AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–867

YOUR HEALTH AND YOUR PRIVACY: PROTECTING HEALTH INFORMATION IN A DIGITAL WORLD

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

NOVEMBER 9, 2011

Serial No. J–112–51

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
87–166 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing 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 THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

AL FRANKEN, Minnesota, *Chairman*

CHUCK SCHUMER, New York
SHELDON WHITEHOUSE, Rhode Island
RICHARD BLUMENTHAL, Connecticut

TOM COBURN, Oklahoma
ORRIN G. HATCH, Utah
LINDSEY GRAHAM, South Carolina

ALVARO BEDOYA, *Democratic Chief Counsel*
ELIZABETH HAYS, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Franken, Hon. Al, a U.S. Senator from the State of Minnesota	1
Coburn, Hon. Tom, a U.S. Senator from the State of Oklahoma	4

WITNESSES

Lynch, Loretta, U.S. Attorney for the Eastern District of New York, U.S. Department of Justice, Brooklyn, New York	5
prepared statement	31
Rodriguez, Leon, Director, Office of Civil Rights, U.S. Department of Health and Human Services, Washington, DC	7
prepared statement	40
McGraw, Deven, Director, Health Privacy Project, Center for Democracy and Technology, Washington, DC	18
prepared statement	51
Myrold, Kari, Privacy Officer, Hennepin County Medical Center, Minneapolis, Minnesota	16
prepared statement	68

QUESTIONS

Questions for Deven McGraw, Leon Rodriguez, and Kari Myrold submitted by Senator Al Franken	73

QUESTIONS AND ANSWERS

Responses of Deven McGraw to Questions Submitted by Senator Franken	76
Responses of Leon Rodriguez to Questions Submitted by Senator Al Franken	78
Responses of Kari Myrold to Questions Submitted by Senator Al Franken	82

SUBMISSIONS FOR THE RECORD

Letter from AARP to Senators Patrick Leahy, Al Franken, Charles Grassley, and Tom Coburn	83

YOUR HEALTH AND YOUR PRIVACY: PROTECTING HEALTH INFORMATION IN A DIGITAL WORLD

WEDNESDAY, NOVEMBER 9, 2011

U.S. SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC

The Subcommittee met, pursuant to notice, at 2:33 p.m., Room SD–226, Dirksen Senate Office Building, Hon. Al Franken, presiding.

Present: Senators Whitehouse, Blumenthal, and Coburn.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator FRANKEN. This hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law will be called to order. This is our Subcommittee's second hearing, and this one will focus on the important issue of health privacy.

Over the past two decades, an incredible thing has happened. You can now put your entire medical history, every chart, every X-ray, every test, every last doctor's note on a thumb drive this size, and even better, once that electronic health record is put on a network, any doctor authorized on that network can access that information instantaneously from across the State or across the country.

This means you don't have to rely on your memory to tell your doctor when your last tetanus shot was. It means that in a crisis, doctors in an emergency room can find out in seconds exactly what medicines an accident victim has been prescribed, and it means that when you change doctors or move cities you can be sure that your doctors will know everything that they need to know about you and your health history.

But the most important story I've heard to explain the need for electronic health records comes from the Hennepin County Medical Center, which I'm proud to say will be represented today by Kari Myrold, their privacy officer. HCMC was one of the first hospitals in Minnesota to develop an electronic health record system. HCMC is actually about five or six blocks from my home in Minneapolis.

As it turns out, HCMC is also just one mile from the I–35W bridge in Minneapolis, which collapsed in August of 2007. One month before that bridge collapsed, they had just completed a full implementation of electronic health records throughout the hospital. But that day in August when the bridge collapsed, its policies

still called for using paper records in the event of a major catastrophe, so when the bridge collapsed and patients starting coming in, staff used paper records for the first two patients.

After those first two, the doctors made a decision to switch to electronic records. They found that it allowed them to call up patients' charts and track patients throughout the hospital and in other systems far easier than paper records. When disaster struck, that decision to use electronic health records allowed the Hennepin County Medical Center to tend to those victims more quickly and more effectively.

Examples like this one quickly persuaded the medical community and Congress of the value of electronic health records, so in 2009 Congress wrote and passed bipartisan legislation called the *HITECH Act* to create financial incentives to get doctors and hospitals around the country to start using electronic health records. I am proud to say that the Hennepin County Medical Center was one of the first hospitals in the Nation to quality for *HITECH Act* funds.

But we need to get all the benefits of electronic health records while still protecting the extraordinarily sensitive information that they contain. I believe all Americans have a fundamental right to know who has their personal information and to control who gets that information and with whom it is shared.

I also think—welcoming the Ranking Member, Senator Coburn. Good afternoon, sir. Doctor.

Senator COBURN. It's still morning back home.

Senator FRANKEN. It is morning in Oklahoma. Let the record show that.

[Laughter.]

Senator FRANKEN. Good morning.

I also think that our fundamental right to privacy includes the right to know that our sensitive information, wherever it is, is safe and secure. Unfortunately, breach after breach of health data has shown us that when it comes to health information our right to privacy is not being fully protected. On the evening of July 28, 2011, a laptop was stolen from the backseat of a consultant's car in the Seven Corners neighborhood in Minneapolis.

That laptop contained the names, dates of birth, Social Security numbers, and medical information for approximately 14,000 patients of Fairview Health Services, and the names and medical information for another 2,800 patients of the North Memorial Medical Center. Those hospitals had told the consultant to encrypt that data. The consultant didn't do that, so it wasn't encrypted.

Sadly, that was the third incident in about a year where the health data of Minnesotans was put at risk as the result of a laptop theft. In fact, since the collection of breach records started in 2009, 91 laptops containing the health information of approximately 1.8 million people have been lost or stolen. That is just a subset of a total of 364 major breaches since 2009 that resulted in the breach of health data of over 18 million Americans. This has been happening since far before 2009.

In 2002, for example, the U.S. Veterans Administration Medical Center in Indianapolis sold or donated 139 computers without removing information on their hard drives that revealed the names

of veterans who had been diagnosed with AIDS or mental illnesses. In 2001, the detailed psychological records of 62 children and teenagers were accidentally posted on the University of Montana Web site for eight days.

The truth is that the same wonderful technology that has revolutionized patient health records has also created very real and very serious privacy challenges. Now, this is not a new problem and we're not the first lawmakers to call it to light. In the past 15 years, Congress has passed major bipartisan legislation to protect health information privacy.

In 1996, Congress passed the *Health Insurance Portability and Accountability Act*, commonly known as HIPAA. HIPAA set out that health care providers and insurers have to protect their health data. It also required that they get their patients' permission before disclosing that information to certain third parties. Yet although HIPAA made strides toward better protecting patients' privacy, it also left some substantial gaps.

So in 2009, Congress passed the bipartisan *HITECH Act* as part of the Recovery Act. The *HITECH Act* extended many of the same privacy and security rules that apply to doctors and hospitals to their contractors. This was called the Business Associate Rule. The *HITECH Act* also required health care providers and health insurers to notify people affected by a breach and increased the civil and criminal penalties for violations of all of these rules.

When Congress passed the *HITECH Act* it sent a clear bipartisan signal that it was time to get serious about health information privacy. Unfortunately, all signs indicate that we're still not there either in terms of the protections we have in place or the way that we've been implementing and enforcing those protections. A lot of the crucial protections of the *HITECH Act* have yet to be implemented.

For example, HHS has yet to issue final enforceable rules on a number of critical protections, like the Business Associate Rule. And while the Department of Health and Human Services and the Department of Justice have increased enforcement in the past one or two years, the overall record of enforcement is simply not satisfactory.

Of the approximately 22,500 complaints that HHS has received since 2003 that it had authority to investigate, HHS has levied a formal fine or civil monetary penalty in one case, just one. They have reached monetary settlement agreements in six other cases.

DOJ's record on this is similarly mixed. Since 2003, HHS has referred about 495 cases to DOJ for prosecution, but since then, DOJ has prosecuted just 16 criminal HIPAA cases. DOJ has reported to me that they have prosecuted some cases under statutes other than HIPAA, like identity theft and computer hacking statutes, but DOJ has no records or estimates of how many of those stem from HIPAA cases. It is hard for Congress to conduct oversight over DOJ without this data.

Now, I want to be clear, there are explanations for these facts and figures and a lot of the responsibility lies on the shoulders of Congress. Congress perhaps should have instituted stronger reporting requirements on DOJ for enforcement, and HHS's low enforcement statistics are in large part the product of what I think is a

wise Department-wide policy to work with companies to fix privacy problems and not just fine them.

But I think it's safe to say that we need to do more to protect this data, and that's what this hearing is all about, figuring out if we are doing enough and doing everything that we should be doing to enforce existing laws, and then figuring out if we need new laws and regulations to fill in the gaps.

Before I turn to my friend, the Ranking Member, I want to recognize that the work we're doing today continues the work that has been done for 15 years here in the Judiciary Committee under Chairman Leahy, and of course in the Health, Education, Labor and Pensions Committee under Chairman Harkin, and their predecessors on both sides of the aisle. I sincerely believe that health information policy and privacy is a bipartisan issue and a bipartisan cause, and one that will require a bipartisan solution.

With that, I will turn to Senator Coburn, who is a watchdog of the Federal Government, and as a physician will have a very valuable voice in today's hearing.

Senator Coburn, good morning.

STATEMENT OF HON. TOM COBURN, A U.S. SENATOR FROM THE STATE OF OKLAHOMA

Senator COBURN. Thank you, Mr. Chairman. Thank you for holding the hearing. I regret I have other obligations so I'm only going to be able to be here for about 45 minutes.

I would make some points. Think about this as a patient's chart in my office. The likelihood with this as a chart, of anybody having access to that other than the people that should have it, it is about zero. Now think about me putting it on a computer and think about the potential for other people having it. When HIPAA was first passed, I was in the Congress and I voted against it, because as a practicing physician the goal was worthy, but the costs associated with it—the Clinton administration admitted that it would cost about $17.6 billion over 10 years. It ended up costing about $9 billion a year back then.

What we're attempting to do is a good thing. What we've attempted in terms of our laws is not going to be cost effective. All you have to do is read the Institute of Medicine report about the increased number of mistakes and the increased errors that are going to come from an electronic medical record.

The other thing we've done with the Affordable Care Act is we've mandated that you're going to have an electronic medical record. So we've mandated all the records that are secure in my office in Muskogee, Oklahoma, are going to go onto a potentially insecure data base. No matter what I do, there's always somebody that's going to get around it and I'm going to spend a lot of dollars as a doctor proving that I've done what the government says I can do, which still may not prevent that data from being there. So I'm anxious to hear.

