, that weaknesses remain in the system that we did not identify, or both.

Using the requirements established by the Federal Information Security Management Act of 2002 and associated NIST and agency guidelines, we evaluated CMS's information security program, as it related to Healthcare.gov, by:

- reviewing agency policies and procedures to determine the extent to which they addressed roles and responsibilities for information security, incident response, and flaw remediation;
- reviewing the system security plans for the FFM and the data hub to determine the extent to which they addressed elements recommended by NIST;
- reviewing the interconnection security agreements between CMS and DHS, DOD, IRS, SSA, and VA to determine the extent to which they addressed elements recommended by NIST;
- reviewing the security control assessments for the FFM to determine the extent to which they complied with NIST guidance;

We performed our work at CMS headquarters in Baltimore, Maryland; and at contractor facilities in Dallas, Texas; and in Reston and Chantilly, Virginia.

To determine the extent to which CMS had addressed privacy concerns in the development and operation of Healthcare.gov and its supporting systems, we compared the requirements of the Privacy Act of 1974 and E-Government Act of 2002 and associated guidance with privacy documentation, such as system of records notices and privacy impact assessments, for the FFM, data hub, and other systems that support Healthcare.gov. We also compared requirements of the Computer Matching Act with computer matching agreements CMS established with DHS, DOD, IRS, SSA, and VA, and the data transfer arrangements CMS made with OPM and the Peace Corps.

We conducted this performance audit from December 2013 to September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Wilshusen and Dr. Barkakati,

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "HealthCare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls" (GAO-14-730).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Jim R. Esquea
Assistant Secretary for Legislation

Attachment

GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "HEALTHCARE.GOV: ACTIONS NEEDED TO ADDRESS WEAKNESSES IN INFORMATION SECURITY AND PRIVACY CONTROLS" (GAO-14-730)

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on this draft report.

The privacy and security of consumers' personally identifiable information (PII) are a top priority for HHS and CMS. As part of that effort, and as noted in GAO's draft report, within HHS, CMS has taken many steps and implemented several security controls to secure PII related to the Federally-Facilitated Marketplace (FFM) and its supporting databases. CMS developed the Marketplace systems consistent with federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. Components of the website that are operational have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institute of Standards and Technology (NIST). Marketplace systems are also in compliance with all the relevant privacy and security statutes, including the Privacy Act. Additionally, the Internal Revenue Service accepted the CMS Safeguard Procedures Report as certification that the confidentiality of federal tax information disclosed to CMS would be adequately protected.

In addition to the security controls examined by GAO in this report, CMS has implemented other measures to protect PII, including penetration testing, which happens on an ongoing basis using industry best practices to appropriately safeguard consumers' personal information. As part of the ongoing testing process, and in line with federal and industry standards, any open risk findings are appropriately addressed with risk mitigation strategies and compensating controls. The security of the system is also monitored by sensors and other tools to deter and prevent unauthorized access. CMS conducts continuous monitoring using a 24/7, multi-layer IT professional security team, added penetration testing, and a change management process that includes ongoing testing and mitigation strategies implemented in real time. These layered controls help protect the privacy and security of PII related to the FFM.

CMS acknowledges that risks exist inherently for every IT system, and appreciates GAO's suggestion of controls and processes that could be improved to further reduce or mitigate risk.

Government Accountability Office Findings

CMS does not concur with GAO's finding that CMS accepted significant security risks when it granted the FFM and the Hub an Authority to Operate (ATO) in September 2013 and allowed states to connect to the Hub. CMS does not concur for the following reasons:

The Hub completed its independent Security Controls Assessment with no high findings on August 23, 2013, and received an ATO on September 6, 2013. The completion of this testing confirms that the Hub complies with federal standards and that HHS and CMS have implemented the appropriate procedures and safeguards necessary for the Hub to operate securely beginning October 1, 2013.

1

[redacted]

Additionally, CMS leadership issued an ATO on September 27, 2013, to operate the FFM application. The initial authorization was limited to six months and was conditioned on a number of strategies to mitigate risks outlined in the ATO, including regular testing that exceeds best practices. As GAO notes, the risk mitigation strategies and compensating controls that were prescribed were implemented and executed as planned.

An independent security control assessor tested each piece of the FFM that went live October 1, 2013, prior to that date with no open high findings. All high, moderate, and low security risk findings for the portions of the website that launched October 1 were either fixed or had strategies and plans that met industry standards in place to fix the findings. The September 3, 2013, ATO identified in the report was only for the Qualified Health Plan and Dental Modules of the website. This September 3, 2013, ATO is separate from the September 27, 2013, ATO for the FFM and the parts of the website that launched on October 1.

Finally, in keeping with industry practice, CMS established strong security controls and standards for each state to meet in order to connect to the Hub. These controls and standards are based on federal security guidelines. Each state had to sign a Computer Matching Agreement, an Interconnection Security Agreement, and an Information Exchange Agreement, all of which bind the state to rules and operating procedures related to data security and privacy. Additionally, each state was required to complete a security plan, a risk assessment which can either be a self-assessment or a third-party assessment, and a corrective action plan to address risks. Every state that was connected to the Hub adhered to these procedures.

CMS acknowledges that it accepted risk in authorizing the FFM to operate or authorizing states to connect to the Hub. However, it disagrees with GAO's classification of the risk as "significant." Every system operates under some level of risk. The purpose of an ATO, as described in NIST 800-18, is to have a senior management official accept the associated risk of authorizing a system to process information.

GAO Recommendation
Ensure that the system security plans for the FFM and Hub contain all the information recommended by NIST.

CMS Response
CMS partially concurs with the recommendation. CMS notes that the CMS Master Security Plan identifies all the agency-level common controls at CMS and these controls were tested on September 6, 2013. Additionally, the Enterprise Information Security Group within the CMS Office of Information Services owns and tests inheritable agency level controls. These are tested on a regular basis as required by NIST. The system security plans of those systems inheriting the common controls (FFM and Hub) did not adequately document those inherited controls, which CMS will correct.

GAO Recommendation

2

[redacted]

Ensure that all privacy risks associated with HealthCare.gov are analyzed and documented in their privacy impact assessments (PIAs).

CMS Response
CMS partially concurs with the recommendation. As GAO notes, CMS developed and documented PIAs for the FFM and the Hub and will have the MIDAS PIA completed before the next open enrollment period begins. The PIAs for the FFM and the Hub were created using the HHS PIA template, which contains a series of questions that must be answered in the PIA to meet the requirements under Section 208 of the eGov Act. The HHS PIA template, which is used for the FFM and the Hub, asks for additional information, going beyond the requirements set by the Office of Management and Budget (OMB) Guidance on privacy impact assessments (M-03-22).

GAO Recommendation
Develop separate computer matching agreements with Office of Personnel Management (OPM) and the Peace Corps to govern the data that is being compared with CMS data for the purposes of verifying eligibility for advance premium tax credits and cost-sharing reductions.

CMS Response
CMS concurs with this recommendation and will commence discussions with OPM and Peace Corps.

GAO Recommendation
Perform a comprehensive security assessment of the FFM including the infrastructure, platform, and all deployed software elements.

CMS Response
CMS concurs that comprehensive security assessments are important, and CMS will continue to test functionality as they become operational through quarterly Security Control Assessments (SCA). CMS disagrees that the infrastructure, platform, or software elements were not tested. An SCA was completed separately for the Infrastructure as a Service and Platform as a Service that host FFM systems, and ATOs were granted, on November 23, 2012, and January 25, 2013, respectively. Another SCA for the infrastructure and platform will be conducted in October 2014. Additionally, in June 2014, the FFM security controls were tested for the fifth time. This test included the application servers and gateway and border devices.

CMS conducts end-to-end comprehensive SCAs in the FFM that are above industry standards. In December 2013, there was a comprehensive FFM SCA that met all industry standards, was an end-to-end test and was conducted in a stable environment with no open high findings. Another comprehensive end-to-end test will be conducted in September 2014, which will test security for open enrollment and plan year functionality.

GAO Recommendation

3

[redacted]

Ensure that the planned alternate processing site for the systems supporting HealthCare.gov is established and made operational in a timely fashion.

CMS Response
CMS concurs with this recommendation. Under a contract with Hewlett-Packard, the backup site is being developed and will be operational by next year. Until then, there is a limited disaster management site.

GAO Recommendation
Establish detailed security roles and responsibilities for contractors, including participation in security controls reviews, to better ensure that communications between individuals and entities with responsibility for the security of the FFM and its supporting infrastructure are effective.

CMS Response
CMS concurs with this recommendation. The CMS Chief Information Officer and Chief Information Security Officer have a unified and comprehensive view of the security of the Marketplace, and work to better ensure that the individuals and entities responsible for the security of the FFM and its supporting system are managed and informed as appropriate. CMS ensured a shared understanding of FFM security when appropriate by using the same security contractor and testing team member for all related security testing including for infrastructure, platform, and cyclical audits. Additionally, the independent test team had a shared knowledge of the development of the system and application. CMS balanced the shared understanding with the FISMA-identified fundamental principles of "need to know" and "separation of duties."

GAO Recommendation
In a separate report, GAO made 22 technical recommendations.

CMS Response
CMS concurred with all of the technical recommendations. Of the 22 technical recommendations, 19 have been resolved, fully mitigated, or will be further reviewed prior to open enrollment. The remaining open findings are being remediated and will be closed by the middle of September.

4

Appendix III: Comments from the Department of Veterans Affairs

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

September 3, 2014

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"HEALTHCARE.GOV: Actions Needed to Address Weaknesses in Information Security and Privacy Controls"*** (GAO-14-729SU). VA generally agrees with GAO's conclusions.

The enclosure provides technical comments to the draft report. VA appreciates the opportunity to comment on your draft report.

Sincerely,

Jose D. Riojas
Chief of Staff

Enclosure

Appendix IV: GAO Contacts and Staff Acknowledgements

GAO Contacts	Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov Gregory C. Wilshusen (202) 512-6244, wilshuseng@gao.gov
Staff Acknowledgments	In addition to the contacts named above, John de Ferrari, Lon Chin, West Coile and Duc Ngo (assistant directors), Mark Canter, Marisol Cruz, Sandra George, Nancy Glover, Torrey Hardee, Tammi Kalugdan, Monica Perez-Nelson, Justin Palk, and Michael Stevens made key contributions to this report.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Forbes

The Unhealthy Truth About Obamacare's Contractors

By Udayan Gupta

On July 16 of this year, Sarah Kliff posted a prescient piece on the Washington Post's Wonkblog. The post, "Meet Serco, the private firm getting $1.2 billion to process your Obamacare application," reported that 90 percent of Serco's U.S. business is with the federal government and that the 25-year-old firm pretty much owes its existence to government contracting.

THE BLAZE

White House Hired Sham Foreign Company for Obamacare, Employees 'Do Nothing'

May 22, 2014 10:09am

Akash Chougule

- Washington Free Beacon - http://freebeacon.com -

Obamacare Serco Scandal Grows

Posted By Washington Free Beacon Staff On May 20, 2014 @ 9:09 am In Issues | No Comments

More employees from the embattled Obamacare contractor Serco are stepping forward with allegations they are being paid to do nothing, KLOR-MO reports.

Chris Nagus with KMOV broke the story last week of a Missouri Serco office where employees at a paper Obamacare processing office had no work to do.

Following his report, Nagus spoke with employees from a Rogers, Arkansas Serco office. The employees were afraid of retribution so their identities were protected.