I know we have a problem with this. What my question is, is whether or not we've gone about it the right way. We're spending a ton of money paying doctors to put records online. They have plenty of money to put records online themselves, but we're going to pay them to do it. They are some of the highest earners in our

country, and yet we've decided we're going to subsidize their computer and their software program for it.

So I look forward to the statements. I have a real concern, both for the privacy issue, but also the goal that we're trying to accomplish may not be accomplishable. There are always going to be people that will go around it. Just ask our Defense Department with China right now, ask our private companies with China right now, the hacking that's going on, the very sophisticated people that are going to try. They've got to get into my office to get it when it's on a piece of paper. They've got to get into my office. So maybe we ought to re-think some of what we're doing, both in terms of privacy, but also cost.

Mr. Chairman, thank you.

Senator FRANKEN. Thank you, Senator Coburn. I'm sorry that you missed the beginning of my statement. I was talking about how HCMC, Hennepin County Medical Center, which is just a few blocks from my home in Minnesota, benefited from the use of electronic health records in the aftermath of the 35W bridge collapse. We will have this discussion. You will hopefully be able to stay for some of the second panel and ask your—I'll certainly yield to you to ask questions before you have to leave before anybody else.

With that, I'd like to now introduce our first panel of witnesses. Loretta Lynch is the U.S. Attorney for the Eastern District of New York. Ms. Lynch is a member of the Health Care Fraud Working Group of the Attorney General's Advisory Committee. In fact, the Health Care Fraud Prevention and Enforcement Action Team in her district has brought major cases involving Medicare and health insurance fraud. Prior to this position she was a partner at a law firm in private practice. Ms. Lynch received her law degree and bachelor's degree at—it's pronounced Harvard.

Leon Rodriguez is the new Director of the Office for Civil Rights at the Department of Health and Human Services. As Director of the office, Mr. Rodriguez oversees enforcement of HIPAA and the *HITECH Act*. Prior to his post at HHS, he was Chief of Staff and Deputy Assistant Attorney General for the Department of Justice Civil Rights Division. Mr. Rodriguez received his law degree at Boston College and his undergraduate degree at Brown University.

Thank you both for being here today. Why don't we start with Ms. Lynch.

STATEMENT OF LORETTA LYNCH, U.S. ATTORNEY FOR THE EASTERN DISTRICT OF NEW YORK, U.S. DEPARTMENT OF JUSTICE, BROOKLYN, NY

Ms. LYNCH. Thank you, and good afternoon, Mr. Chairman, Ranking Member Coburn, and Members of the Subcommittee. Thank you for the opportunity to join our partners at the Department of Health and Human Services in discussing the enforcement of Federal laws protecting patient medical records.

As U.S. Attorney for the Eastern District of New York, and as you've heard, a member of the Health Care Fraud Working Group of the Attorney General's Advisory Committee, I can tell you that patient privacy is of utmost importance to the Department of Justice.

Strong privacy protections help ensure that patients are candid with their health care providers about their medical needs. For patients, the public disclosure of personal medical details can lead to profound humiliation. Breaches of medical privacy can also result in financial losses, in the millions of dollars, to government and private health care plans.

Protecting patient health records is especially critical as our country tries to reduce health care costs by promoting the use of electronic medical records. Through the *Health Insurance Portability and Accountability Act*, or HIPAA, as recently strengthened by the HITECH amendments, Congress has provided three distinct tools to enforce HIPAA's protections: first, HHS is empowered to impose civil monetary penalties; second, State attorneys general can initiate civil proceedings for injunctive relief and financial penalties; and third, the Department of Justice can investigate and prosecute violations of HIPAA's criminal provisions.

In order to carry out the multi-tier enforcement system developed by Congress it is essential that the agencies enforcing HIPAA act together in a coordinated manner. Currently, the FBI routinely coordinates potentially criminal HIPAA violations with the Office for Civil Rights for HHS. HHS has an established process for receiving complaints of potential HIPAA violations from the public and also receives information about potential violations through self-disclosure from health care providers.

HHS forwards to the FBI all HIPAA complaints or disclosures which may involve criminal violations of the statute. If the local U.S. Attorney's Office determines that the particular matter is not appropriate for criminal prosecution, HHS OCR can then determine whether to assess a civil monetary penalty.

The Department also prosecutes a number of cases which may involve breaches of medical privacy but which come to the FBI or the Department through other referral methods such as complaints of identity theft or Medicare fraud. The smaller subset of medical record privacy breaches that warrant DOJ criminal enforcement generally tend to fall into one of three fact patterns.

First, we've prosecuted criminally when medical records and identities were stolen to commit massive health care frauds. These cases caused grave societal harm, both because the patients' historical medical and insurance records are corrupted, and also because there are often massive losses, profoundly draining precious health care payment resources.

Recently, the Department charged 73 defendants, alleged members of an Armenian-American organized crime enterprise, involving more than $163 million in fraudulent Medicare billing in 25 States. The scheme was allegedly accomplished through the theft of the identities of the doctors and thousands of Medicare beneficiaries. That indictment included RICO charges predicated upon identity theft and credit card violations.

Second, we prosecute when medical records are stolen for the purpose of embarrassing particular patients, for example, to sell the records of a celebrity patient to a media outlet or to extort ransom payments to avert the disclosure of customer health records. An administrative assistant at the UCLA Medical Center pleaded

guilty to illegally obtaining celebrity health records after receiving thousands of dollars from a media outlet.

In September 2009, an Indianapolis defendant was sentenced to three years in prison for stealing health insurance records of over 900,000 individuals. The defendant had threatened to publish this personal information and confidential medical data on the Internet unless each victim insurance company paid him $1,000 per week for four years.

Finally, we bring criminal cases where the ultimate motive is to steal patients' identities to commit financial fraud. When the conduct rises to the level meriting a criminal prosecution, we are fortunate to have a variety of criminal statutes to address the various fact patterns that we see in the medical records privacy cases.

In addition to the HIPAA criminal provision, the Department's prosecutors can utilize health care fraud statutes, unlawful computer access statutes, identity theft statutes, and conspiracy statutes, and we are extremely appreciative of Congress' support in providing each of these tools.

Mr. Chairman, thank you for inviting me here to testify today, and I am pleased to answer any questions that you may have.

Senator FRANKEN. Thank you very much, Ms. Lynch. Your complete written testimony will be made part of the record.

[The prepared statement of Ms. Lynch appears as a submission for the record.]

Senator FRANKEN. Mr. Rodriguez, you have about five minutes or so.

STATEMENT OF LEON RODRIGUEZ, DIRECTOR, OFFICE FOR CIVIL RIGHTS, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, WASHINGTON, DC

Mr. RODRIGUEZ. Good afternoon, Chairman Franken, good morning, Ranking Member Coburn, and good afternoon Senators Whitehouse and Blumenthal. Thank you very much for having me before the Committee today. It is an honor to be here and to talk about the important work that the Office for Civil Rights does in enforcing the HIPAA statute and the HITECH statute.

I'd like to focus in my oral remarks on the new authorities that we have under the HITECH statute and the direction that I expect my office will be taking in the years to come.

As the Chairman has observed, the HITECH statute created significant new requirements and authorities in the privacy and security realm. The first of these is the breach notification rule which has been in effect as an interim final rule since 2009. We have received a number of notifications during that time of significant breaches of health information.

One of the things that is notable about many of those breaches—in fact how low-tech they are—in many cases the breaches involve theft or loss of actual hard items, such as laptops or Blackberries, in addition to the expected hacking, improper access to health information. So our experience under the breach notification rule has been an important pathway for us to identify and then develop means to close some of the real vulnerabilities that exist in the area of health information.

Another notable element of our experience with the breach notification rule, and it's also borne out in our larger enforcement program, is the degree to which business associates are the source from which protected health records are compromised. So it is an important part of the HITECH statute that authorized us to, and we are currently working diligently on regulations that will help us initiate our enforcement in this area, given that many of these records in fact come from business associates.

Now the HIPAA requirements will be extended directly to business associates, whereas before only covered entities were subject to those requirements, who were then required to extend those requirements via contract to business associates.

Finally, and most importantly, the HITECH statute has given us much increased penalties for violations of the privacy and security rules. So whereas before the maximum penalties were capped at $25,000 per year, for identical violation, we are now in an environment where those penalties are capped at $1.5 million per year, for identical violation, giving us a very strong enforcement tool with which to police these issues.

In fact, you've seen the very beginnings of that policing. You've seen our case against Massachusetts General Hospital, a teaching institution in Boston, where loss of protected health information exposed a number of other vulnerabilities and deficiencies in the manner in which the hospital maintained its protected health information.

In the case of our enforcement, which is covered in detail in our prepared remarks, against CVS and Rite Aid, you had a situation where hard-copy records were placed in the dumpster. We talk about the vulnerabilities that are out there, and it could not be more prosaic than that. Hard-copy records were placed in the dumpster, potentially exposed to having people see incredibly detailed, incredibly personal health information of their neighbors.

In these cases we've seen fines range from a million to millions of dollars, so pretty significant fines. I am the first Director of the Office for Civil Rights to come to the office with experience, both extensive experience in law enforcement and as a health provider lawyer. It is my commitment to really ramp up the enforcement of the office in the months and years to come and to have us in a place where these examples that I've talked about are just the beginnings of our enforcement in this area.

Additionally, under HITECH, we are in the middle right now of an audit pilot where we will be auditing for compliance with the privacy and security rules as many as 150 entities. This will show us where a number of vulnerabilities may exist and also provide us necessary information as we shape our permanent audit program. Finally, in this area, we have been involved in extensive collaboration with State attorneys general in the area of privacy enforcement.

It's a pleasure to be here today and I look forward to answering your many questions.

Senator FRANKEN. Thank you, Mr. Rodriguez. Again, your remarks will be in the record for whatever I told Ms. Lynch.

[Laughter.]

Mr. RODRIGUEZ. OK.

[The prepared statement of Mr. Rodriguez appears as a submission for the record.]

Senator FRANKEN. I would note, as you said, that there has been a ramp-up in enforcement, but I'm going to probably be focusing some of my questions here on some of the—and asking for explanations of some lack of enforcement.

I want to definitely be able to get through this panel. I hope that the Ranking Member can stay for some of the testimony of the next panel just to hear, because I think that while today we're talking about privacy and some of the problems that we've had in this, I think that both Ms. McGraw and Ms. Myrold will be speaking—especially Ms. Myrold who works at HCMC—to some of the benefits that we've had from electronic health records. For example, that file that the Ranking Member held up that would be in his office on one of his patients who is wonderfully taken care of by him, if it was the middle of the night in Oklahoma—I'm sorry. What town in Oklahoma are you from?

Senator COBURN. It's on a need-to-know basis.

[Laughter.]

Senator FRANKEN. OK.

Senator COBURN. I'm an Okie from Muskogee.

Senator FRANKEN. OK. OK. Oh, you're from Muskogee?

Senator COBURN. Yes.

Senator FRANKEN. OK. Well, I didn't need to know that.

[Laughter.]

Senator FRANKEN. But now I do. OK.

Well, let's say you are asleep in your home in Muskogee and somebody—one of your patients was in Vienna. So there.

[Laughter.]

Senator FRANKEN. Now, the point is if that their electronic health records were available, it might be helpful. That's my only point.

So let's go with the questions. Mr. Rodriguez, since 2003 when the privacy and security rules became enforceable, the Department of Health and Human Services has received over 64,000 complaints from consumers for alleged violations of the rules; about 22,500 of those were against entities that HHS had the authority to investigate.

Of those 22,500, HHS has secured one civil monetary penalty and only six other monetary settlements. I know a large part of this is your Department's policy of trying to get businesses to voluntarily comply with health regulations rather than fining them, and I generally think that's a good thing. I also know that again, in the past year, HHS has increased enforcement by a lot. But these figures seem quite low. How would you explain them?

Mr. RODRIGUEZ. Sure. I think, Senator, first of all, I think you've identified what the—correctly identified what has been the Department's policy until HITECH was passed, which was to give covered entities under investigation the opportunity to implement corrective action, and that would serve as a basis for resolution of those cases.

HITECH has changed the environment significantly in two ways. The first is there no longer is a hard requirement that a covered entity be given that opportunity. We will still do it in many and

most cases, but there is not necessarily a hard requirement that a covered entity be given that opportunity to implement corrective action before we move to penalties.

The other thing that HITECH has done is that it has dramatically increased the penalties, particularly for those entities that have engaged in wilful neglect of their obligations under the privacy and security rules. So, I think that's the reason why that has occurred historically. As I said, I think you have witnessed what are essentially the beginnings of the change in that environment.

Senator FRANKEN. I think one of the problems is that there are a lot of important regulations that HHS has yet to finalize in order to implement the protections of the *HITECH Act*. For example, HHS has yet to issue final enforceable regulations for the Business Associate Rule, and we were talking about business associates here, which requires contractors and consultants that receive health information to protect it, much in the same way that hospitals and insurers already have to.

This is a really big problem because the whole purpose of the HITECH Act was to plug the holes left by HIPAA. But those holes aren't plugged because the regulations have been delayed. When do you anticipate issuing the Business Associate Rule and other remaining rules in final form? It's been two and a half years since the act was passed. Go ahead.

Mr. RODRIGUEZ. I certainly agree, Senator Franken, that the proposed Business Associate Rule really does plug what is a considerable hole in the privacy and security enforcement architecture. What I can tell you, Senator, is that we've received extensive comments on both the business associate proposed rule and a number of other provisions under HITECH, that we have worked diligently to analyze those comments and to prepare regulatory text based on our analysis, and we are working as diligently as we can toward a final rule. I can't give you a timeframe at this time.

Senator FRANKEN. OK. Well, hurry up.

Ms. Lynch, HHS has referred to DOJ 495 cases for potential criminal prosecution since 2003, but the Department has informed my office that DOJ has prosecuted just 16 individuals for criminal HIPAA violations. My understanding based on your testimony is that DOJ prosecutes a large number of medical privacy cases under other criminal statutes for things like identity theft or wire fraud. Can you tell me how many of the 495 cases referred by HHS DOJ has prosecuted under a statute other than HIPAA? Is that something you know?

Ms. LYNCH. Well, actually—and thank you for the question, Senator. I think I would not be able to give you a specific numerical answer on that, in large part because of the different way in which cases are tracked from an HHS referral to the way a case is opened up within the U.S. Attorney's Office.

In particular, once we charge a case, if we were to use another statute—for example, identity theft or a computer intrusion statute—if that were our lead charge it would be recorded in that way. We wouldn't necessarily see the HHS connection. So I do think that unfortunately the numbers that you have are not reflective of the entire picture of what the Department is doing in relating to med-

ical privacy cases in general, because those cases actually are ongoing.

We do still receive referrals again through the process, through the pipeline from HHS, through the FBI, after their review, sending a subset over to us. I would say that in terms of those overall cases we're charging around 10 a year, some up, some down. We're obtaining convictions of around 10 a year, again, some up, some down depending upon the year, and these are often of multiple defendants for cases involving not just HIPAA, but these other statutes as well.

Senator FRANKEN. OK. Thank you. I just want to note that that was a very straightforward answer, and thank you for it. Based on the first part of the answer it seems because of the way you track this, it's impossible for you to really give me a definitive answer. Perhaps we could work together to try to find a way to change the tracking so that we could do our due diligence in terms of oversight in seeing how this is working.

Ms. LYNCH. Absolutely. I think the Department is eager to work with staff of this Committee, to work on ways to improve that and to provide you the information that you need because there are a lot of cases out there.

Senator FRANKEN. Thank you very much.

The Ranking Member.

Senator COBURN. Well, thank you both. Very enlightening testimony.

Let me go through the three main areas for you all: fraud, extortion, and patient identity theft. Correct? Patient identity theft. That was your testimony. That's the main three areas. Which is the largest area?

Ms. LYNCH. At this point, again, without having the specific numbers in front of me, but knowing of the extensive efforts we're doing particularly in Medicare fraud, I would probably say the fraud area is the largest. But again, it's going to encompass a lot of different types of activities.

Senator COBURN. And in cases involving HIPAA medical records, in your office in New York, how many cases have you all prosecuted?

Ms. LYNCH. I'm aware of one—one or two that we currently have going on. We also have a civil matter that's been settled. Again, we focus a lot on the Medicare fraud of it—aspects of it—and we may not in fact include the HIPAA statute all the time because the nature of the case, the facts may lend themselves to a different type of charge.

Senator COBURN. You're going to prosecute where you can get the greatest amount of success and relief, correct?

Ms. LYNCH. Correct. Particularly relief. Correct.

Senator COBURN. We know that the HITECH and HIPAA regulations in terms of using those laws to prosecute Medicare fraud and identity theft. What do we have in terms of the utilization to prosecute the misuse of a Medicare patient's Social Security number or a Medicare provider's billing number?

Ms. LYNCH. Well, I think——

Senator COBURN. Because that's where the fraud is.

Ms. LYNCH. Yes. Absolutely. Well, the health care fraud statute has been a very successful tool for us, working in conjunction with HHS, in prosecuting large numbers of defendants for that. The cases in my testimony that were recently brought down, but also under the A teams which are located in several offices, mine included, we've done a number of those cases where patient data is used, sometimes illegally obtained, sometimes, sadly, obtained from patients who are involved in the fraud. But at this point in time, the health care fraud statute would be one, and then after that, identity theft.

Senator COBURN. Would you think that increasing the penalties in terms of utilizing patients' Medicare and Social Security number or provider number would be beneficial in your all's effective carrying out of the law?

Ms. LYNCH. I think that right now—thank you for that. I think that right now we have a very effective framework of that. We would certainly welcome the opportunity to work with you on adjustments that could be made. If you're thinking in terms of the HIPAA penalties, there's a three-tier system, as I'm sure you're aware, of penalties.

Senator COBURN. I'm thinking of raising the penalties for intentionally selling Medicare provider numbers or Medicare Social Security numbers, patient numbers or provider numbers, because that's where we see a lot of this in terms of the multitude of layers of fraud in terms of false billing to Medicare.

Ms. LYNCH. Right.

Senator COBURN. Mr. Rodriguez, what do you all do right now to educate people that are under your purview to bring them up to speed with your new regulations and compliance? Since you're a little stronger now in terms of trying to get the enforcement, what are you doing to educate?

Mr. RODRIGUEZ. There are a series of activities in which we are engaged, and I very much appreciate the question. To begin with, our Web site contains extensive information, both on the original HIPAA requirements and then the new HITECH requirements, and they're readily accessible to any health provider who wishes to educate themselves on those requirements.

In addition, we have an extensive media campaign where we talk about the requirements, particularly in publications that target the health care industry. We also make our staff available extensively to speak to health industry groups in order to convey the requirements under the statute. This is an area to which I am personally very committed. It is my intention to continue and intensify where necessary these education efforts.

Senator COBURN. OK.

Thank you, Mr. Chairman.

Senator FRANKEN. Thank you.

Senator Whitehouse.

Senator WHITEHOUSE. Thanks, Chairman Franken. I thank the witnesses for attending.

The flip side of the privacy issue with respect to your responsibilities is the opportunity that electronic records provide for investigative purposes. Senator Coburn and I were allies in a long battle to

get the Drug Enforcement Administration to get off its insistence on paper records.

And I can't speak for Senator Coburn, but what frustrated me was that I knew that there was some old DEA agent someplace who could remember making a case and sitting there with the paper records and thinking that that was what had to be protected, when in fact you can do an enormous amount of good, particularly with prescription abuse, which is exploding in this country right now, if you could get information as to what the peculiarities are with the dispensation of, particularly, controlled pharmaceuticals.

So if a doctor goes from zero bottles of Vicodin a week to 500, or if the same Medicare or billing number ends up getting controlled substances at five different doctors, that gives a wonderful opening to law enforcement to be able to focus its resources on areas that are going to be productive.

I'm wondering what your experience has been with the utility of electronic prescription records, Medicare billing records, and other data sources at targeting law enforcement at the real miscreants in this area, and how vulnerable you think the process that de-individualizes that data so that people can look through it without necessarily knowing who the individuals are associated with that data, how effective that de-individualization is, and what its weaknesses are. I'll ask both of you the same question.

Ms. LYNCH. Sure.

Senator WHITEHOUSE. U.S. Attorney Lynch first.

Ms. LYNCH. Thank you, sir. I'm sorry, I didn't mean to jump the gun there.

Senator WHITEHOUSE. No, go ahead.

Ms. LYNCH. Thank you. I appreciate the opportunity to talk about that, because in fact what you have just described is an important part of our current health care fraud prosecution strategy. Through the A team, as I mentioned, we do a lot of work both with the FBI and with HHS Office of Inspector General, particularly in New York, at looking at fraudulent billing cases.

As I mentioned to the Ranking Member, some of these involve the misuse of patient data and some of them involve simply false billing for non-existent services. In recent years, the improvement, I should say, in the real-time tracking of Medicare billing through upgrades to the HHS system has been invaluable to us in letting us see exactly the types of shifts that you are referring to.

In the metropolitan New York City area, for example, we are able to look now and see data that is less than one month old as opposed to having to wait for, as you mentioned, the paper records or even a slower computer record that could be months old. By that time, a clinic that is giving out a lot of false billings could have folded up and moved on by the time we found our way to it. Using the exact kind of data that you mentioned, much more real-time analysis enables us to use other investigative tools.