Some of the familiar allegations include one man who said he has processed about 40 health insurance applications in six months. Moreover, the Rogers office had a day and night shift to make outbound calls. An unnamed worker told Nagus they are prohibited from calling anyone after 9 and yet are required to stay on the clock until midnight.

"So why even be there until midnight?" Nagus asked.

"I don't know," said the Serco employee. "Good question."

"So they make the calls stop at 9, so from 9 to midnight are the callers kind of bored?" Nagus continued.

"Yeah, there's nothing going on," the employee said. He added workers were not allowed to leave early.

The Rogers, Arkansas Serco office is still hiring even though there is little work. Several other anonymous Serco workers told the local media attendance is more important than processing applications, even if there is nothing to do.

Article printed from Washington Free Beacon: **http://freebeacon.com**

URL to article: **http://freebeacon.com/issues/obamacare-serco-scandal-grows/**

NATIONAL REVIEW ONLINE WWW.NATIONALREVIEW.COM PRINT

OCTOBER 30, 2013 4:00 AM

Serco's Checkered History

Red flags have gone up concerning operations of the giant company around the world.

By Jillian Kay Melchior

The CEO of Serco, a British-based company whose North American division received one of the largest contracts to work on the Obamacare insurance exchanges,[1] resigned Friday amid allegations that the company had defrauded the British government of millions of pounds.

Even as myriad other allegations emerged about its work around the globe, Serco spent heavily on lobbying in Washington, D.C., and secured a multi-year contract potentially worth $1.249 billion to handle paper applications for the Obamacare exchanges. Serco did not respond to e-mail and voice-mail requests for comment.

Public records demonstrate Serco's concentrated effort to woo the U.S. government. In recent years, it has spent more than a million dollars[2] on lobbying and political activities, including $6,450 donated to President Obama's election campaign, according to the Sunlight Foundation.[3] This year, as the Centers for Medicare & Medicaid Services (CMS) was considering proposals for insurance-exchange work, Serco spent $100,000[4] to hire Greenberg Traurig, former home of Jack Abramoff, to lobby regarding the "implementation of [the] Patient Protection and Affordable Care Act," according to January registration papers.[5]

Among the Greenberg Traurig lobbyists working on the Serco account was Mark Hayes,[6] a former Senate health-policy aide.[7] During his time on Capitol Hill, Hayes "was instrumental in the key coverage, financing and delivery system reform provisions of the Patient Protection and Affordable Care Act," according to his Greenberg Traurig bio, and "acted as lead Republican staff negotiator for the 'Group of Six' health-care reform negotiations."[8] Less than a year after the ACA was signed, Hayes left Capitol Hill to become a lobbyist, representing several health-sector clients.[9]

Earlier this year, Hayes became a central subject of a federal insider-trading investigation.[10] The *Washington Post* reported that Hayes had sent information on April 1 about a significant Medicare policy change to an analyst at Height Securities. The analyst then "sent out an alert to Height's hundreds of investor clients — ahead of the administration's public announcement — and trading in Humana, Aetna, and other health-care stocks immediately soared."[11] Hayes could not be reached for comment, and it's unclear whether the investigation is continuing. Papers filed in May, after the incident, stated that Hayes was expected to cease lobbying for

Serco.[12]

Regardless of the recent federal scrutiny of Hayes, Serco's big spending seems to have paid off. In early July, the Obama administration awarded Serco a contract worth up to $1.249 billion[13] to manage paper applications for the new insurance exchanges. The company will determine eligibility for tax credits, Medicaid,[14] and exemptions from tax penalties.[15] Privacy concerns have already arisen, because in 2011, a data breach at the U.S. Thrift Savings Plan for federal employees – managed by Serco — jeopardized the Social Security numbers and confidential information of more than 120,000 participants.[16]

Just weeks after the Obama administration announced Serco's contract award, news broke that Britain's Serious Fraud Office had opened an investigation into the corporation, which had government contracts to electronically monitor criminals released from prison. An audit discovered that Serco and another company may have been overbilling the government by as much as $80.8 million. As many as one in six criminals whose monitoring was being paid for by the British government were reportedly either dead, back behind bars, no longer under supervision, or no longer living in the U.K.[17]

Furthermore, although U.S. companies that are part of a foreign company are obligated to report any billing wrongdoings abroad, Serco did not give CMS such notice, Reuters reported in July.[18] Nevertheless, the Obama administration defended its decision to award the $1.249 billion contract to Serco, claiming it was a "highly skilled company" with "a proven track record in providing cost-effective services to numerous other federal agencies."[19]

Shortly after that, more red flags went up. In August, the London police opened an investigation into Serco after allegations that it had falsified documents for another government contract for transporting defendants from confinement to court. Serco had repeatedly delivered prisoners late, and after it received a warning last summer, evidence emerged of "potentially fraudulent behavior," according to the U.K. secretary of state for justice.[20] Shortly thereafter, Serco said it had "identified misreporting" among its employees.[21]

Even so, in late September, the U.S. amended Serco's CMS contract, adding $87 million in value,[22], though it's unclear what work that will entail or whether it will add to the $1.249 billion potential worth of the original contract. As of this writing, contract officers and media spokespeople from CMS had not responded to NATIONAL REVIEW ONLINE's requests for more details.

Serco's big role in the Obamacare exchanges is even more disturbing in the light of its record with the British National Health Service.

In 2006, Serco won a contract to provide out-of-hours physician service in Cornwall, England. *Guardian* reporter Felicity Lawrence reported that the quality of service promptly declined, as

Serco cut costs by cutting staff. Reportedly, there were sometimes more than 90 patients at a time waiting on the telephone help line. And according to whistleblowers, Serco on at least one occasion, had only one general practitioner available overnight for the entire county.[23] Furthermore, "in 2010," Lawrence wrote, "a Cornish boy, Ethan Kerrigan, six, died as a result of a burst appendix when the Serco out-of-hours service advised putting him to bed rather than sending a [general practitioner] to examine him."[24]

The Care Quality Commission, which regulates British health services, soon found that Serco's managers "routinely altered daily performance reports which showed if the service was meeting its targets for responding to calls from patients on time." [25] And in March 2013, the National Audit Office reported that within a six-month period Serco had on 252 occasions made "unauthorized changes to performance data" that it offered to the NHS about its operations in Cornwall to hide poor performance and create a favorable impression.

Nor are the Cornwall derelictions Serco's only health-care debacle. In 2009, the British government awarded a $1.29 billion contract outsourcing its biggest pathology lab to GSTS Pathology, a joint venture of Serco, King's College Hospital, and Guy's & St. Thomas' Hospital. In 2011, the pathology lab saw a whopping 400 "clinical incidents"; these errors included blood and tissue samples' being mislabeled or lost altogether, the *Guardian* reported. Records requests by Corporate Watch, a not-for-profit organization, revealed that one patient got the wrong blood-test results, and another got inaccurate results for a kidney-damage test.[26] The Care Quality Commission reported in June 2012 that GSTS had failed to comply with regulations for staff training and supervision.[27]

Recent news outside the health-care sector has also called Serco's ethical standing into question.

Last month in Britain, a 23-year-old Romani woman claimed that at Yarl's Wood immigration detention center — which is run on contract by Serco — officers coerced women to engage with them sexually, "offer[ing] to make life easier, saying they would have more chance of winning their case or staying in the country" if they acquiesced.[28] Since then, three more women have made similar allegations about inappropriate sexual behavior at Yarl's Wood.[29] And last year, three staffers at Yarl's Wood were dismissed after allegations of "sexually inappropriate behavior."[30] Earlier this year, Serco "paid an undisclosed sum to a 29-year-old asylum seeker from Pakistan who claimed she was sexually assaulted by a nurse at Yarl's Wood, although the company did not admit liability," the *Guardian* reported.[31]

Furthermore, in 2004, a 14-year-old boy, Adam Rickwood, committed suicide at a Serco-run youth facility, becoming the youngest person to die in British custody in modern times. At the inquest, the jury found that staff had inappropriately used a violent restraint method against Rickwood, who had already been saying he would commit suicide if forced to remain in the facility.[32] Staffers had hit him in the nose, giving him a severe nosebleed that was untreated,

the inquest found. Shortly afterward, Rickwood hanged himself with a pair of shoelaces.[33]

NATIONAL REVIEW spoke with Harriet Wistrich, a lawyer for several of the Yarl's Wood women. She said that though she has direct knowledge only of the detention-center operations of Serco, she thinks the American public has reason to question the $1.249 billion contract award.

"Serco has got a lot of bad marks about it," Wistrich says, adding that it is "far too large, and that means that they can get away with scandals without it really affecting their ability to carry on bidding for things."

Allegations have also emerged in Australia about significant problems at Serco-run facilities. Last year, a 2010 Serco training manual was leaked online. It detailed how employees could use physical force to control those held at immigration detention centers, including punches, baton strikes, kicks, and temporarily debilitating blows to pressure points.[34] The Australian minister for immigration and citizenship said that the manual, which had since been replaced, did "not reflect very clear guidelines agreed to by Serco and the Department of Immigration on engagement with people in detention facilities."[35]

A 2011 inspection by the Australian government found "dangerous overcrowding, inadequate and ill-trained staff, no crisis planning and no requirement that Serco add employees when population exceeded capacity" in the Serco-run facilities.[36] And in September 2013, *Guardian* reporters discovered that though Serco was contractually required to submit regular reports to the Australian government about several of its detention centers, it had failed to do so.[37] Furthermore, the Australian government has found that since Serco took over facilities, instances of self-harm by immigrant detainees, including children, have increased significantly. [38][39]

The Obama administration must have known about Serco's checkered history, even as it was being lobbied to award the corporation an ACA insurance-exchange contract. Any one of these scandals would have been troubling enough, but taken together they make you wonder what the U.S. government was thinking — as with so much of the rest of Obamacare.

— Jillian Kay Melchior is a Thomas L. Rhodes Fellow for the Franklin Center for Government and Public Integrity.

EDITOR'S NOTE: This article has been amended since its initial posting.

[1] http://reporting.sunlightfoundation.com/2013/aca-contractors/

[2] http://reporting.sunlightfoundation.com/2013/aca-contractors/

[3] http://reporting.sunlightfoundation.com/2013/aca-contractors/

[4] http://www.opensecrets.org/lobby/firmsum.php?id=D000000344&year=2013

[5] http://soprweb.senate.gov/index.cfm?event=getFilingDetails&filingID=6b0a...

[6] http://www.opensecrets.org/lobby/lobbyist.php?id=Y0000044727L&year=2013

[7] http://dc.citybizlist.com/article/mark-hayes-joins-greenberg-traurig-its...

[8] http://www.gtlaw.com/People/HayesMark?tab=fullBio

[9] http://www.opensecrets.org/lobby/lobbyist.php?id=Y0000044727L&year=2013

[10] http://stream.wsj.com/story/latest-headlines/SS-2-63399/SS-2-294024/

[11] http://articles.washingtonpost.com/2013-05-06/business/39064677_1_greenb...

[12] http://soprweb.senate.gov/index.cfm?event=getFilingDetails&filingID=90f1...

[13] http://1.usa.gov/1ePW2R9

[14] http://www.ft.com/intl/cms/s/0/7415d1cc-ea3b-11e2-b2f4-00144feabdc0.html...

[15] http://www.nytimes.com/2013/07/05/health/british-company-is-awarded-cont...

[16] http://www.securityweek.com/serco-quietly-announces-server-hack-affected...

[17] http://www.telegraph.co.uk/news/uknews/crime/10337602/Serco-referred-to-...

[18] http://www.reuters.com/article/2013/07/16/us-usa-healthcare-serco-idUSBR...

[19] http://www.reuters.com/article/2013/07/16/us-usa-healthcare-serco-idUSBR...

[20] http://www.telegraph.co.uk/news/politics/10272109/Serco-staff-investigat...

[21] http://www.telegraph.co.uk/finance/newsbysector/supportservices/10272814...

[22] http://www.usaspending.gov/explore?tab=By+Prime+Awardee&typeofview=compl...

[23] http://www.theguardian.com/business/2012/jun/01/serco-allegations-out-ho...

[24] http://www.theguardian.com/society/2012/may/25/questions-outsource-nhs-care

[25] http://www.cqc.org.uk/media/cqc-publishes-report-out-hours-gp-services-c...

[26] http://www.theguardian.com/society/2012/sep/30/pathology-labs-takeover-f...

[27] http://www.corpwatch.org/article.php?id=15790

[28] http://www.theguardian.com/uk-news/2013/sep/14/detainees-yarls-wood-sexu...

[29] http://www.theguardian.com/uk-news/2013/sep/21/sexual-abuse-yarls-wood-i...

[30] http://www.theguardian.com/uk-news/2013/sep/14/detainees-yarls-wood-sexu...

[31] http://www.theguardian.com/uk-news/2013/sep/14/detainees-yarls-wood-sexu...

[32] http://www.dailymail.co.uk/news/article-1351137/Jury-finds-unlawful-forc...

[33] http://www.theguardian.com/society/2011/jan/13/adam-rickwood-inquest-cus...

[34] http://issuu.com/crikey/docs/serco_manual?e=3600405/2599388

[35] http://www.smh.com.au/wa-news/government-takes-baton-to-old-serco-detent...

[36] http://www.nytimes.com/2011/09/29/world/asia/getting-tough-on-immigrants...

[37] http://www.theguardian.com/world/2013/sep/16/g4s-serco-australia-asylum-...

[38] http://www.ombudsman.gov.au/files/suicide_and_self-harm_in_the_immigrati...

[39] http://www.nytimes.com/2011/09/29/world/asia/getting-tough-on-immigrants...

The Blaze

White House Hired Sham Foreign Company for Obamacare, Employees 'Do Nothing'

May. 22, 2014 10:00am

Akash Chougule

Just when you thought the unfolding saga of Obamacare couldn't get any stranger, it does. Witness last week's bombshell – a whistleblower alleges American taxpayers are paying workers "to do nothing but sit at their computers."

First reported by KMOV News 4, the whistleblower painted a picture reminiscent of the cult classic "Office Space," telling the St. Louis station that employees went weeks literally doing nothing. What were they supposed to be doing? Processing ObamaCare paper applications.

Instead, they were sitting around playing games – all on the American taxpayer's dime.

Lavonne Takatz worked from October to April at the Wentzville, Missouri facility where the transgressions occurred. She told the St. Louis Post-Dispatch: "We played Pictionary. We played 20 Questions. We played Trivial Pursuit."

Another former employee told KMOV management told them to "act like we were working" and "look at the screen as if we were reading things." Employees were banned from speaking to the media, even after they left the company. The company is called Serco, a British firm awarded a $1.2 billion contract to manage paper applications for President Obama's health care law.

Instead, they were sitting around playing games – all on the American taxpayer's dime.

Share:

Serco was a boondoggle of its own amidst Obamacare's disastrous rollout. The former Serco employee explained that there were 1,800 people waiting to get one out of 20 applications that came through.

Since the workload was so light, they were told "to sit at their computers and hit the refresh button...no more than every 10 minutes." If they refreshed more than that, they were called into a supervisor's office and told to stop, reported the Post-Dispatch. Takatz says that Serco even provided books to read.

According to Center for Medicare and Medicaid Services (CMS) data, throughout October and November only 17 percent of exchange applications were on paper – far below the one-third rate the Congressional Budget Office projected. And yet at the same time there was a

backlog of 50,000 to 60,000 paper applications – each representing a customer left in the dark about their status.

The Obama Administration awarded Serco with the contract last summer. Of course, as has been the case with so many recipients of this administration's generosity, a cloud of insider politics hangs over the award.

Serco spent more than $1 million on lobbying and other political activities, including a donation to the Obama campaign – presumably common practice for a company that does 90 percent of its business with the federal government.

Interestingly, one of Serco's hired lobbyists, Mark Hayes, was the central subject of an insider-trading investigation. But Serco's dark history goes far beyond one lobbyist – it appears to stretch across the Atlantic Ocean.

Just days after Serco was awarded the Obamacare contract, they came under investigation from Britain's Serious Fraud Office. An audit discovered that Serco and another company had been overbilling the government by over $80 billion (USD). Serco, Inc. in the United States did not alert the government that their parent company was under foreign investigation, despite being required by law to do so.

No US questioned the contract issued to Serco during the summer of 2013 – but now they are looking at the contributions the company made to the Obama campaign and the companies transgressions in Britain and Australia. Chip Somodevilla/Getty Images

In August, London police investigated allegations that Serco falsified documents on a British government contract. In 2006, they were contracted to provide certain healthcare services in England, but the Guardian found that quality of service had declined drastically as a result. Another contract in 2011 resulted in 400 "clinical incidents." In March of 2013, Britain's National Audit Office found that Serco had made "unauthorized changes to performance data" 252 times in six months.

However, ineptitude and employee boredom have not been Serco's only problems. Multiple reports have surfaced of staff being physically and sexually violent at another Serco-run facility, leading the Australian government to join the British in their suspicion of the worldwide corporation.

Given the seriousness of the various allegations against Serco, the Obama administration must have known about the company's troubling past, and yet they were awarded the enormous taxpayer-funded contract anyway.

As Jillian Kay Melchior wrote for National Review, "Any one of these scandals would have been troubling enough, but taken together they make you wonder what the U.S. government was thinking — as with so much of the rest of Obamacare."

Now, members of Congress want CMS to respond to questions that should have been answered long ago – before the rollout, before Serco was awarded the gigantic contract, before Obamacare was passed and signed into law.

Unfortunately, as with many of Obamacare's expensive consequences, it is too little too late.

Lavonne Takatz told the Post-Dispatch she feels like she "was stealing money from people." If only the Obama administration shared her concern.

Akash Chougule is a policy analyst at Americans for Prosperity.

U.S. House of Representatives

Committee on Oversight and Government Reform

Darrell Issa (CA-49), Chairman

Behind the Curtain of the HealthCare.gov Rollout

MAJORITY STAFF REPORT
U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
SEPTEMBER 18, 2014

Table of Contents

EXECUTIVE SUMMARY

The Obama Administration entrusted the Centers for Medicare and Medicaid Services (CMS) with the lead role in the implementation of the Patient Protection and Affordable Care Act, or ObamaCare. Within CMS, the Center for Consumer Information and Insurance Oversight (CCIIO) was responsible for developing and operating the federally-facilitated exchange, or federally-facilitated market place (FFM), in the 36 states that declined to set up their own state exchange.

In what would prove to be a very prescient observation, on May 11, 2010, Jonathan Gruber, considered by many as an architect of ObamaCare, questioned whether the Administration could get the job done: "I do not believe the relevant members of the Administration understand the President's vision or have the capability to carry it out."[1] In particular, Mr. Gruber singled out CMS, writing that "[t]he agency is demoralized, the best people have left, [and the] IT services are antiquated ...."[2] Part of Mr. Gruber's concerns can be illustrated by the launch of the law's first open enrollment season. After more than three years of development at CMS, Healthcare.gov crashed almost immediately. As a result, users experienced long wait times, errors, bugs, and other problems.

For the past four years, the Oversight and Government Reform Committee has conducted vigorous oversight of the implementation of ObamaCare, including the disastrous launch of Healthcare.gov. The problems regarding CMS's failure to launch a functioning website are consistent with broader issues in transparency and accountability within the Administration. Officials at CMS and HHS refused to admit to the public that the website was not on track to launch without significant functionality problems and substantial security risks. There is also evidence that the Administration, to this day, is continuing its efforts to shield ongoing problems with the website from public view.

Despite its position within the Department of Health and Human Services (HHS), the CMS development team resisted greater involvement from senior HHS officials, opting to bypass HHS and instead work through Senior White House official Todd Park. The broken lines of communication between CMS and HHS continued throughout the project's development. Eventually, CMS shared so little information that Bryan Sivak, HHS Chief Technology Officer, sought informal reports from former HHS employees tasked to CMS to help with Healthcare.gov, often communicating over non-official, private email. The hostility between CMS and HHS ultimately proved detrimental to the project. For example, after Mr. Sivak received evidence from an informant that Healthcare.gov was not ready to launch on October 1, 2013, Mr. Sivak and other senior HHS IT officials suggested a phased launch, or Beta launch, instead of launching the website nationwide. This suggestion was ignored by senior HHS and CMS leadership.

In addition to conflicts between CMS and HHS, documents obtained by the Committee show hostile factions within CMS itself, particularly over website security. Teresa Fryer, CMS

[1] Memorandum from David Cutler, to Larry Summers (May 11, 2010), *available at* http://www.washingtonpost.com/blogs/wonkblog/files/2013/11/Cutler-implementation-memo-1.pdf.
[2] *Id.*

Chief Information Security Officer, testified that other CMS officials obscured the true nature of the security problems in the days leading up to the launch: "[O]ur job as security experts is to portray the posture or the events that are happening and to brief senior leadership management on the security issues that are being raised during testing. And I felt that they were not being properly briefed or properly portrayed, the issues that were happening that week during security testing."[3] Ms. Fryer's team was challenged by Thomas Schankweiler, an Information Security Officer at CMS, who led security efforts for the CMS team responsible for the development of the FFM. When the MITRE Corporation's independent assessment of the website showed significant problems with the website's security, Mr. Schankweiler criticized the accuracy of the report and sought to change it.

The federal exchange launched on October 1, 2013, despite concerns raised by Ms. Fryer. CMS went through an unprecedented process in order to authorize the exchange: for the first time, Administrator Marilyn Tavenner, instead of the Chief Information Officer, signed the document authorizing the system to go live and launched the website. Rather than being transparent about this process, CMS sought to hide this from state partners and other oversight entities. These examples illustrate a larger pattern of deception surrounding the Administration's implementation of ObamaCare.

Although many of these problems originated with CMS, it is HHS and the Administration who ultimately bear responsibility for the failures with the agency's poor management and oversight. The frustration with the Administration's lack of accountability can best be summed up in a November 2013 email sent by an HHS employee to Mr. Sivak:

> Here is what I don't understand. Is there some misunderstood 'understanding' going on here? I mean it is a complete embarrassment for the President to get up and say 'he never knew' that there was [sic] problems prior to Oct. 1. Either that is a lie (I don't particularly believe he is a blatant liar) or his staff is not communicating. I mean you knew it, but your leadership only wanted to hear beautiful music and talk about rainbows and unicorns. [United States Chief Technology Officer] Todd [Park] had to have known it, but somehow he had the utmost faith in [CMS Deputy CIO] Henry [Chao] and team. I'm just totally missing how it got to this point. And I don't mean the technical delivery…I mean the out and out incompetence. Unless it is some sort of conspiracy…Maybe the House of Cards is real! But clearly, these people are not smart enough to pull it off. So, yeah, I'm a little confounded. How did one week Henry Chao tell us there was no way Account Transfer would be ready, then a meeting at the White House and a week later, oh, yeah, everything is back on track, we'll meet the dates? That's what I mean by WTF. You could definitely see the CYA moves coming a mile away.[4]

Following the collapse of Healthcare.gov, the Administration endeavored to keep the true nature of the website's problems out of the public eye. Days after the launch, Administration

[3] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).