In a case in my district last summer, we used extensively—we used undercovers. After getting some informant information, we used undercovers to go into a clinic that was billing in Brooklyn, and because of what we saw in there, we were able to marry that with the data showing a spike in billings that we felt were fraudulent and we were able to obtain court-authorized electronic surveil-

lance of that particular clinic and arrest not only doctors but also some patients who, sadly, were participating in the scheme. They were elderly patients being paid to turn over their numbers there. So that's a little bit different from the theft of the information. There, people are basically providing it.

Senator WHITEHOUSE. Let me jump in for the last couple of seconds to ask Mr. Rodriguez to respond also.

Mr. RODRIGUEZ. Sure. First of all, as a former health care fraud prosecutor, and including one who has worked on many drug diversion cases, I full well know the seriousness of the problem that you've identified, Senator. We see in many of the health care privacy cases very often there is also, as U.S. Attorney Lynch has identified, sometimes a component of either a health care fraud or drug diversion that actually initiates those cases rather than them coming in as privacy complaints. In fact, they start on the health care fraud or drug diversion side of the house. So it's a very real problem that you've identified. We collaborate with prosecutors in cases where those sorts of issues have been identified.

Senator WHITEHOUSE. My time has expired. Thank you, Mr. Chairman.

Senator FRANKEN. Thank you for your questions, Senator.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you both for being here.

I want to ask you about the gaps in HIPAA health data protection. I speak as an author of one of the bills that had been reported out of this Committee, S. 1535, the Personal Data Protection and Breach Accountability Act. There are three bills, and that bill is one of them. Of all the data breach bills currently being considered by the Senate, my proposal is the only one that explicitly protects health information. All three bills allow "covered entities" regulated by HIPAA to continue to be governed by that regime, but only the bill that I have authored, S. 1535, explicitly extends its protections to health data held by companies that are not currently covered by HIPAA.

So my question to both of you is, what types of entities hold health data that are not covered by HIPAA, and do you think it's important to ensure that that health data held by third-party companies not covered under the current law also be protected, that they be required, in fact, as the bill would do, to take steps to protect it against theft or other kinds of breaches and the other kinds of protections—for example, remedies, insurance, notification, and so forth—that the laws would provide?

Mr. Rodriguez.

Mr. RODRIGUEZ. Yes. Thank you, Senator Blumenthal, for that question. As you know, the HIPAA statute really covers three types of what we call covered entities: health care providers, health plans, and health care clearinghouses. Health providers are defined as those health providers that transmit certain standard health information transactions electronically. Excluded from that definition can be providers who don't transmit health information transactions electronically, typically, for example, in a private-pay sort of enforcement. So there clearly are health care providers out there who are not currently subject to the HIPAA statute.

Having said that, it is our sense that the HIPAA statute does cover the vast majority of health care business that occurs in the United States.

Senator BLUMENTHAL. What about the other two categories besides the providers?

Mr. RODRIGUEZ. Again, if you fall outside of those three definitions, which include health plans, exactly what the name suggests, or health insurance plans, and health clearinghouses, which are entities that take non-standard health information and convert it to standard information, typically for billing but also potentially for other purposes. There are clearly other sorts of entities outside of those definitions that have health information and are not currently covered by the HIPAA statute.

Senator BLUMENTHAL. Would you recommend to the Senate and the Congress that it extend those protections to entities not covered currently by the HIPAA statute?

Mr. RODRIGUEZ. We certainly would be very willing to work with the Senator and his staff, providing technical assistance on that bill. I'm not permitted to specifically endorse a particular——

Senator BLUMENTHAL. Well, is there a reason that you would recommend against it? In other words, why shouldn't those same protections be extended to those other entities that have possession of this same kind of sensitive and confidential information?

Mr. RODRIGUEZ. No. And I would suggest the way—we would be most pleased to work with the Senator and his staff on that bill, on providing technical assistance in your work on that bill.

Senator BLUMENTHAL. Thank you.

Did you have a comment, U.S. Attorney Lynch?

Ms. LYNCH. No. Just to echo what Mr. Rodriguez said, I think the Department would also look forward to working with the Senator on looking at those issues as well.

Senator BLUMENTHAL. Thank you.

In the short remaining time I have left, I would like to ask whether you are satisfied that there have been sufficient criminal prosecutions under the HIPAA statute. I know that some may have been—some cases may have been recommended for prosecution, but not actually done.

Mr. RODRIGUEZ. Actually, the health privacy environment reminds me very much of the health care fraud environment in which I worked for a significant portion of my professional life. The trend that we saw in the health care fraud environment is a large number of criminal cases and a large number of civil cases where, for example, the *False Claims Act* and other authorities provided really significant monetary penalties to police health care fraud, and very often in many cases those monetary penalties were really the right approach, the right hammer, if you will, to policing health care fraud issues. I think the health privacy environment is very similar.

While there is a certain layer of cases that do merit criminal sanctions, in my view, where the real frontier is, is in our leveraging these new, stiff penalties that we have under the HITECH statute and expanding our utilization of those penalties.

Senator BLUMENTHAL. You're talking about civil penalties?

Mr. RODRIGUEZ. Yes, sir.

Senator BLUMENTHAL. And why not criminal penalties?

Mr. RODRIGUEZ. Because our experience is that many of the cases that we see, in terms of the complaints that we receive, point to not cases of intentional disclosure of protected information for the sorts of criminal reasons that U.S. Attorney Lynch identified, but rather wilful neglect to follow the obligation by a covered entity to follow the obligations that the law imposes.

Senator BLUMENTHAL. My time has expired but I want to thank you both again for your being here and for your very helpful testimony. Thank you.

Senator FRANKEN. All right. Yes. Thank you, Senator.

The Ranking Member has to leave, but we will extend to him the opportunity to ask questions for the record. I also want to thank U.S. Attorney Lynch and Mr. Rodriguez for your testimony, and you are now excused. You can go.

We will proceed to the second panel of this hearing. I would like to introduce our second panel. We have Kari Myrold, who is the privacy officer of Hennepin County Medical Center in Minneapolis, again, about five or six blocks from my home there. It's a great, great hospital.

As privacy officer, Ms. Myrold oversees the implementation and use of electronic health records and ensures HCMC's compliance with State and Federal privacy laws and ensures that patient records are private and secure. Ms. Myrold received her law degree from Hamline University in St. Paul and her undergraduate degree from St. Cloud State University in St. Cloud, Minnesota. Welcome.

Deven McGraw is the director of the Health Privacy Project at the Center for Democracy and Technology. Ms. McGraw was recently appointed by Secretary Sebelius to serve on the Health Information Technology Policy Committee. Prior to this, she was the chief operating officer of the National Partnership for Women and Families. Ms. McGraw received her undergraduate degree at the University of Maryland, her Master of Public Health from Johns Hopkins, and her law degree in LLM at Georgetown University Law Center.

Thank you, Ms. McGraw, thank you, Ms. Myrold, for joining us. Your complete written testimony will be made a part of the record, and you each have five minutes or so for any opening remarks you would like to make.

Ms. Myrold, please go ahead.

STATEMENT OF KARI MYROLD, PRIVACY OFFICER, HENNEPIN COUNTY MEDICAL CENTER, MINNEAPOLIS, MN

Ms. MYROLD. Mr. Chairman and Senators Whitehouse and Blumenthal, thank you for the opportunity to appear on behalf of Hennepin County Medical Center as a provider in this hearing with regard to the electronic health record and privacy rules.

Although Hennepin County is a very fascinating facility, I could tell you lots of things about it, I am here really to speak to one of those things in particular. However, to put it in perspective, I would like to let you know that Hennepin County Medical Center is a 477-bed hospital with six primary clinics and a number of specialty clinics. It also is a teaching facility and is noted as Min-

nesota's premier Level One trauma center, both for adults and pediatrics.

In 2002, Hennepin County Medical Center embarked upon a journey to implement an integrated electronic health record. We had siloed applications. Say you had an application coming out of the neonatal unit, one out of radiology, and maybe one out of the emergency department. Hennepin County Medical Center decided to integrate both the patients' records throughout the facility as well as include the revenue cycle management system.

Hennepin County Medical Center's goals in doing this were to enhance the patient experience, improve the quality of care and patient safety throughout the facility, support research and education, and sustain the organization. Although improvement is ongoing in the electronic health record, there are always updates to be made.

Hennepin County has actually achieved these goals, including adding certain modules such as Care Everywhere, which is our software provider's application for the health information exchange within our metro area, and that actually is done with patient consent that we provide that opportunity for patients and other providers to be able to treat patients throughout different facilities.

We also have added a mychart module, which is really the e-patient chart access where a patient can logon, schedule their own appointments, check their lab results, and view their own record. Then, most recently, we added a Carelink module, which is for our community users, so instead of faxing or delivering an inch of paper to, say, a long-term care facility, what we can do now is we train and provide access for one or two individuals from that facility, that's one example, for a discharge from one of our units. So that long-term care facility access person can then determine whether or not that would be an appropriate placement upon discharge for that person.

Then through performance and improvement of our electronic health record, I would just like to note that Hennepin County Medical Center has actually achieved Stage Six on a 0 to 7 scale through the Health Information Management System Society adoption model, and really that is—we're working toward Stage Seven in 2012, and that's the top. Only one percent of hospitals nationwide actually achieve Stage Seven.

Also, in fulfilling one of our goals that I mentioned earlier, in being able to capture and measure data, Hennepin County Medical Center was an early attester to meaningful use. We have actually received our first payment and that was actually over $1 million. That was in August of 2011. Only 10 percent of hospitals at that point in time had achieved that status.

Hennepin County Medical Center is a public subsidiary hospital; therefore we were subject, long before HIPAA, to the Minnesota Government Data Practices Act. Minnesota was, therefore, a little bit advanced with regard to privacy rules. We also are subject to accreditation standards through the Joint Commission; they have an information chapter, and through that we have to make sure that we provide privacy and security for our patient data. And then along came HIPAA, and then, of course, HITECH.

Chairman Franken has already indicated the critical example we had of testing our first test case with the electronic health record in the tragic collapse of the 35W bridge. Along with using the patient health record, we also tested that for auditing of staff access with regard to privacy violations.

There are a number of areas where I can see improvement necessary throughout the rules, and some of those might be that model policies and procedures could have been included with regard to the rules. There are a number of organizations who apply policies inconsistently, and when you do have a question or investigation with the OCR, one of the first things they're going to be asking you for is your policies.

They have been very cooperative in assisting you in modifying any that you might need, but there's a lot of time and attention given to these in advance and I think models would have helped in that regard. Business associates, data breach notification, expanding the definition of a covered entity, encryption, and then accounting of disclosures are other areas where I certainly can see that we could make improvements.

Thank you.

Senator FRANKEN. Thank you very much, Ms. Myrold.

[The prepared statement of Ms. Myrold appears as a submission for the record.]