[4] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Nov. 18, 2013 3:14:35 EST). [emphasis added]

officials downplayed the website's problems by blaming the high volume of visitors to the site. However, documents show that high-ranking officials knew that high volume was not the root cause of the website's considerable functionality issues, and acknowledged that the press did not know the full story. When CMS officials learned that account creation figures were leaked to the press, they responded by further restricting access within CMS to the data. CMS officials advised consumers to contact the ObamaCare call centers, despite concerns about their effectiveness. Angry and embarrassed that software developers were bashing Healthcare.gov code on the popular website Github, CMS officials removed the code from public view.

The Administration has repeatedly attempted to obstruct Congressional investigation of the launch of Healthcare.gov. In August 2014, CMS informed the Committee that it had lost emails responsive to the Committee's subpoena of documents relevant to development of Healthcare.gov. CMS Administrator Marilyn Tavenner admitted to deleting her own emails during the time period of ObamaCare implementation. Her actions prevent Congress from conducting effective oversight, and also prevent the public from accessing information under the Freedom of Information Act (FOIA).

Even after the first open enrollment period ended, the obstruction continued. In May 2014, CMS officials stopped releasing monthly updates on the number of ObamaCare enrollees, causing even supporters of the law to question this decision. In August 2014, CMS refused to provide the *Associated Press* documents related to the exchange's security which were requested under FOIA. CMS cited unspecified security concerns which the *Associated Press* pointed out "conflicts with President Obama's promise not to withhold government information over 'speculative or abstract fears."[5] Even more recently, CMS refused to provide to the Government Accountability Office (GAO) documentation related to 13 incidents related to data security. The GAO was conducting an audit of the exchange's privacy and information security controls on behalf of 48 congressional offices.

This Committee's oversight shows multiple troubling instances where ineffective government agencies concealed information about their failures not only from their own colleagues and leaders, but also from the news media, state partners, Congress, and the American people. The examples referenced in this report raise serious concerns about the Administration's transparency and accountability over ObamaCare implementation. As the next open-enrollment period approaches, many questions still remain.

The Administration has already spent a billion dollars on a website that is still not fully operational, and it remains unclear whether the Administration has corrected the many deficiencies that led to the disastrous launch. The same government officials responsible for the lack of transparency and accountability a year ago remain in positions of authority. Administration officials must be held accountable for obstructing public and private access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[6]

---

[5] Jack Gillum, *US Won't Reveal Records on Health Website Security*, THE ASSOCIATED PRESS (Aug. 19, 2014), *available at*: http://bigstory.ap.org/article/us-wont-reveal-records-health-website-security.

[6] Jonathan Easley, *Obama Says His is the 'Most Transparent Administration in History'*, THE HILL, Feb. 14, 2013.

FINDINGS

Accountability Breakdowns

- HHS officials contemplated a "covert ops mission" to circumvent incompetent CMS officials: **"I grow weary of the bullshit passive/aggressiveness of Henry [Chao], or rather his lack of engagement to the point that we can only speculate that it is passive/aggressiveness. ... The other way to do this is through a complete covert ops mission to unseat the CMS FFE rules engine."**

- CMS refused to share information with HHS officials they felt were not adequately invested in the development of Healthcare.gov. When HHS's Frank Baitman asked CMS's Henry Chao for more visibility into the project, Mr. Chao wrote: **"If you can't recognize a burning house and its implications, what good is it to have a bunch of firemen tell you there's a burning house if you're not going to do anything about it."**

- When HHS employee Julie Herron transferred to CMS before the website's launch, she funneled information about security testing to HHS's Bryan Sivak, who told Ms. Herron **"I don't want to tell anyone that we talk anymore."** Mr. Sivak used Ms. Herron's information about system readiness results to recommend that HHS **"declare victory without fully launching [the website]."**

- CMS official Teresa Fryer acknowledged that that other CMS officials did not properly convey the true state of security testing leading up to the launch: **"Kevin Charest [HHS CISO] has asked for an update of the FFM testing by noon tomorrow and I'm going to give him a truthful update of exactly what is going on. I am tired of the cover ups."**

- When CMS officials were unhappy with the negative results of MITRE's independent security assessment, CMS's Thomas Schankweiler sought to have it changed: **"We need to hit the pause button on this report and have an internal meeting about it later next week. It is important to look at this within the context of the decision memos and ATO memo that is going up for Tony [Trenkle, CMS Chief Information Officer] and Michelle [Snyder, CMS Chief Operating Officer] to sign. ... It is very possible that this report will be reviewed at some point by OIG, and could see the light of day in other ways."**

- After the launch, HHS officials sharply criticized CMS's management leading up to the launch of Healthcare.gov. Referencing an email in which a CMS official admits the system could not handle more than 500 concurrent users, **Mr. Baitman wrote "Frankly, it's worse than I imagined!" and Mr. Sivak replied, "Anyone who has any software experience at all would read that and immediately ask what the fuck you were thinking by launching."**

Transparency Failures

- On October 6, 2013, five days after the website's disastrous launch, Todd Park, a White House official, assured the public that high volume was the reason for the so-called glitches: "These bugs were functions of volume.... Take away the volume and it works." However, high ranking CMS and HHS officials who reported to Mr. Park knew that high volume was not primarily to blame. **Two days after the launch, HHS's Bryan Sivak wrote "This is a fucking disaster. It's 1am and they don't even know what the problem is, for sure. Basic testing should have been done hours ago that hasn't been done." A CMS employee responded, "This is going to turn ugly and someone is going to leak that CMS has no clue about the problem."**

- CMS and HHS officials acknowledged that the public and the press did not know the truth about Healthcare.gov's problems. **A CMS employee wrote, "Politico has a Day 2 story that talks about the issues. Quotes NY as having the 'most detailed' explanation but it's still just stating overwhelming traffic that 'couldn't have been replicated in testing'." Mr. Sivak responded, "1. Bad architecture 2. Not enough testing. Pretty simple really."**

- CMS reduced internal access to user account metrics when the media reported accurate figures, suspecting a leak within CMS. **CMS's Marianne Bowen wrote, "[s]ome of the metrics that are being reported are showing up in newspapers and they're close enough to reality to know someone with knowledge of the metrics is talking."**

- CMS removed Healthcare.gov code from open source project, Github, for public relations reasons because developers were publicly criticizing the code: **"[t]his Github project has turned into a place for programmers to bash our system, submit service requests (!) and now people have started copying Marketplace source code that they can see and making edits to that (!!). ... I am sure there may be some blowback from this decision but I think it is better to take a short term hit with this deletion than to let this bashing of the source code continue on our official Github site on an ongoing basis."**

- In response to draft talking points that noted concerns about the lack of training for consumer representatives at the ObamaCare Call Centers, CMS's Julie Bataille wrote, **"We NEVER want to say most of this publicly. We need consumers to call us and not worry about these details."**

- In violation of federal record-keeping rules, Administrator Tavenner deleted her emails, and instructed subordinates to do so as well. In an email, dated October 5, 2013, Ms. Tavenner forwarded a complaint from Jeanne Lambrew, a key White House advisor, about call center workers giving callers incorrect information: **"Please delete this email –but please see if we can work on call script [redacted]."**

I. INTRODUCTION

Many of Healthcare.gov's failures stem from the Administration's lack of transparency and collaboration within its own agencies. Part II of this report documents counterproductive infighting between officials at the Centers for Medicare and Medicaid Services and their colleagues at the Department of Health and Human Services, as well as factions within CMS, whose tendency to look for others to blame when problems arose contributed to a complete breakdown in accountability within the Administration. Part III explores the Administration's lack of transparency with the news media, independent oversight agencies, state partners, and the American people. Part IV details how the Administration's obstruction continues, as leaders within HHS and CMS escape accountability for their actions.

II. ACCOUNTABILITY BREAKDOWNS

CMS and HHS officials failed to effectively collaborate and communicate during the testing and launch of Healthcare.gov, leading to disastrous outcomes. CMS officials developing the exchange refused to share vital information with senior IT officials at HHS, even while communicating directly with White House officials. Left out of the loop, HHS officials resorted to using informants within CMS to obtain crucial information, often communicating over private email. Furthermore, hostile factions developed within CMS, as competing groups sought to have their opinions heeded. Many administration officials acknowledged that the truth about the state of security testing was obscured by unrealistic timelines and poor communication. These tense relationships resulted in blame-shifting, little collaboration, and ultimately, a complete lack of accountability on the part of officials responsible for the Healthcare.gov debacle.

A. HHS Officials Used Informants to Obtain Information about Healthcare.gov from Secretive CMS Officials.

The relationship between CMS and HHS IT officials deteriorated in the months leading up to the website's launch, as CMS officials refused to share vital information with superiors at HHS, opting instead to communicate directly with White House officials. In January 2013, Frank Baitman, HHS Chief Information Officer (CIO), asked Tony Trenkle, CMS CIO, and Henry Chao, CMS Deputy CIO and a key manager in the development of Healthcare.gov, for greater access to information regarding the development of Healthcare.gov. Mr. Baitman wrote that "[g]iven the importance of this project to the Secretary and the White House, it'll continue to receive very high level attention; thus, we need to ensure that emerging issues – which are inevitable – are effectively understood and analyzed at the appropriate level."[7] Mr. Baitman expressed concerns about "poor information flow between policy, operational and IT planners/developers," and noted that "critical knowledge is concentrated in key personnel at CMS."[8] He recommended that critical project knowledge be "more broadly distributed" and that

[7] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Tony Trenkle, Chief Information Officer, CMS, et.al (Jan. 22, 2013) [HHS-0108861.2].
[8] *Id.*

he and Bryan Sivak, HHS Chief Technology Officer (CTO), have more "visibility" into CMS's efforts.[9]

Mr. Chao, citing a conversation he had with United States Chief Technology Officer Todd Park, disagreed with Mr. Baitman's assessment that HHS should be given more visibility into the Healthcare.gov project. Mr. Chao wrote to Mr. Trenkle that "[m]y discussion with Todd just now is sort of the opposite of what Frank [Baitman] is asking for … in order to have the so-called 'visibility' you have to at least in some way understand the complexity and vastness of the undertaking."[10] He continued:

> If you can't recognize a burning house and its implications, what good is it to have a bunch of firemen tell you there's a burning house if you're not going to do anything about it. If you want to know how many houses burned down, how many firemen you have, and how many fire engines you have then we can tell you on a monthly basis, but that would be HHS passively receiving information. If they want to play an active role then they really have to roll up their sleeves, otherwise it'll be just time wasted trying to convey issues and options to a body that is not in position to make the proper calls.[11]

Mr. Chao further questioned whether HHS was as invested in the project as CMS, writing that "[w]ithout that personal investment in establishing the basis for understanding the operational aspects of the program (which HHS clearly does not have), there is no way to have a meaningful dialogue about the issues that 'visibility' provides you."[12]

Poor communication and collaboration between CMS and HHS continued after Mr. Baitman's January 2013 email. On March 18, 2013, HHS employee Zac Jiwa complained to Mr. Sivak about the lack of transparency at CMS's Office of Information Services (OIS). CMS's secrecy created barriers to HHS's attempt to develop a program to calculate modified adjusted gross income, a key figure used to determine an applicant's eligibility for subsidies. Mr. Jiwa wrote:

> [a]t the end of the day, OIS, through its contracts with CGI and QSSI, will have to carry the torch to make this project successful. Chris [Lunt, another HHS employee] nor I can do it alone and unless they have 'marching orders', I don't see them putting the necessary resources behind it. I grow weary of the bullshit passive/aggressiveness of Henry [Chao], or rather his lack of engagement to the point that we can only speculate that it is passive/aggressiveness.[13]

Mr. Jiwa then contemplates going around CMS officials by conducting a "complete covert ops mission to unseat the CMS FFE [federally-facilitated exchange] rules engine."[14] He concludes

---

[9] *Id.*
[10] *Id.*
[11] *Id.* [emphasis added]
[12] *Id.*
[13] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Mar. 18, 2013) [SIVAK_HOGR 000017]. [emphasis added]
[14] *Id.* [emphasis added]

that "As much as I like that idea ... I think we have little chance of pulling off a coup and we do not want to bite off more than we can chew."[15]

In a September 6, 2013, email chain on cyber-security concerns, Mr. Baitman once again reiterated concerns about being kept uninformed about the development of the website. He wrote to Michelle Snyder, CMS Chief Operating Officer:

> One of the challenges I have faced is the lack of vision into the Marketplace development effort since I came onboard – as well as the Marketplace security preparations. We're just getting a copy of the hub ATO [authority to operate], and will begin to review the testing and other documentation over the weekend. The larger issue, as you well know, is with the FFM modules – where I'm told that a code freeze still has not occurred. It's going to be quite a challenge to do user acceptance and security testing, remediation, and regression testing on our timeline.[16]

He then reiterated his offer to assist CMS with "specific resources" and noted that his "offer stands" in the last month leading up to the launch.[17]

In early September 2013, Mr. Baitman arranged for his staff to conduct separate testing of the marketplace during the week of September 22, 2013, on various application scenarios (i.e. types of households, types of tax filers) and common security risks. Mr. Baitman wrote, "[a]s with all large enterprise systems, there are certain to be bugs, dead-ends, or incorrect calculations. I'd like to know about them before we go live the following week!"[18] While it is unclear whether this testing ultimately took place, Mr. Baitman's plans for separate testing indicate not only dysfunctional lines of communication between HHS and CMS, but also inherent suspicion between the two entities. HHS did not trust CMS to inform them fully, and CMS did not trust HHS to give helpful input.

An August 2013 email chain further illustrates the odd relationship between CMS and HHS on the project, as HHS officials began to secretly seek information about the project though informants. Julie Herron, a former subordinate to Mr. Sivak, had been transferred to CMS to work on activities occurring on "Day 2", referring to website components not needed on October 1st, but needed shortly afterwards. Ms. Herron funneled information to Mr. Sivak about the development of Healthcare.gov. For example, she wrote that "Jon, Ketan, & Henry [Chao] are apparently locked in the Command Center (still) working through issues and I suspect that will continue until launch."[19] Mr. Sivak indicated that he wanted to keep communications with Ms.

---

[15] *Id.* [emphasis added]

[16] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Michelle Snyder, Chief Operating Officer, CMS (Sept. 6, 2013) [HHS-0103206]. [emphasis added]

[17] *Id.*

[18] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Timothy Monteleone, Director, Capital Planning and Investment control, Dep't Health and Human Services, et. al (Sept. 11, 2013) [HHS-0106573].

[19] Email from Julie Herron, Project Manager, Dep't Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Aug. 20, 2013) [SIVAK_HOGR 000280,81].

Herron secret from CMS, writing "I don't want to tell anyone that we talk anymore :)."[20] In reply, Ms. Herron wrote "Good point."[21]

In the same email chain, Ms. Herron informed Mr. Sivak via email that she would probably not have "day-to-day access to the Day 1 work."[22] Mr. Sivak responded, "I don't see how you wouldn't get access to day 1 stuff – how are you supposed to help with day 2 if you don't know what day 1 is? ... If you don't get access, I'm probably going to start being a little bit of a dick, which will give you ample opportunity to badmouth me and gain the trust of people at CMS."[23]

On September 10, 2013, Ms. Herron forwarded Mr. Sivak a message from another staff member involved with the project. The email, titled "From Ed" read:

> I don't know who is making the calls about what gets cut and what stays. The relationships between OIS, OC [Office of Communications], and CCIIO are very opaque. CGI seems to have failed to deliver so much that all the timelines and deadlines of the last 8 months seem like a total fiction. It does not surprise me that Bryan [Sivak] has only seen parts. I would be very surprised to hear if there is a working end-to-end version in existence. I have yet to hear of one. So to your question of how I'm feeling about launch...not good. Kind of Heartbroken, actually. Whatever launches, if functional, will only technically meet the criteria of launching the exchange. It will be riddled with confusing and hard-to-use compromises. But I don't really. I'm not seeing anything that's being delivered. I'm just piecing things together through the grapevine.[24]

Mr. Sivak responded, "like I said, it's all negative. I'm going to embark on a campaign to declare victory without fully launching. We'll see."[25] Mr. Sivak testified that on September 10, 2013, he along with Frank Baitman approached HHS leadership about implementing a phased launch of Healthcare.gov, similar to a beta test.[26] Mr. Baitman and Mr. Sivak brought up the idea of a delayed launch at a meeting of HHS leadership including Deputy Secretary, Bill Corr, Director of the HHS Office of Health Reform, Mike Hash, and CMS Administrator, Marilynn Tavenner.[27] However, both testified that their suggestion was rejected.[28]

---

[20] *Id.* [emphasis added]
[21] *Id.*
[22] *Id.*
[23] *Id.* [emphasis added]
[24] Email from Julie Herron, Project Manager, Dep't Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human (Sept. 10, 2013). [emphasis added]
[25] *Id.* [emphasis added]
[26] A beta test is "a field test of the beta version of a product (as software) especially by testers outside the company developing it that is conducted prior to commercial release." (*available at:* http://www.merriam-webster.com/dictionary/beta%20test).
[27] Transcribed Interview Franklin Baitman, Chief Information Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 14, 2014); Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C. (Feb. 12, 2014).
[28] *Id.*

After the launch, Mr. Baitman and Mr. Sivak traded emails in which they sharply criticized CMS's management of the project. Mr. Sivak showed Mr. Baitman emails that were made public by Congress in the wake of Healthcare.gov's disastrous launch. In these emails, dated September 27, 2013, a CMS official working on the FFM development, wrote "the facts are that we have not successfully handled more than 500 concurrent users filling out applications in an environment that is similarly in size to Day 1 production."[29] In response, Mr. Baitman wrote "Frankly, it's worse than I imagined!"[30] Mr. Sivak replied, "Anyone who has any software experience at all would read that and immediately ask what the fuck you were thinking by launching."[31] Mr. Baitman answered, "but, and here's the thing, these people DID have software experience! Henry [Chao], Dave [Nelson], and as I understand it, Todd. Not to mention the vendors. The protestations in these files are remarkably muted given the reality."[32]

From the perspectives of Mr. Baitman and Mr. Sivak, CMS made a grave error in judgment by fully launching the website on October 1, 2013, given the problems the project had encountered. They even suggested to HHS leadership that the website launch be limited to a smaller population in order to identify and fix inevitable problems at launch. The breakdown between HHS and CMS is significant, not only because it prevented HHS from fully assisting with its resources and expertise, but also because HHS was not in a position to effectively monitor the project's progress and provide oversight when needed.

Senior Administration officials appear to have had a remarkable lack of interest in the IT progress and accepted positive reports uncritically. This sentiment can be encapsulated in a conversation between Mr. Jiwa and Mr. Sivak in November 2013. Mr. Jiwa wrote:

> Here is what I don't understand. Is there some misunderstood 'understanding' going on here? I mean it is a complete embarrassment for the President to get up and say 'he never knew' that there was problems prior to Oct. 1. Either that is a lie (I don't particularly believe he is a blatant liar) or his staff is not communicating. I mean you [Bryan Sivak] knew it, but your leadership only wanted to hear beautiful music and talk about rainbows and unicorns. Todd [Park] had to have known it, but somehow he had the utmost faith in Henry [Chao] and team. I'm just totally missing how it got to this point. And I don't mean the technical delivery…I mean the out and out incompetence. Unless it is some sort of conspiracy…Maybe the House of Cards is real! But clearly, these people are not smart enough to pull it off. So, yeah, I'm a little confounded. How did one week Henry Chao tell us there was no way Account Transfer would be ready, then a meeting at the White House and a week later, oh, yeah, everything is back on track, we'll meet the dates? That's what I mean by WTF. You could definitely see the CYA moves coming a mile away.[33]

---

[29] House Energy and Commerce Committee, *available at*: http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/20131121-Sept26to30AdministraitonEmails.pdf.

[30] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Bryan Sivak Chief Technology Officer, Dep't of Health and Human Services (Nov. 22, 2013) [SIVAK_HOGR 000170]. [emphasis added]

[31] *Id.* [emphasis added]

[32] *Id.* [emphasis added]

[33] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Nov. 18, 2013 3:14:35 EST). [emphasis added]

Ultimately, the Administration bears responsibility for ensuring that an appropriate monitoring framework was in place for the exchange's development.

B. Hostile Factions within CMS Fought About Negative Security Test Results, as Officials Sought to Alter an Unflattering Independent Security Assessment.

Two separate teams within CMS conducted security testing for the federal exchange, also known as the Federally-Facilitated Marketplace. The first team, headed by Thomas Schankweiler, an Information Security Officer at CMS, coordinated the day-to-day security activities of the FFM development, working closely with CMS Deputy CIO Henry Chao and the development team. The second team was run through the Enterprise Information Security Group (EISG) within CMS, headed by Teresa Fryer, the Chief Information Security Officer. EISG's role was to oversee the Security Control Assessment, a key milestone the system would undergo in order to begin operations. Instead of collaborating, documents show significant conflicts between Mr. Schankweiler's FFM development team and Ms. Fryer's EISG team. This counterproductive infighting contributed to poor security testing results and Mr. Schankweiler's scheme to contest negative and embarrassing findings from the independent assessment.

In late September 2013, Ms. Fryer's EISG team tasked The MITRE Corporation, a federally funded research and development firm with expertise in this area, to conduct a security assessment for the FFM. MITRE's role was to provide an independent assessment of the FFM system prior to launch. However, at the time, significant components of the FFM remained unfinished and MITRE faced difficulties in testing the system. Their inability to effectively test the system was a significant concern for both the MITRE testers and Ms. Fryer's EISG team. Because of these concerns, Ms. Fryer testified that she recommended denying the Authority to Operate (ATO) for the FFM, which would prevent the system from launching, due to concerns over problems with security testing.[34] However, other CMS employees disagreed with Ms. Fryer and advocated signing the ATO regardless of security concerns.[35]

Ms. Fryer testified she felt that the daily reports on SCA tests did not fully convey the testing challenges experienced by the security testers.[36] For example, in a September 17, 2013, email, Ms. Fryer wrote: "there were many interruptions affecting testing such as the environment was unstable and EIDM was also down. So not much testing got done."[37] Therefore, despite the fact that there were no security vulnerability "findings" during that day of testing, very little testing was actually performed given the components of the system that were inoperable that day. Ms. Fryer then wrote to Mr. Linares "Kevin Charest [HHS CISO] has asked for an update of the FFM testing by noon tomorrow and I'm going to give him a truthful update of exactly

[34] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Dec. 17, 2013).

[35] Ordinarily, the Chief Information Officer's signature on an ATO signifies that the federal system was sufficiently tested to be secure, and was ready to go-live. However, due to the problems with the security testing, CMS CIO Tony Trenkle took the unprecedented step of elevating the ATO decision to Administrator Tavenner who authorized the FFM on September 27, 2013.

[36] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).

[37] Email from Teresa Fryer, Chief Information Security Officer, CMS, to George Linares, Chief Technology Officer, CMS (Sept. 17, 2013) [HHS-0103293].

what is going on. I am tired of the cover ups."[38] In a transcribed interview, Ms. Fryer testified: "[O]ur job as security experts is to portray the posture or the events that are happening and to brief senior leadership management on the security issues that are being raised during testing. And I felt that they were not being properly being briefed or properly portrayed, the issues that were happening that week during security testing."[39]

CMS's FFM development team was harshly critical of Ms. Fryer's EISG team in return. For example, on September 17, 2013, Henry Chao criticized MITRE's security testers for conducting "business as usual." He wrote:

> This is not business as usual and I neither have the time nor patience to explain what situation we are in right now. I had hoped the SCA testers would appreciate the intent of the message of dire urgency I gave to them about wrapping up testing as early as possible, including starting on Monday, but they followed their usual procedure and did not start early until they met with all the people and got all the demos. In other words they paid no attention to me to not treat this as business as usual. If they would have started earlier and not Cut [sic] out at 5pm maybe they wouldn't be saying they don't have enough time.[40]

Chao concluded, "Security testing is of utmost importance but it is just one factor to balance among multiple factors to meet the implementation date so I appreciate any support I can get on this front." Ms. Fryer forwarded Mr. Chao's email to George Linares, CMS CTO, writing, "I am not going to continue with the bullshit email conversation with Henry."[41] Ms. Fryer then rebutted Mr. Chao's criticisms and blamed the FFM development team for the delayed timeline: "the environment wasn't available for testing on Monday" and that the hours available for security testing were "dictated by CIISG [Consumer Information and Insurance Group, the CMS group responsible for developing the exchange] and CGI."[42]

Once MITRE completed their September Security Assessment, Mr. Schankweiler's FFM development team was unhappy with the report and sought to have it changed. On September 26, 2013, Darren Lyles, one of the IT security officials assigned to the FFM development team, wrote Ms. Fryer:

> The Draft SCA [security control assessment] Report has been called into question by CGI [primary contractor building the FFM] and CIISG [Consumer Information Insurance Group, the team within CMS that works with contractors to develop the FFM and other Healthcare.gov components] Stakeholders. There are assertions made in the report that are deemed to be erroneous and misrepresentative of what

---

[38] *Id.* [emphasis added]
[39] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).
[40] Email from Henry Chao, Deputy Director of the Office of Information Services, CMS, to Teresa Fryer, Chief Information Security Officer, CMS, et. Al. (Sept. 17, 2013) [HHS-013293].
[41] *Id.*
[42] *Id.*

> actually occurred. I have attached the report that has been commented on by CGI and would like to submit this for your review."[43]

Michael Mellor, Ms. Fryer's deputy, responded to Mr. Lyles: "Keep in mind – that the purpose of the SCA is to provide an independent assessment of the security posture of a system. As part of that independent assessment, the maintainer of the system likely will not agree with all of the findings and the SCA report."[44]

Mr. Schankweiler, Mr. Lyles' superior, then responded to Mr. Mellor, insisting that the report should be reviewed by senior CMS officials and worried the report would be seen by others outside CMS: "We need to hit the pause button on this report and have an internal meeting about it later next week. It is important to look at this within the context of the decision memos and ATO memo that is going up for Tony [Trenkle, CMS Chief Information Officer] and Michelle [Snyder, CMS Chief Operating Officer] to sign."[45] Mr. Schankweiler then wrote the report was "only partially accurate, and extremely opinionated, false, misrepresentative, and inflammatory." Mr. Schankweiller noted that "It is very possible that this report will be reviewed at some point by OIG, and could see the light of day in other ways."[46] Mr. Schankweiler offered to "look at the report from the government perspective and provide ... analysis."[47]

On October 7, 2013, the lead security tester for MITRE, Milton Shomo, wrote Jane Kim, a CMS official on Ms. Fryer's EISG team, "CCIIO [Centers for Consumer Information and Insurance Oversight, one of the divisions at CMS responsible for running the exchange] and CGI Federal had some issues with some of the information in our Marketplace ... draft SCA report from the assessment we did in August and September. MITRE stands behind everything in our report as an accurate description of the assessment. I would like to be able to deliver the final report and book package as soon as we can so hopefully there will not be too much delay in getting us the word to produce the final report."[48] Ms. Kim responded that the EISG team, unlike the FFM development team, "considered the report done last week" and that they "basically agreed with all of MITRE's comments."[49]

Mr. Shomo later wrote to Ms. Kim, "My feeling is that CCIIO is dragging their feet on saying go ahead with the final report since they were somewhat unhappy with the draft report."[50] On October 9, 2013, Ms. Kim informed Ms. Fryer that "Darren [Lyles] still has not gotten back

---

[43] Email from Darren Lyles, to Teresa Fryer, Chief Information Security Officer, CMS (Sept. 26, 2013) [HHS-0017249]. [emphasis added]

[44] Email from Michael Mellor, Deputy Chief Information Security Officer, CMS, to Darrin Lyles, Information System Security Officer, CMS (Sept. 27, 2013). [emphasis in original]

[45] Email from Thomas Schankweiler, Security Officer, CMS, to Michael Mellor, Deputy Chief Information Security Officer, et. al. (Sept. 27, 2013). [emphasis added]

[46] *Id.*

[47] *Id.* [emphasis added]

[48] Email from Milton Shomo, Principal Information Systems Engineer, MITRE Corp., to Jane Kim, Office of Administrator, CMS (Oct. 7, 201, 4:06 EST). [emphasis added]

[49] Email from Jane Kim, Office of Administrator, CMS, to Milton Shomo, Principal Information Systems Engineer, MITRE Corp., (Oct. 7, 201, 4:27 EST).

[50] Email from Milton Shomo, Principal Information Systems Engineer, MITRE Corp., to Jane Kim, Office of Administrator, CMS (Oct. 7, 201, 4:36 EST).

to Jim [Bielski, MITRE tester]. At this point, I consider our draft the draft report. We've taken the legitimate concerns into account."[51]

Independent security testing is a key aspect in a systems oversight. Documents reviewed by the Committee show conflicts between those responsible for building the exchange and those responsible for assessing the system's security. MITRE testers were forced to conduct their assessment while other developers were still making changes to the system and this arrangement lead to numerous conflicts. Finally, when MITRE issued a draft report, CMS officials developing the exchange were unhappy with the results and inappropriately sought to alter the report in their favor. While there is a role for the project owners to provide feedback, security control assessments must remain fully independent from government influence to produce the desired effect: an unbiased look at the security risks inherent in the system.

III. TRANSPARENCY FAILURES

In the wake of Healthcare.gov's disastrous launch, CMS and HHS acted to obscure the full extent of the problem from public view. Despite public assurances that the website's numerous functionality errors were due to a "high volume" of users on the site, documents show that high-ranking officials knew that was not the case. To prevent more public criticism, CMS officials narrowed employee access to account user statistics in fear that accurate numbers had leaked to the press, agreed to conceal problems with call centers from the public, and removed Healthcare.gov code from an open source project intended to foster collaboration.

Recently, Administrator Tavenner informed the Committee that, in violation of federal record-keeping rules, she inappropriately deleted some of her emails that may have been responsive to Congressional inquiry. CMS's lack of transparency extended to state partners as well. When the Idaho Exchange Board requested a copy of the FFM Authority to Operate, CMS officials contemplated backdating a new document to present as the ATO instead of the true document. These examples illustrate how CMS has been hostile to transparency interests, and has hindered a full understanding of the Administration's actions during the implementation of ObamaCare.

A. High-Ranking CMS and HHS Officials Acknowledge the Public was Misinformed about Healthcare.gov's Problems after the Launch.

The high-profile, error-ridden launch of Healthcare.gov attracted significant attention from both the public and the press. Administration officials assured the public that the website was designed to handle 50,000 to 60,000 simultaneous users and that higher than expected volume caused the website to be unusable. For example, on October 6, 2013, five days after the website's launch, Todd Park told USA Today that the "bugs" causing the website to be

[51] Email from Jane Kim, Office of Administrator, CMS, to Teresa Fryer, Chief Information Security Officer, CMS (Oct. 9, 2013).

dysfunctional were entirely due to the large quantities of users visiting the site: "These bugs were functions of volume.... Take away the volume and it works."[52]

Despite their public stance, CMS decision-makers knew that the problems with Healthcare.gov were far more complicated and far-reaching than high volume, and that fixing the so-called "glitches" would be a significant and time-consuming task. Documents obtained by the Committee show that Mr. Park's assertion that Healthcare.gov could function properly with 50,000 to 60,000 users was false. On September 25, 2013, six days before the launch, Monique Outerbridge, one of CMS's primary managers on the FFM project, emailed CMS Chief Information Officer Tony Trenkle about the latest results of the performance tests. She wrote, "We just found out Healthcare.gov can only handle 10,000 concurrent users. Performance testing results in the toilet."[53] Mr. Trenkle responded, "ugh."[54]

In the days immediately following the launch, an email exchange between HHS CTO Bryan Sivak, and Julie Herron, a former employee of his who had transferred to CMS to work on the website launch, confirmed that volume was not the sole reason for the website's problems. In the email chain dated October 3, 2013, Mr. Sivak wrote that "This is a fucking disaster. It's 1am and they don't even know what the problem is, for sure. Basic testing should have been done hours ago that hasn't been done."[55] Ms. Herron responded, "This is going to turn ugly and someone is going to leak that CMS has no clue about the problem."[56] She then commented about Healthcare.gov:

> So basically effed from the start. Which means there must have been only the most basic of tests otherwise someone would have caught it. Or they knew and just crossed their fingers and hoped for the best. Politico has a Day 2 story that talks about the issues. Quotes NY as having the 'most detailed' explanation but it's still just stating overwhelming traffic that 'couldn't have been replicated in testing'.[57]

Mr. Sivak responded, "1. Bad architecture 2. Not enough testing. Pretty simple really."[58]

In her email to Mr. Sivak, Ms. Herron noted that even the "most detailed" explanation coming from the Administration was inaccurate and feared that someone would "leak" that CMS did not even know what went wrong. Later that night, Mr. Sivak updated Ms. Herron that contractors "tweaked" some elements of the website, but they are "shooting in the dark. ... They haven't identified the root cause."[59]

---

[52] Tim Mullaney, *Obama adviser: Demand overwhelmed HealthCare.gov*, USA TODAY, Oct. 6, 2013.
[53] Email between Monique Outerbridge and Tony Trenkle (Sept. 25, 2013) [HHS-0110879].
[54] *Id.* [emphasis added]
[55] Email from Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services to Julie Herron, Project Manager, Dep't Health and Human Services (Oct. 3, 2013) [SIVAK_HOGR 000038-000040]. [emphasis added]
[56] *Id.* [emphasis added]
[57] *Id.* [emphasis added]
[58] *Id.* [emphasis added]
[59] *Id.*

CMS's confusion over Healthcare.gov's capacity problems continued long after the disastrous October 1st launch. On October 13, 2013, Henry Chao emailed his team that Administrator Tavenner had asked him "[h]ow many users can the system handle?" Mr. Chao, requesting help, wrote "[g]iven the behavior of the production environment I am at a loss as to how to answer that question."[60]

B. CMS Engaged in Schemes to Conceal Vital Information from the Public.

Internal emails obtained by the Committee show that CMS and HHS personnel actively engaged in efforts to obscure the truth about Healthcare.gov's significant problems from the news media and the public. CMS officials encouraged consumers to sign up via call centers when the website was unworkable, but emphatically agreed that CMS should not tell consumers there were operational problems with call centers as well. When CMS found that the media had reported accurate account user creation figures, they immediately suspected a leak within CMS and further restricted access to the figures. Finally, despite posting portions of the Healthcare.gov source code on the website Github, initially intended to encourage improvement and collaboration between CMS and web developers, CMS decided to remove the code when developers started to criticize the code.