Senator FRANKEN. Ms. McGraw.

STATEMENT OF DEVEN McGRAW, DIRECTOR, HEALTH PRIVACY PROJECT, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC

Ms. MCGRAW. Thank you very much for the opportunity to testify. I want to start by saying that people like Ms. Myrold and her colleagues at the Hennepin County Medical Center and others across the country who are adopting electronic medical records and proving that they can actually be a big difference in how health care is delivered in our country, both in terms of cost and quality, they're really the reason why I do this work.

The public, when you survey them, is very supportive of the commitment we're making to health information technology. We are already starting to hear about some promising results, and I think we're going to hear more in the very near future.

At the same time, we know that the public consistently expresses a concern about the privacy and confidentiality of their digital health records, and for good reason. The amount of breaches that we see are one reason why people are concerned, but for about a quarter of the population, based on survey data, these privacy concerns are going to cause us to withhold information from our health care providers because we're not confident that that information will be kept confidential, or we might not be truthful about our circumstances, or we might decide not to seek care at all. That's a problem. Even though it's only for about a quarter of the population we don't want to leave them out of the revolution that we're trying to seed.

Then for the rest of us who may not exercise concerns to that degree, it's still going to jeopardize our trust in the electronic health

record system that we're trying to create and our willingness to support it, quite frankly, with taxpayer dollars.

So clearly Congress recognized that this was an important issue to address and in the stimulus legislation there are a number of really important changes to the HIPAA privacy and security rules, and we supported each and every one of them. But making actual progress in terms of implementation, as has been pointed out, has been agonizingly slow and we wish that were not the case.

So I just want to use the few minutes I have to try to cram in some of what's in my written remarks, but I'm glad to hear the rest of it will get in.

As has already been emphasized, we need the regs. We really need the regs. Give me the regs. You know, Congress—you wanted these provisions to go into effect a year post-enactment, and here we are almost three years later and we don't have most of them.

We know that the administration can act promptly when it's a high priority. We saw the regulations for the Medicare shared savings program finalized within five months of being proposed. I guess I just don't understand why this takes so long. I recognize that it's not just in the hands of the Department of Health and Human Services, so I guess I'll use my bully pulpit to call on the administration to get the review done and get them out.

The improvements in HITECH on enforcement were badly needed, but we don't yet have a consistent, reliable enforcement environment. I'm very glad to hear the testimony of both of the individuals on panel one with respect to a strong commitment to enforcement. We think it's incredibly important.

But we also are very much on board with more transparency with respect to how HIPAA is enforced, both on the DOJ and the HHS side. Summary statistics don't really tell you very much about what's really going on in the field in terms of compliance with HIPAA, and particularly where the Department is likely to continue to try to seek voluntary corrective action on the part of institutions.

And I agree, this is not a bad idea per se, but I personally would like to know more about the circumstances under which voluntary correction is sought. Are there any patterns to it? Is there a need for us to provide more guidance to the field or to enforce in more areas?

HIPAA does not protect all health data. Senator Blumenthal, you pointed this out in your questions. It only covers certain types of health information held by certain entities in the health care system. It covers some things, but not other things.

Health data is rapidly migrating out of the traditional health care system, mostly because it's increasingly being shared by consumers online. Eighty percent of people who are online do searches for health information and there are presumptions made about them based on those searches that often result in them being targeted for ads. But that was the subject of another hearing.

But personal health records offered by internet companies, social networking sites like Facebook and those that are dedicated to specific diseases, none of that data is going to be covered by HIPAA. Congress took care of breach notification for personal health records, but beyond that there are no other protections in law be-

yond what these companies might commit to doing in their privacy policies, if they make any such commitment at all.

If they breach a commitment, then the Federal Trade Commission can hold them responsible. If they don't make a commitment or they make a vague commitment, we don't really have the sort of comprehensive set of rules that we do have on HIPAA-covered entities and we need it.

I guess I'll squeeze in, last, regulations on business associates, downstream contractors. They are important source of health care data. As was pointed out by Mr. Rodriguez, the subcontractors have been a big part of the breach problem. He says we need the HIPAA regs to provide the enforcement on business associates right away. But it also needs to be very clear that a contractor gets data for a specific purpose and should be limited in how they use that data to accomplishing that purpose, and we're not quite there yet.

So I'll stop and be happy to answer your questions. Thank you again for the opportunity.

Senator FRANKEN. Thank you, Ms. McGraw.

[The prepared statement of Ms. McGraw appears as a submission for the record.]

Senator FRANKEN. Thank you, Ms. Myrold, for your testimony. I'm sure that a lot of what you have in your written testimony that you didn't get to, you'll be able to get to via these questions.

Ms. Myrold, the Hennepin County Medical Center has made significant investments in electronic health records. You made that clear. At the same time, it's made a big investment in policies and technologies that will protect patient privacy. Why is—and I think Ms. McGraw spoke to this—patient privacy so important in health care? How does it affect treatment?

Ms. MYROLD. Well, I think, number one, patients need to be comfortable and confident, have confidence in their providers, so that when they're in there seeking treatment they want to make sure that they're able to disclose everything that they need to disclose in order to get the right treatment. Having that confidence means that their information is going to be protected.

Reputations are harmed. Over and above all, a provider is also a business. So if you want to maintain your patient base and attract more patients, you want to make sure that you're not one that's in the headlines breaching patient information. So it's sensitive data and the right thing to do is make sure that you protect that data. There are also mandates, of course, that we have to comply with.

Then at HCMC, one of the things that we have found is that if you're encouraging your own employees to seek care throughout your clinics and your hospital, the first thing you want to make sure is that those employees know that their information is going to be protected from other employees.

Senator FRANKEN. Thank you.

Ms. McGraw, as you mention in your testimony, HIPAA and the *HITECH Act* are not comprehensive. Health information privacy laws don't protect all health information, they just protect certain health information when it is in the hands of certain kinds of companies or providers. Can you give us examples of companies that

have a lot of health information which are not covered under HIPAA or the *HITECH Act*, and what kinds of information they may have?

Ms. MCGRAW. Sure. So just some examples of some entities, and they're largely in the Internet space, the examples that we know of that are getting increasing amounts of health data that would not be covered under HIPAA, either as a covered entity as a business associate, would be a personal health record vendor like Microsoft's Health Vault. Google had a personal health record product but they have since closed that line of business. But there's a consortium of employers called Dossia that also offers a personal health record to their employees, and Dossia is not at all covered.

PHRs collect data from consumers that they get that they either input themselves or that they get from their medical providers, because they have a right to get a copy of their health data, and so the uptake on these is low to date, but it's increasing. It's more than doubled over the past couple of years, and we expect it to increase.

Again, people do searches online for health data. People are increasingly using social networking sites in order to interact with people who have similar conditions that they do and to share concerns about diseases and symptoms, and none of those entities would be covered under HIPAA, yet they are getting increasing amounts of health data, very sensitive health data in some circumstances.

Senator FRANKEN. If these entities aren't covered by HIPAA or the *HITECH Act*, I'd like for you to tell us what kind of protection information held by these entities have under Federal law. Could these companies sell this information to third parties?

Ms. MCGRAW. Sure. So one thing that HITECH did do for at least the personal health record vendors was to say if you as a PHR vendor breach data, then you have to notify the individual and the Federal Trade Commission of the breach. But that was the extent of the protections that are applied to this particular part of the ecosystem. So, just the PHR vendors and just breach notification.

So as a result, what you have is the Federal Trade Commission's traditional authority to crack down on unfair and deceptive trade practices. So in your privacy policy as a company, if you say I will not sell your data and then you sell it, then the FTC has the authority to come after you for violating the terms of your privacy policy. But if you make no commitments with respect to the sale of data or you say outright, I'm going to sell your data, there certainly isn't a law that prohibits you from doing that.

Senator FRANKEN. Thank you. That makes sense.

Ms. Myrold, the last part. In the past, Ms. McGraw and others have called for health care providers, insurers, and other entities covered by HIPAA and the *HITECH Act* to place tighter restrictions on the health information they share with their business associates. My understanding is that Hennepin County Medical Center has actually been a model in this regard and that you place very high restrictions on what your business associates can or cannot do with the health information they receive. Can you describe that policy?

Ms. MYROLD. Certainly. HCMC does have a very tight process. We actually require all of our vendors to define for us which PHI—Protection Health Information—that they are in need of, how they are going to be using that Protected Health Information. Basically relying on what HIPAA has as the minimum necessary rule, we're only going to allow them access to what it is they need in order to perform the services for us that they're going to be performing.

If a privacy—or if a vendor is actually going to be accessing, like I mentioned the long-term care facility earlier, we actually provide them privacy training as well. It's required prior to their actually accessing our electronic health record. Then of course we also ask for them to comply with any security requirements. We used to ask for them to pay for a third-party vendor to get a current security assessment.

Now that was actually quite difficult for some of the vendors, and so what we're asking for now is that even if they've performed some kind of an internal security assessment, we want something that's been done within that past year. So if we're accessing through VPN tunnels, or however we're going to be sharing data through portals, however, we're going to be sending them information, we want to make sure that that's secure and they have that set up within their own technology.

Senator FRANKEN. Ms. McGraw, would you like to explain how business associate agreements could be crafted more narrowly and whether you think this is a change that should be pursued through statute or regulation?

Ms. MCGRAW. Sure. So the way that business associate agreement could be crafted more narrowly would be to emphasize that the agreements have to specify the permitted uses of the data and not—to me the regs err on the opposite side of that question, which is to say the agreement must say what cannot be done with the data, which means if it's not prohibited and as long as it's within the confines of what's permissible under HIPAA, then it can be done.

That's why we've heard some anecdotal reports of business associates who essentially have provisions in their contracts that say we can use this data to meet our business purposes. So since the agreement doesn't prohibit them from using data in certain ways, they could do so based on the contract that they have.

I think we would much prefer to have a provision that requires some defining of the permissible uses versus, stating that you can do it unless it's prohibited. This is absolutely accomplishable by regulation, but I think it's always helpful when Congress sends a signal to the regulators about what it would like to see. It can be accomplished from a legal standpoint through a reg, but we certainly would not—we would be willing to work with you on legislation that would provide a more clear signal to the Department about what Congress wants to see.

Senator FRANKEN. Thank you.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman.

Ms. Myrold, we suffer from the price of new technologies pretty often. The casualties in automobiles are a significant issue, but the value to the U.S. of the automobile is pretty widely respected by

everybody. With respect to health information technology, a lot of Americans are seeing the privacy cost of things going wrong and of private health information escaping, but often don't have the same access to the value of health information technology that one does from the experience of driving a car.