CMS Officials Agreed to Conceal Problems with Call Centers from Public

In the days after the immediate launch, CMS scrambled to use alternate methods for enrollment, since the website was essentially unworkable for consumers. One version of talking points, drafted by CMS Communications staff on October 5, 2013, gave a detailed explanation for how consumers could enroll on the federal exchange: online, through the call center and via paper application.[61] The talking points explained how the call centers could enroll consumers in place of the unworkable website, noted that paper applications were the least desirable option because they would take longer to process, and cautioned that there would still be some problems with CMS's alternate plan to enroll consumers.[62] For example, the talking points warned that "While all CSRs [customer service representatives] should have been trained to date, there is the possibility that some continue to direct callers to Healthcare.gov to create accounts. CSRs have also been directed to revert to PDF when the on-line tool is not available."[63] Also, the talking points noted that applying via paper application "adds time" for the determination of subsidy eligibility.[64]

In response to the draft talking points, Mary Wallace from the CMS Office of Communications asked "Who is the audience? Is this for public or just up the chain explanation?"[65] Aryana Khalid, Marilyn Tavenner's Chief of Staff, replied, "[u]p the chain at

---

[60] Email from Henry Chao, Deputy Director of the Office of Information Services, CMS, to Keith Rubin, et. al. (Oct. 13, 2013) [HHS-0021259]. [emphasis added]
[61] Email from Aryana Khalid, Chief of Staff, CMS, to Mary Wallace, Deputy Director of the Office of Communications, CMS (Oct. 6, 2013) [HHS-0135925,26].
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

WH. Not public. I want to get it right and put it to bed. They are annoying :)."[66] In response, Ms. Wallace wrote, "I don't think we ever want to explain this way to the public. That's why I was asking."[67] Julie Bataille, Director of the CMS Office of Communications chimed in, "[t]otally agree. We NEVER want to say most of this publicly. We need consumers to call us and not worry about these details. Reality is that we will need to go back and forth in the background operationally as needs arise. And I think they want to know you can apply and enrolle [sic] at the call center."[68]

However, throughout October, call centers continued to experience significant problems. CNN reported that "In the first days, half of the calls to the phone center had problems, paper applications could not be processed..."[69] Furthermore, an October 3rd document acknowledged widespread problems with the call center.[70] CMS decided to encourage the public to apply through call centers even when CMS knew that there were serious problems, such as lack of training for customer service representatives and delayed processing system for paper applications.

CMS Feared Accurate User Account Statistics Would Leak to the Press

In addition to keeping valuable information about enrollment problems from consumers, CMS officials tightly controlled access to statistics about user accounts in the days after the launch, preventing much of it from becoming public. CMS's Enterprise Identity Management System (EIDM) controls user accounts for Healthcare.gov, and EIDM statistics would record and report how many users set up accounts through Healthcare.gov. In an October 12, 2013, email, Marianne Bowen of CMS Office of the Administrator informed other CMS officials that someone within CMS had shared EIDM user account creation statistics with the press. Ms. Bowen noted that she was responsible for "pulling together metrics for the Administrator, the White House staff and this week the President related to EIDM account set up," and that QSSI, a federal contractor, updated her every hour with new metrics.[71] Ms. Bowen wrote "[s]ome of the metrics that are being reported are showing up in newspapers and they're close enough to reality to know someone with knowledge of the metrics is talking."[72] She continued: "The Administrator and Michelle [Snyder, CMS COO] have asked me to see if I can limit the CMS exposure to this information ... there are lots of CMS staff on those notes [from QSSI] that frankly don't appear to need to know this info."[73] She then asked to remove "any but the most critical CMS staff" from the hourly updates, and to "please keep the metrics close."[74]

---

[66] *Id.*
[67] Email from Julie Bataille, Deputy Director of the Office of Communications, CMS, to Mary Wallace, Deputy Director of the Office of Communications, et. al. (Oct. 6, 2013) [HHS-0135925,26].
[68] *Id.* [emphasis added]
[69] Lisa Desjardins, *Documents show first days of Obamacare rollout worse than initially realized,* CNN, Nov. 6, 2013, http://politicalticker.blogs.cnn.com/2013/11/06/documents-show-first-days-of-obamacare-rollout-worse-than-initially-realized/.
[70] *Id.*
[71] Email from Marianne Bowen, Office of the administrator, CMS, to Marc Richardson, Director, Division of Healthcare Information Systems, CMS, et. al (Oct. 12, 2013) [HHS-0103728].
[72] *Id.* [emphasis added]
[73] *Id.*
[74] *Id.*

CMS Removed Healthcare.gov Code from Open Source Website in Response to Criticism

In an April blog post, HHS touted the openness of their website, writing "everything HHS does will be published on GitHub. GitHub is an open source code repository developers can use to share and collaborate on projects."[75] In June, 2013, CMS posted code for some portions of Healthcare.gov, primarily parts of the website that provided information to the public, onto Github.

Mr. Sivak testified that posting source code on Github was a "valuable exercise" because it "leverag[ed] the whole idea is that if you can post the code and there is something that could be done better or improved, then somebody out there in the community can help you make it better and improve it."[76] For example, he explained how Github could be used to strengthen a program's security:

> One of the best ways to ensure the security of any given piece of code is to publish the source code because you have legions of experts out there who can review it and point out any flaws in the code and/or any flaws in the programming that would introduce security risks. Many eyes can solve problems like that; whereas, you know, if you keep things internally, you are never, you know, really guaranteed that all -- you know, enough people are going to be looking at something to spot any issues. It is one of the basic tenets of open source code.[77]

However, on October 11, 2013, CMS employee Jon Booth, complained to top CMS officials including Administrator Tavenner and Mr. Chao, that "this Github project has turned into a place for programmers to bash our system."[78] He recommended that CMS remove the code from Github and noted that, "I am sure there may be some blowback from this decision but I think it is better to take a short term hit with this deletion than to let this bashing of the source code continue on our official Github site on an ongoing basis."[79]

In internal discussions, CMS officials stated two reasons for removing the code: the "bad PR" associated with the online Github discussions and the feeling that it would be a "real or perceived security risk."[80] This shows a lack of understanding of how the internet works. As Mr. Sivak testified, once the source code was posted it could never be erased: "It was nearly 100 percent certainty that once the repository was deleted, somebody would have reposted it."[81] It is unlikely that CMS's concern for website security motivated the decision to remove the code,

---

[75] David Cole, *New Healthcare.gov is Open, CMS-Free,* Apr. 10, 2013, http://www.hhs.gov/digitalstrategy/blog/2013/04/new-heathcare-open-cms-free.html.
[76] Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C. (Feb. 12, 2014).
[77] *Id.* [emphasis added]
[78] Email from Jon Booth, Director, Website & New Media Group, CMS, to Marilyn Tavenner, Administrator, CMS, et. al. (Oct. 11, 2013) [HHS-0021188,89,90]. [emphasis added]
[79] *Id.* [emphasis added]
[80] *Id.*
[81] Transcribed Interview with Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C (Feb. 12, 2014).

partly because it was already publicly available for reposting, and also because the publicly released code did not handle parts of the website that dealt with personal information.

Although Mr. Booth described Mr. Sivak as the "champion" of the idea to post the source code on Github, CMS decided to remove the code without consulting Mr. Sivak and others at HHS.[82] Mr. Sivak testified that, in response to his questions, Ms. Bataille, Director of the CMS Office of Communications, told him the code was removed because CMS was concerned about the publicity the source code was getting and that CMS was afraid the public misunderstood the nature of the code.[83] Mr. Sivak testified that he would have recommended against removing the code because of the benefits that continued collaboration with the developer community would bring, and also that the code would simply be reposted by someone else once it was deleted by CMS anyway.[84]

C. Administrator Tavenner Deleted Emails, Violating Federal Record Keeping Laws and Impeding Oversight.

On October 10, 2013, Chairman Issa and Senate Health, Education, Labor and Pension Committee Ranking Member Lamar Alexander wrote to Secretary Sebelius, requesting documents related to the launch of Healthcare.gov. Due to the Administration's refusal to voluntarily provide documents responsive to the request, the Committee was forced to issue a subpoena on October 30, 2013. On August 7, 2014, more than nine months after the subpoena was issued, CMS informed the Committee that "some of Ms. Tavenner's potentially responsive emails might not be retrievable."[85]

According to a letter to the National Archives, Administrator Tavenner, had "copied or forwarded emails to immediate staff for retention and retrieval, and did not maintain her own copies." However, this practice was not followed consistently and some emails were lost as a result. While some responsive emails sent within HHS might be retrievable, CMS admitted that "[w]hile we have not identified any specific emails that we will be unable to retrieve, it is possible that some emails may not be available to HHS."[86]

Not only did the Administrator's actions prevent responsive documents from being produced for Congressional oversight, but it also restricted private citizens, the press or good government organizations from accessing documents on this and other issues affecting CMS over that time period through the Freedom of Information Act. As Freedom of Information Act expert and *Washington Examiner* editor Mark Tapscott explains, "reports and other official documents, emails, telephone text messages and instant messages on government business are

---

[82] Email from Jon Booth, Director, Website & New Media Group, CMS, to Marilyn Tavenner, Administrator, CMS, et. al. (Oct. 11, 2013) [HHS-0021188,89,90].
[83] Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health & Human, in Washington, D.C. (Feb. 12, 2014).
[84] *Id.*
[85] Letter from Jim R. Equea, Assistant Secretary for Legislation, Dep't Health & Human Services, to Rep. Darrell Issa, Chairman, H. Comm. on Oversight and Government Reform (Aug. 7, 2014).
[86] *Id.*

required to be preserved by federal record-keeping regulations... for historical purposes and because they are accessible under the Freedom of Information Act."[87]

Equally troubling is an email sent to Ms. Bataille, Director of CMS Office of Communications. In an email, dated October 5, 2013, Ms. Tavenner forwarded a complaint from Jeanne Lambrew, a key White House advisor, about call center workers giving callers incorrect information. Ms. Tavenner wrote to Ms. Bataille "Please delete this email –but please see if we can work on call script [redacted]."[88] It is unclear whether Ms. Tavenner similarly instructed other officials to delete emails from White House advisors that were forwarded to them. Given CMS's sloppy record handling official documents, it is impossible to know for sure.

D. CMS Officials Suggest Backdating Documents in Response to State Partner's Request for Security Verification Documents.