I've been involved with provider groups in Rhode Island, like the Aquidneck Medical Associates and with community health centers like Thundermist, and nursing homes, and a whole variety of health care providers who have had a common experience, which is that it is a real pain in the neck to get onto electronic health records, but once they are, they can't possibly imagine going back to the bad old days of paper files.

I'm just wondering for the record of this hearing what your experience has been, on balance, with the Hennepin County Medical Center's transition to electronic health records and more advanced health information technology. On a net basis, how good a thing has it been? Would you consider going back?

Ms. MYROLD. I don't think they'd ever consider going back. I think that's basically because patient safety is number one. If you have access to all the medications that a patient is on in one chart, or if you have a number of providers that can be accessing that chart, say consulting from one department to another and they're looking at the same chart, that's going to provide you much better patient care.

It was a very high cost to implement this, and like I said, it's a public hospital, and so it's not as if there was a lot of extra dollars there. But they chose knowing, and after going through quite a significant selection process and design process, that this was going to definitely aid in their critical care of their patients.

Senator WHITEHOUSE. Thank you.

Ms. McGraw, you came here to lobby us, but I'm going to lobby you back.

Ms. MCGRAW. Oh. Oh, good.

Senator WHITEHOUSE. The Center for Democracy and Technology is an important voice in these issues, and I feel very strongly that we stand to gain immense advantage from a much more robust health information infrastructure. In the earlier panel, we talked a little bit about the law enforcement investigative advantage, which would not exist if it were not for that. Ms. Myrold just talked about a patient safety advantage. I think that the day will come fairly soon when a robust-enough health information infrastructure will support personalized medicine apps.

So in the same way you've got an iPhone now and you can download an app to it, there will be competition with apps that will help individual patients through their course of treatment, particularly where they have chronic conditions, and will help doctors make sure that things aren't forgotten, a little bit the way a pilot does a checklist before take-off.

Too much of what goes wrong in health care goes wrong because those simple, preventable things don't get done. I think that the time will come very soon when there is enough information out there that we will learn an enormous amount, or perhaps even create new industries, out of looking at all that health information and being able to figure out what's a strange anomaly, why is that

happening, why is this good thing associated with these conditions or this bad thing associated with those conditions, and we'll learn from that.

If we're going to do that we have to have good access to that health information data. It has to be de-individualized. Nobody needs to know that it's Deven McGraw's data, they simply need to know that a person with these characteristics has this circumstances.

Ms. MCGRAW. Yes.

Senator WHITEHOUSE. So I hope that the Center for Democracy and Technology will be an energetic advocate for the propagation of a robust health information infrastructure, knowing that there are these critical fault lines where patients have to be protected not only in their individual data, but also when it's being looked at in the aggregate. Are you comfortable that the way that—we're adequately poised to be able to review that aggregated data in a de-individualized way so that privacy is not impinged by that process?

Ms. MCGRAW. Right. Well, we—thank you very much for that question, Senator. We at CDT have enjoyed a very good working relationship with you and your staff over many years. The reason why we do this work is because we believe so completely in the power of technology to be transformative in this regard, and the idea of privacy is to enable that transformation, to make sure that consumers trust it enough to be comfortable with their data being part of it, whether it's an identifiable form, which it needs to be in some circumstances, but much more often it doesn't need to be identifiable.

It can be de-individualized, which I actually like that term very much because it's different from de-identification, which is a HIPAA term of art. We have done work in the past, and we're continuing to do work, on issues of how you can make sure that data is not uniquely identified to an individual but can still—but you can still robustly use it to do comparative effectiveness research, to examine trends, even for business analytics.

I mean, data drives good decision making, and it should be doing that in health care, too. So we're convinced. Whatever more we need to do, we'd be happy to work with you on that. But that is our central philosophy, that the technology is good. The use of the Internet by people to improve their health is good. We need to makes sure it's a trustworthy environment so that everybody is comfortable in that space.

Senator WHITEHOUSE. Good. Well, I appreciate that. I'm at the age where I can remember before word processing, I can remember when the Selectric typewriter was a big deal. Certainly I can remember pre-Google. My kids, you know, look at my description of the pre-Google environment and just say, "Dad, you're so weird." They kind of don't get that there was ever a point when we could have been so primitive that you couldn't just Google something and, poof, there it was in front of you.

I think that the same thing is going to happen in health care, that we're in the pre-Google moment with respect to personalized health care, supported by individual applications that are supported by a robust health information infrastructure. The time will

come, I think before my kids have kids, so that they don't have to, on this particular subject, be told by their kids, Mom, Dad, you're so weird. But thank you for helping that day come sooner.

Senator FRANKEN. I was the first writer on "Saturday Night Live" to get a word processor. Thank you, Senator Whitehouse.

[Laughter.]

Senator FRANKEN. Senator Blumenthal.

Senator BLUMENTHAL. Senator Whitehouse and Senator Franken are so much older than I; I have no idea about those days.

[Laughter.]

Senator BLUMENTHAL. Not.

[Laughter.]

Senator BLUMENTHAL. But my kids still think I'm weird.

Senator WHITEHOUSE. He did a lot of arguing in front of the U.S. Supreme Court. When he started, the quill that they give you was for real.

[Laughter.]

Senator BLUMENTHAL. It's close to the truth.

I am struck, Ms. McGraw, by one of the observations in your testimony. And let me just say, both of your written testimonies are absolutely superb. I know that you haven't covered all of it in your conversation with us, but I am very grateful for it and will follow up on a number of the points.

But one of the points that struck me is your observation that "the health care industry appears to be rarely encrypting data." You then observed, "To the best of our knowledge, no one has done a comprehensive study of the reasons why the health care industry has not embraced the use of encryption." What possible justification can there be? Doesn't that fact itself cry out for the kind of data breach protection with strong remedies and enforcement and penalties if they fail to encrypt data?

Ms. MCGRAW. So we clearly think it does. We thought that providing an exception in the breach notification provision that was enacted on both HIPAA-covered entities and for the personal health record vendors, provided an exception for entities that adopt encryption, would be a very strong incentive for them to adopt encryption.

What we see from the breaches that have been reported for HIPAA-covered entities since 2009 is that, as was mentioned earlier, a good two-thirds of them are due to theft or loss of media that is an attractive target for theft or is easily lost, like the thumb drive that Senator Franken held up in his opening statement, or laptops. Geez, how many stolen laptops have we had? You had the number in your opening remarks. There are a number of them. Or hard drives that either can be easily walked out the door if nobody's looking or are inadvertently left in computers that are being sold or given away.

So that's why I say it looks like encryption is rarely happening. The best reasons that I've been given, just through anecdotal remark, are it slows down access to data sometimes and it's expensive, and it can be expensive if you're talking about encrypting an entire server because that's a lot of data.

But it's not that expensive to encrypt a thumb drive, and it's not that expensive at all to require people to sign onto a secure server

to get access to the data so they don't have to have it on portable media to begin with. So we have really tried very hard to provide incentives to encrypt and not to have a hard-core requirement to encrypt on the health care industry in order to make concessions in areas where it might be too expensive for some health care providers or it might slow down access to data where instantaneous access is pretty critical.

Yet, even on portable media where you don't have the timing issues and you don't have the cost issues, it's not happening. We would like to see more done in this regard, whether it's in the form of some more specific requirements or whether more guidance about when the Office of Civil Rights expects entities to encrypt. I think that would also be helpful.

Senator BLUMENTHAL. And I gather from both your written testimony and from your responses to my questions and Senator Franken's that you would certainly not object, you might even recommend, to many of the entities not now covered under HIPAA also be included in these protections, both as to encryption and any other requirements for systematic safeguarding of this information.

Ms. MCGRAW. Absolutely. We wholly supported the provision in your bill on breach notification that it include health data. We thought that was an important advance. We have similarly supported consumer privacy bills that are pending, largely in the House, quite frankly, to do—provide, you know, a more comprehensive set of privacy protections for consumer data that of course would include health data, but also include financial data and other personal information that people routinely share. So we are absolutely supportive of that. This environment, the wild, wild west for data is not an environment of trust.

Senator BLUMENTHAL. And not one conducive to the spread and reliance on IT.

Ms. MCGRAW. That's correct.

Senator BLUMENTHAL. Let me turn to another area that I think is important and certainly is worth a lot more than the two minutes I have remaining, but again I will follow up with you. You know, as a former enforcer, I was the attorney general of the State of Connecticut—in fact, I think the first attorney general to enforce the HIPAA protections under HITECH and a former U.S. Attorney—I happen to believe that these laws are useful only to the extent they are rigorously enforced and that they have effective penalties.

So in terms of enforcement, maybe I could ask for both of you to make some observations about whether or not laws so far have been effectively enforced as widely and rigorously as they should be, and whether you think additional penalties should be included.

Ms. MYROLD. Well, Senator Blumenthal, I think that listening to the previous two speakers I began to wonder, what's wrong with the current enforcement provisions and why aren't we enforcing anything under the privacy rules? Are the facts not fitting within the context of the statute, or what's actually—is it not a big enough case? What's really going on there? Why aren't people encrypting? Why aren't business associates complying?

I think a big reason is the final rules aren't here. We don't have final rules in, what, three areas? I think people just—they've lost

credibility. People aren't taking it seriously. Until we actually get those final rules and people, knowing that they're going to actually be enforced, you're probably not going to see a lot more compliance. It's a big issue.

Senator BLUMENTHAL. Ms. McGraw.

Ms. MCGRAW. I would completely—what she said.

Senator Blumenthal. So quote you.

Ms. MCGRAW. Ditto.

Senator BLUMENTHAL. We need the rules.

Ms. MCGRAW. Yes, we need the rules. We need the rules.

Senator BLUMENTHAL. That was part of your opening statement.

Ms. MCGRAW. Yes. And I would echo something else that she said when she talked about model policies. Like, more guidance is always helpful to the field. I think we're always going to have the law a little bit behind where the technology is going, but we can refresh by, you know, periodically putting out to the field what we expect of them rather than waiting for them to do something that looks more like a violation.

Senator BLUMENTHAL. Thank you.

Senator FRANKEN. Thank you, Senator.

And I want to thank you both for your testimony and for your work. I'm very proud of representing you, Ms. Myrold. And thank you for your work, Ms. McGraw.

In closing, I want to thank the Ranking Member, Senator Coburn, and I want to again thank all the witnesses that appeared with us today.

I think there are few kinds of information more sensitive than health information, and technology has given us this wonderful opportunity to harness that information in a way that will make health care easier and more effective. I just want to make sure that we're getting all of those benefits. I think that what Ms. McGraw is saying and what you are acting on at HCMC is that when patients can be assured that there's privacy, that's when this electronic health information can be put to its fullest benefit. I think the benefits are clearly manifest.

Like I said at the start of this hearing, I do believe we can do more to protect our information, both in terms of the laws we have on the books, and we need regs. I think you said "we need the regs, we need the regs, we need the regs." We're the Senate. You could have just said it once. We would have heard you.

[Laughter.]

Senator FRANKEN. But anyway, there is work to be done here. We will hold the record open for one week for submission of questions for the witnesses and for other materials.

This hearing is adjourned.

[Whereupon, at 4:03 p.m. the hearing was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

Additional Material Submitted for the Record

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"Your Health and Your Privacy: Protecting Health Information in a Digital World"

Wednesday, November 9, 2011
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

Loretta Lynch
U.S. Attorney for the Eastern District of New York
U.S. Department of Justice
Brooklyn, NY

Leon Rodriguez
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Washington, DC

Panel II

Deven McGraw
Director, Health Privacy Project
Center for Democracy and Technology
Washington, DC

Kari Myrold
Privacy Officer
Hennepin County Medical Center
Minneapolis, MN

PREPARED STATEMENTS OF WITNESSES

Department of Justice

STATEMENT OF

LORETTA E. LYNCH
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

REGARDING

EXAMINATION OF THE ENFORCEMENT OF FEDERAL HEALTH INFORMATION PRIVACY LAWS

PRESENTED

NOVEMBER 9, 2011

Statement of
Loretta E. Lynch
United States Attorney
Eastern District of New York

Before the
Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

Regarding Enforcement of Federal Health Privacy Information Laws
November 9, 2011

Chairman Franken, Ranking Member Coburn, members of the Subcommittee - Thank you for the opportunity to join our partners at the Department of Health and Human Services in discussing the Administration's efforts to enforce Federal laws protecting patient medical records. We consider patient privacy to be of utmost importance for many reasons. Strong privacy protections help ensure that patients are candid with their doctors and other health care providers so that they receive the care they need. Privacy breaches chip away at the confidential patient-physician relationship, erode patient candor, and thus interfere with medical professionals as they gather the information they need to deliver accurate, quality, and thorough medical care.

Unauthorized access to medical records can have many other profound repercussions for patients, as well as for public and private health plans, medical providers, financial institutions, and other businesses. For patients, the public disclosure of intimate details of personal medical conditions or treatments can be devastating, with consequences ranging from profound embarrassment and humiliation to the loss of employment. Moreover, when stolen patient identities are used in a scheme to bill for

medical services that are never provided, future health care and health benefits may be affected. False treatment information memorialized in a patient's records can fatally distort the diagnosis of a future medical affliction. Future critical medical services may be denied by a health plan on the basis of an earlier-billed phantom surgery or durable medical equipment.

In addition, a patient can be negatively affected by the destruction of a hard-earned credit rating, destroyed as a consequence of fraudulently opened credit card accounts or bogus loans. And finally, record breaches can result in significant financial losses to government and private health care plans, financial institutions, and other businesses, oftentimes in the millions of dollars. Protecting patients' health records is especially critical as our country rapidly moves to improve our capacity to provide quality health care for all and to reduce costs, in part through the use of electronic medical records.

Coordination between the Departments of Justice and Health and Human Services

To successfully deter and punish breaches of medical record privacy, interagency cooperation between the Departments of Justice and Health and Human Services is critical. Congress has provided a wide range of administrative, civil and criminal tools with which medical records breaches can be addressed. For example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as recently strengthened by the commonly named "HITECH amendments" included in the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), provides three distinct tools to enforce HIPAA's protections:

- First, the Secretary of the Health and Human Services, with DOJ concurrence, is empowered to impose civil monetary penalties ("CMPs"), which can amount to $50,000 or more per violation and up to a total of $1,500,000 in a single calendar year, for repeated violations of a provision of the medical privacy and security rules;
- Second, under a new authority added by the 2009 HITECH amendments, State attorneys general can initiate civil proceedings for injunctive relief. Damages on behalf of a State's citizens for violation of HIPAA medical privacy provisions can be up to $25,000 in a calendar year; and
- Third, the Department of Justice can investigate and prosecute HIPAA violations under the HIPAA criminal statute found at 42 U.S.C. § 1320d-6. The most egregious violations of HIPAA are subject to a period of incarceration up to 10 years, and a statutory fine up to $250,000.

Because HIPAA provides these multiple enforcement options to penalize privacy breaches, coordination among the enforcers is necessary. Pursuant to an informal agreement between the Departments of Justice and Health and Human Services, the Federal Bureau of Investigation ("FBI") routinely coordinates with the Office for Civil Rights of the Department of Health and Human Services ("HHS-OCR") regarding complaints filed with HHS-OCR that may represent a HIPAA criminal violation. While the FBI has jurisdiction for the investigation of criminal violations of the medical privacy law, HHS-OCR has responsibility for medical privacy and security violations that are civil in nature. HHS-OCR has an established process for receiving complaints of potential HIPAA violations from the public and also receives information about potential

violations through self-disclosure from health care providers and other covered entities. By agreement with the Department of Justice, HHS-OCR forwards to the FBI all HIPAA complaints or disclosures involving potential criminal violations. HHS-OCR then refrains from taking any action until the FBI reviews the referral, conducts any necessary investigation, and obtains an assessment from the local United States Attorney's Office. If the U.S. Attorney's Office declines a matter, it is returned to HHS-OCR for investigation and potential assessment of a CMP. Similarly, if the FBI or U.S. Attorney's Office concludes that a matter reported directly to the Department of Justice does not warrant criminal prosecution, it can be referred over to HHS-OCR for potential action.[1]

Before the Recovery Act enhanced HIPAA's enforcement tools, the Secretary was obligated to refer virtually every HIPAA complaint it received involving a potential criminal violation of HIPAA to the Department of Justice for evaluation for criminal prosecution. This dynamic was the consequence of a pre-Recovery Act provision of the HIPAA statute which prohibited the Secretary from imposing a civil money penalty (CMP) if "the act constitutes an offense punishable under [the HIPAA criminal statute]." Given the nearly identical offense language predicate for assessing a CMP and for charging a HIPAA misdemeanor offense, a large universe of potential HIPAA offenses, which had not been committed under fraudulent pretenses, to inflict harm or for personal or commercial gain, were referred even though they were susceptible to more efficient

[1] On occasion, we receive direct referrals from sources other than HHS-OCR. For example, we have received referrals from local law enforcement agencies who find abandoned medical records in office building dumpsters. Medical providers and health insurance plans that discover that their computers have been hacked and records stolen have also reached out to Federal law enforcement. We have also received referrals directly from health care providers who were subject to a corporate integrity agreement entered with the HHS Office of Inspector General as a consequence of an unrelated health care fraud.

resolution under the civil monetary penalty statute. In an abundance of caution, a much larger number of referrals were sent to the Department of Justice than would have otherwise been made. This decline in criminal referrals has continued in recent years – there were 13 referrals in fiscal year 2010 and 16 referrals in fiscal year 2011.

Common Schemes to Steal Medical Records

The subset of medical record privacy breaches that warrant criminal enforcement generally tend to fall into one of three fact patterns. First, we have prosecuted criminally when medical records and identities were stolen to commit massive health care frauds. We have found that these cases cause grave societal harm, both because the patients' historic medical and insurance records are corrupted and because there are often massive losses, profoundly draining precious health care payment resources. Recently, indictments were unsealed in the Southern District of New York and four other Districts charging seventy-three defendants, including a number of alleged members and associates of an Armenian-American organized crime enterprise, with various health care fraud-related crimes involving more than $163 million in fraudulent billing. The health care fraud scheme was allegedly accomplished through the theft of the identities of doctors and thousands of Medicare beneficiaries through the operation of at least 118 different phony clinics in 25 States for the purposes of submitting Medicare reimbursements. Racketeering charges were included, predicated in part on identity theft and access device fraud.

Second, we have prosecuted when medical records were stolen for the purpose of embarrassing or threatening to embarrass a particular patient or health care entity – for example, to attack the credibility of the patient publicly, to sell the records of a celebrity

patient to a media outlet, or to extort ransom payments to avert the disclosure of customers' health records. For example, this past June in the District of Arizona, a defendant was sentenced after pleading guilty to violating the HIPAA privacy statute by accessing sensitive medical and psychiatric records of several State employees who were involved in a State administrative hearing to which she was a party. The defendant then disclosed this information by including it in a letter that she sent to the Governor to complain about a State agency's use of employees with psychiatric records.

Similarly, in December 2008, an administrative assistant at the UCLA Medical Center in Los Angeles pleaded guilty in the Central District of California to illegally obtaining protected health records after she received at least $4,600 from a media outlet in exchange for providing the private medical information of a celebrity patient at the facility. And in September 2009, an Indianapolis defendant was sentenced to three years in prison for stealing insurance records of over 900,000 individuals. The records included personally identifiable information, confidential medical information, and confidential email communications. The defendant had threatened to publish this personal information and confidential medical data on the Internet, unless each victim insurance company paid him $1,000 per week for four years.

Finally, we bring criminal medical record theft cases where the ultimate motive was financial fraud against financial institutions or other businesses. Two recent cases from the District of Maryland illustrate this type of theft and fraud. In 2010, five defendants were indicted in Maryland for a fraudulent credit card scheme using information stolen from Johns Hopkins Hospital patient records. The indictment charged that more than 50 businesses and individuals were victimized. Earlier this year, a Federal

grand jury in Baltimore indicted four defendants, including a former employee of the University of Maryland Medical Center, in connection with a scheme in which the identifying information of medical center patients and others was stolen and used to defraud financial institutions. As another example, in the Southern District of Florida in 2009, we convicted two defendants of offenses related to the theft of patient records from Palmetto General Hospital designed to further a credit card fraud scheme.

We see other criminal activity involving the theft of medical records as well, although less frequently. For example, the theft of a laptop or other computer equipment, where the motive may have been to just steal computer equipment, can include the unknowing theft of electronic medical information data on tens of thousands of patients. We have also prosecuted medical identity theft where the primary purpose of the scheme was to prepare and submit multiple fraudulent tax returns.