CMS's lack of transparency extended to communications with their state partners as well. On September 30, 2013, the Idaho Exchange Board requested that CMS provide them information about the federal exchange's "security assessment" in advance of a meeting during which the Board would vote on whether or not to allow the federally-facilitated marketplace to open in their state on October 1st. A CMS employee explained: "Basically, they would like to know if we have access to any of the privacy/security assessments that have been done on the FDSH [Federal Data Services Hub] whether they be internal or external reviews."[89]

Andrea Greene-Horace, a CMS CCIIO employee, explained the Board's request in further detail in an email to Mr. Schankweiler, the FFM's Information Security Officer and others. Ms. Greene-Horace wrote:

> The board members want the 'authority to operate' and want us to provide a link to the FFM's 'Authority to Operate.' They read the Office of the IG's initial review but cannot find a [sic] 'Authority to Connect' or an 'Authority to Operate' for the FFM...They would rather have the document. Please advise on your approach in case we get more requests.[90]

An Authority to Operate is a certification that a system has undergone an independent risk assessment and meets the requirements to launch. Typically, an agency's Chief Information Officer signs the ATO, but in this case, CMS CIO Tony Trenkle refused to sign it because of his concerns about MITRE's security testing results.[91] Instead, he took an unprecedented step by asking CMS Administrator Marilyn Tavenner to sign the ATO.[92] During transcribed interviews,

---

[87] Mark Tapscott, *Mailyn Tavenner's deleted emails pose wuestion: Is the FOIA the law federal officials break most often?*, Aug. 19, 2014, http://washingtonexaminer.com/marilyn-tavenners-deleted-emails-pose-question-is-the-foia-the-law-federal-officials-break-most-often/article/2552153. [emphasis added]

[88] Email from Marilyn Tavenner, Administrator, Dep't of Health and Human Services, to Julie Bataille, Director of Office of Communications, CMS (Oct. 5, 2013) [HHS-0134965].

[89] Email between CMS employees (Sept. 30, 2013) [HHS-0018435, 36].

[90] *Id.*

[91] Transcribed Interview with Tony Trenkle, Chief Information Officer, CMS, in Washington, D.C (Dec. 4, 2013).

[92] *Id.*

no CMS official interviewed by the Committee could recall another instance in which the Administrator, instead of the CIO, authorized a system to go-live.[93]

That afternoon, Mr. Schankweiler, an Information Security Officer at CMS, spoke by phone to the Idaho Exchange Board.[94] Mr. Schankweiler showed the Board the ATO for the Data Services Hub, the component that connects the exchange with state and federal agencies. However, Mr. Schankweiler refused to share the decision memo authorizing the FFM to go-live, arguing that it was "sensitive."[95] In fact, Mr. Schankweiler's testimony was required only because CMS could not provide an ATO for the FFM. Based on Schankweiler's testimony, the Board voted to proceed with the launch of YourIdahoHealth.org, without the requested documentation from CMS.[96] However, Board members expressed continued reservations about the lack of documentation.[97]

After Mr. Schankweiler spoke with the Board by teleconference, he reported back to his colleagues that they "do have one action regarding the request for follow up document to support the verbal attestation provided during [the call] ... They are now looking for document of the ATO memo for the FFM."[98] Mr. Schankweiler noted that the Board and others were "looking for the normal ATO package, with the Decision Memo standing behind it accepting the risk. There is a standard ATO memo that should be created for this. The OIG, Congress, and now the states are looking for this ATO memo. We likely will want to present that with the Decision Memo backing it up."[99]

George Linares, then-Acting CTO for CMS, concerned about requests from external parties to review the FFM's security documentation, wrote: "So in the case that external parties ask to see the FFM ATO, we need to have the standard ATO form available."[100] Mr. Linares then suggested creating a standard-looking ATO form, backdated to the date of the Decision Memo so that this document would appear to be the document certifying the exchange to go-live on October 1, even though that document did not exist.[101] Mr. Linares wrote "I am just concerned with states asking to see the ATO letter and only having the Decision Memo to show."[102] Ultimately, this backdated document was not created.

---

[93] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Dec. 17, 2013); Transcribed Interview with Tony Trenkle, Chief Information Officer, CMS, in Washington, D.C (Dec. 4, 2013); Transcribed Interview with Kevin Charest, Chief Information Security Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 8, 2014); Transcribed Interview, George Linares, Chief Technology Officer, CMS, in Washington, D.C. (Jan. 10, 2014); Transcribed Interview Franklin Baitman, Chief Information Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 14, 2014).

[94] Austin Hill, *Idaho insurance exchange votes to press forward despite concerns about data security*, IDAHO REPORTER (Sept. 30, 2013).

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] CMS email (Sept. 30, 2013) [HHS-0018433, HHS-0018434].

[99] CMS email (Sept. 30, 2013) [HHS-0018451]. [emphasis added]

[100] *Id.*

[101] *Id.*

[102] *Id.*

The discussion about backdating the ATO demonstrates that CMS officials were aware of the non-standard process used to issue the FFM ATO and considered the FFM decision memo as "sensitive." They acknowledged that if outside entities such as Congress, GAO, and the IG reviewed the memo, it would lead to additional questions on the FFM's security. To avoid that, they contemplated steps to make this memo look more legitimate.

IV. OBSTRUCTION CONTINUES AS THE ADMINISTRATION FAILS TO HOLD LEADERS ACCOUNTABLE FOR TRANSPARENCY FAILURES

Despite numerous complaints about the Administration's pattern of deception throughout ObamaCare implementation, Administration officials continue to obstruct the news media, independent oversight agencies, and congressional investigators, and conceal important information from the American public to protect their political interests. In August 2014, CMS refused to disclose federal records about the security of Healthcare.gov as requested by the *Associated Press* under the Freedom of Information Act.[103] In May 2014, the Administration stopped releasing monthly updates on ObamaCare enrollment figures, without providing any justification.[104] The Government Accountability Office informed the Committee in a briefing that CMS refused to provide GAO with reports of 13 Healthcare.gov "security incidents," even though the GAO was conducting an audit of efforts taken by CMS to ensure the site's security.[105] Officials must be held accountable for obstructing access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[106]

HHS Refused to Provide Documents Requested by the Associated Press *Under Freedom of Information Act*

In late 2013, the *Associated Press* submitted a Freedom of Information Act request for federal records regarding the security of Healthcare.gov, such as the kinds of security software and computer systems behind the federally-funded system.[107] The *Associated Press* requested the records amid concerns that the website was not secure and presented threats to personally identifiable information. However, on August 19, 2014, the Administration denied the *Associated Press* access to the documents.[108] A CMS spokesperson stated that the release of the documents "would potentially cause an unwarranted risk to consumers' private information."[109]

However, as the *Associated Press* pointed out, "the government, in its denial of the AP request, speculates that disclosing the records could possibly, but not assuredly or even probably, give hackers the keys they need to intrude" which conflicts with President Obama's promise not

---

[103] Jack Gillum, *US Won't Reveal Records on Health Website Security*, THE ASSOCIATED PRESS (Aug. 19, 2014), *available at*: http://bigstory.ap.org/article/us-wont-reveal-records-health-website-security.
[104] Kyle Cheney, *Administration Stops Monthly ACA Enrollment Reports*, POLITICO PRO (May 21, 2014).
[105] GAO Briefing with Committee staff (Aug. 27, 2014).
[106] Easley, *supra* note 6.
[107] Gillum, *supra* note 103.
[108] *Id.*
[109] *Id.*

to withhold government information over "speculative or abstract fears."[110] The *Associated Press* also quotes industry consultant David Kennedy, who testified before the Science and Technology Committee last year, as saying "Security practices aren't private information."[111] This appears to be yet another example of the Administration obstructing oversight in order to prevent public criticism in an election year. The Associated Press has asked CMS to reconsider the decision, but to date, CMS has refused to provide even redacted documents.

The Administration Stopped Releasing Monthly Updates on ObamaCare Enrollment Figures

Another example of the Administration's continued hostility to transparency is the decision to halt the release of monthly reports on ObamaCare enrollment figures. Although HHS had issued monthly reports on enrollment numbers throughout the open enrollment period, in May 2014, the Administration stopped issuing the monthly updates, which *Politico* described as a "major pipeline of information about the impact of the health law heading into the 2014 campaign season."[112] According to an administration spokesman, "HHS issued monthly enrollment reports during the first marketplace open enrollment period in order to provide the best understanding of enrollment activities as it was taking place. ... Now that this time period has ended, we will look at future opportunities to share information about the marketplace that is reliable and accurate over time as further analysis can be done but we do not anticipate monthly reports."[113]

HHS refused to provide a reason for their decision to stop releasing the reports, which had helped policymakers assess benchmarks in President Obama's hallmark program. According to *Politico*, the agency offered no information about the timing or level of detail in any future updates.[114] HHS's decision to stop updating the public on enrollment figures sparked outrage among both ObamaCare supporters and critics. Prominent ObamaCare supporter Charles Gaba, the blogger behind acasignups.net, wrote that "HHS has lost their mind and will deserve every bit of criticism that they receive over it."[115] He added, "The ACA is the Obama administration's single most important policy. Whether you support or oppose it, you have to admit that the ACA has a significant impact on the rest of the economy and many other aspects of American society. ... However, for the remainder of President Obama's term in office, at least, they should absolutely continue to issue monthly reports even during the 'off season.'"[116] An August 27, 2014, letter by U.S. Senators John Barrasso and Lamar Alexander requested updated enrollment figures, noting that the Administration has not released information on exchange enrollment since May.[117]

---

[110] *Id.*
[111] *Id.*
[112] Cheney, *supra* note 104.
[113] *Id.*
[114] *Id.*
[115] Charles Gaba, *HHS To Stop Issuing Monthly Reports*, May 21, 2014, http://acasignups.net/14/05/21/hhs-stop-issuing-monthly-reports.
[116] *Id.*
[117] Liz Wolgemuth, *Barrasso, Alexander: Americans Deserve to See New, Accurate Obamacare Enrollment Date*, Aug. 27, 2014, http://www.help.senate.gov/newsroom/press/release/?id=7efd4ccd-45eb-440f-ad76-b5a77cf5be09.

The Administration Refused to Provide the Government Accountability Office with Requested Information

In addition to obstructing policy makers and congressional investigators by refusing to make enrollment figures public, the Administration stonewalled the Government Accountability Office during a recent audit on the security of the Healthcare.gov website. Forty-eight congressional offices requested that GAO, an independent, non-partisan agency, conduct an audit of the security mechanisms CMS put in place to protect personally identifiable information through Healthcare.gov.

In the course of this audit, GAO requested to review reports for 13 "security incidents" that CMS reported had occurred to Healthcare.gov. When GAO briefed Congressional staff about the report, they revealed that CMS refused to provide copies of the reports.[118] After several requests by GAO, CMS provided a one paragraph summary, stating that none of the incidents resulted in a successful hack.[119] However, GAO was unable to draw conclusions without the actual incident reports, which CMS has refused to provide.[120]

V. CONCLUSION

The Committee's oversight shows multiple troubling instances where ineffective government agencies concealed information about failures that led to the disastrous launch of Healthcare.gov not only from their own colleagues and leaders, but also from the news media, state partners, Congress, and the American people. The examples referenced in this report raise serious concerns about Administration's transparency and accountability. As we enter into the next open-enrollment period, many questions still remain.

The Administration has already spent a billion dollars on a website that is still not fully operational, and it remains unclear whether the Administration has corrected the many deficiencies that led to the disastrous launch. The same government officials responsible for the lack of transparency and accountability remain in positions of authority. Administration officials must be held accountable for obstructing public and private access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[121]

---

[118] GAO Briefing with Committee staff (Aug. 27, 2014).
[119] *Id.*
[120] *Id.*
[121] Easley, *supra* note 6.

○