Various Statutes Used to Prosecute

Because the fact patterns involved in medical records privacy cases are so varied, the criminal statutes used to prosecute medical records privacy cases are also varied. In fact, cases charging just a violation of the HIPAA criminal statute, 42 U.S.C. § 1320d-6, are a small portion of our cases involving breaches of medical privacy. We often bring such cases under identity theft and unlawful computer access statutes rather than the HIPAA statute. When appropriate, we also bring an aggravated identity theft charge that carries a mandatory two year sentencing enhancement. Some prosecutions focus on the payment for the disclosed medical records and charges are brought under the Medicare anti-kickback statute. We also may charge defendants under the general conspiracy statute through which we may be able to reach a wider range of defendants. And we have

charged violations of the general health care fraud statute as well in medical records privacy cases. Differing fact patterns among cases will guide a prosecutor's choice of charging statutes.[2]

This wide range of fact patterns and statutes used to charge those who breach the privacy of medical patients makes the task of accurately capturing all of the cases prosecuted by the Department in this area a difficult one. The Department's case tracking systems are organized by principal charging statute; as such, they do not allow us to track precisely all medical privacy breach cases prosecuted where a statute other than the HIPAA statute was the primary one contemplated or charged. Nevertheless, we can report that the FBI currently has 56 pending investigations associated specifically with violations of the HIPAA statute. In addition, during fiscal year 2011, Federal prosecutors working with the FBI brought cases charging 16 individuals and obtained 16 convictions in cases under HIPAA as reflected in the FBI's case tracking system. The FBI also obtained one additional medical privacy breach conviction in a case it worked with local prosecutors. Again, these numbers do not include any additional cases in which a medical record privacy breach occurred but the HIPAA statute was not the primary one charged. In addition, as noted above, these numbers reflect only those cases where criminal prosecution, as opposed to a civil or administrative remedy, was deemed the most appropriate enforcement option.

---

[2] One additional factor may have previously influenced some prosecutors to bring medical privacy cases under non-HIPAA statutes. In 2005, the Department's Office of Legal Counsel ("OLC") issued an opinion concluding that in most situations only "covered entities" (medical providers, health plans and health care clearing houses) could be prosecuted directly under HIPAA. Others, such as the employees of covered entities, could not be prosecuted directly under the statute according to OLC. The HITECH amendments in 2009 subsequently removed this impediment to prosecution by amending the HIPAA statute to reach employees of covered entities, as well as other individuals.

Conclusion

Our track record in prosecuting health care privacy cases demonstrates the seriousness with which we take the unlawful breach of medical privacy and our commitment to investigate and prosecute these cases criminally when the facts warrant criminal sanction. The Department of Justice looks forward to continuing to work in this important area with Congress and with our partners at the Department of Health and Human Services.

Thank you for affording me the opportunity to testify today. I would be pleased to answer any questions you might have.

Testimony
Before the Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
United States Senate

Statement of

Leon Rodriguez

Director
Office for Civil Rights
U.S. Department of Health and Human Services

For Release on Delivery
Expected at 2:30 p.m.
Wednesday, November 9, 2011

Introduction

Mr. Chairman and members of the Subcommittee, it is an honor for me to be here today in my capacity as the Director of the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS). The privacy and security of personal health information is essential to and at the core of the work of HHS to improve access to and the quality of the health care provided to individuals. OCR administers and enforces the health information Privacy, Security, and Breach Notification Rules, issued under the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA, and the Health Information Technology for Economic and Clinical Health (HITECH) Act. In doing so, we play an important role in ensuring that individuals' sensitive health information remains private and secure, and that individuals have important rights with respect to their health information. I thank you for the opportunity to testify today on the role of the HIPAA Privacy, Security, and Breach Notification Rules in the protection of individuals' health information maintained in electronic health records and elsewhere.

HIPAA established a national, uniform baseline of privacy and security protections for individuals' health information, and the HITECH Act, part of the American Recovery and Reinvestment Act, strengthened and expanded these protections. The HITECH Act's unprecedented investment in health IT has greatly accelerated the adoption of electronic health records (EHRs) among providers and supported efforts to rapidly build capacity for exchanging health information. At the same time, the HITECH Act acknowledged that, to achieve the full potential of health IT to transform care, patients and providers must trust in the confidentiality of sensitive health information. To further that goal, the HITECH Act builds upon the framework of privacy and security protections established by HIPAA. I will provide a brief overview of the HIPAA Privacy and Security Rules, the HITECH Act modifications to HIPAA, and OCR's enforcement of these protections.

Background

HIPAA was designed to improve the efficiency and effectiveness of the health care system by promoting the electronic exchange of health information. At the same time, Congress

recognized that advances in electronic technology, if not properly regulated, could erode the privacy and security of that health information. To address this, Congress incorporated provisions into HIPAA requiring the adoption of Federal privacy and security protections by certain health care providers, health plans, and health care clearinghouses. The HIPAA Privacy Rule requires these entities, known as covered entities, to have safeguards in place to ensure the privacy of individuals' identifiable health information. The rule also sets forth the circumstances under which covered entities may use or disclose an individual's information, and gives individuals rights with respect to their information, including rights to examine and obtain a copy of their health records and to request corrections. The HIPAA Security Rule requires covered entities to implement administrative, physical, and technical safeguards to protect health information in electronic form. The Rules also require HIPAA covered entities to contractually bind their business associates -- contractors or other persons hired to perform services for covered entities that involve individuals' health information -- to safeguard and only use or disclose the information as permitted by the Privacy Rule.

The HITECH Act not only promotes the adoption of health information technology and electronic health records but also works to build confidence in the privacy and security of the information in these records by strengthening and expanding HIPAA's privacy and security protections in a number of areas, such as by:

- Extending key responsibilities HIPAA placed on covered entities directly to their business associates, such as safeguarding and not misusing individuals' health information;
- Adding new requirements for notification of breaches of health information;
- Significantly strengthening HIPAA enforcement by increasing the civil money penalties for HIPAA violations and strengthening the Secretary's ability to act on HIPAA violations, particularly where there has been willful neglect;
- Strengthening individuals' rights to get an electronic copy of their health information;
- Generally prohibiting the sale of health information; and
- Further limiting the use and disclosure of personal health information for marketing and fundraising purposes.

The Department has issued a number of rules to implement these enhancements and is working hard to finalize those that remain in proposed form.

OCR enforces the HIPAA Privacy and Security Rules by investigating complaints from the public about potential violations of the Rules, as well as breach reports that covered entities are required by the HITECH Act to submit to the Secretary. OCR also may initiate an investigation in the form of a compliance review when privacy and security incidents are brought to our attention by the media, government agencies, or other sources. For the most part, the investigations are conducted by investigators in our 10 regional offices across the country. In addition to its investigations, OCR provides technical assistance to covered entities to foster compliance with the HIPAA Rules, and education and outreach to make the public aware of their rights under HIPAA. OCR is committed to expanding and improving its technical assistance and public education materials and finding new and innovative ways to communicate with all who have an interest in keeping health information private and secure.

OCR also coordinates HIPAA enforcement with the Department of Justice, which shares enforcement jurisdiction over HIPAA violations. HIPAA gives the Secretary of HHS the authority to impose civil money penalties for HIPAA violations, and the Department of Justice authority to enforce criminal violations. If a complaint implicates the criminal provision of HIPAA, OCR will refer the complaint to the Department of Justice. From April 2003, the date covered entities were required to be in compliance with the HIPAA Privacy Rule, to the end of September of this year, OCR referred 495 cases of potential criminal violations to the Department of Justice. Further, in cases in which the Secretary wishes to impose a civil money penalty, the Secretary is required to obtain prior authorization from the Attorney General of the United States.

OCR recently issued two annual reports to Congress, required by the HITECH Act, that describe in detail OCR's history of enforcement of the HIPAA Rules, as well as specific enforcement information for 2009 and 2010, and the number and nature of breaches that have been reported to the Secretary in 2009 and 2010 under the Breach Notification Rule. We also make available to

the public up-to-date enforcement data and information on our web site. I will now describe some of the highlights contained in the reports and on our web site.

Enforcement of the HIPAA Privacy and Security Rules

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, and compliance with the Security Rule was required by April 20, 2005. The Secretary delegated the authority to administer and enforce the Privacy Rule to OCR, but initially delegated Security Rule enforcement to the Centers for Medicare & Medicaid Services. However, since that time, the Secretary recognized that the future increase in electronic health information as a result of the adoption of electronic health records would result in more cases that would implicate the HIPAA Security Rule, and would create an increased need for privacy and security to be addressed jointly. At the same time, having a unified enforcement approach to privacy and security would increase efficiency and result in better enforcement outcomes. Therefore, the Secretary re-delegated to OCR the authority to administer and enforce the HIPAA Security Rule on July 27, 2009.

From April 2003 through September of this year, HHS received more than 64,000 HIPAA Privacy Rule complaints and, since October 2009, we have received over 470 complaints alleging potential violations of the HIPAA Security Rule. The number of complaints that OCR receives has increased nearly every year since 2003, indicating a steadily increasing awareness and concern from the public about the privacy and security of their health information, and about their rights.

In about 15,000 of the more than 22,500 cases eligible for enforcement (*e.g.*, alleging a violation against an entity subject to the HIPAA Rules), we have required covered entities to make changes in privacy and security policies and practices, and to take other corrective actions. These actions have resulted in systemic changes that are designed to benefit all individuals served by the covered entities. The number of entities taking corrective action to resolve existing and prevent future compliance problems as a result of OCR enforcement continues to increase steadily each year. In the other 7500 cases eligible for enforcement, OCR investigations found no violation.

Since 2003, we have continued to see many of the same compliance issues through our investigations, and we have used our strongest enforcement tools to address some of these common issues.

For example, we see cases of employees inappropriately accessing patient information, in many cases in electronic data systems, for which they do not have a work-related need. These include hospital employees improperly accessing the health information of ex-spouses, friends, neighbors, or celebrities. Unlike paper systems, the audit trails of electronic systems enhance our ability to identify and track such privacy violations.

We also have seen multiple cases of improper disposal of records – whether it is pharmacies throwing prescription bottles and other health information away in dumpsters that are accessible to the public, or private practices going out of business and leaving patient records behind at their prior places of business.

Many cases involve providers failing to give individuals copies of their records, a fundamental right of individuals under HIPAA and a means of empowering consumers to engage in and manage their own health. Other cases involve misdirected communications, such as explanation of benefits mailings, often resulting from failures to test information systems or other system errors. I will discuss some of these cases in more detail later on in my testimony.

Breach Reports to the Secretary

The HITECH Act required the Secretary to issue breach notification requirements for HIPAA covered entities and their business associates. OCR issued a Breach Notification Rule as an interim final regulation in 2009, effective for breaches discovered on or after September 23, 2009. A breach is an impermissible use or disclosure of individuals' health information under the Privacy Rule which comprises the privacy or security of the information. The Rule requires covered entities to notify individuals, the Secretary, and in some cases, the media, of breaches of unsecured (*e.g.*, unencrypted) protected health information. In the case of a breach at a business associate of a covered entity, the Rule requires that the business associate inform the covered

entity of the breach so that the proper notifications can be made. As of November 4, 2011, OCR has received and posted on its website 364 reports of breaches involving more than 500 individuals.

Larger breaches commonly involve theft or loss of computers or electronic media housing unencrypted health information. For example, each of the six largest breaches this year involved the health information of between 175,000 individuals to over 4.9 million individuals. The three most extensive breaches, involving the health information of a total of almost 8 million individuals, were due to the loss of unencrypted backup media or disk drives. The next two largest breaches, which affected a total of over 900,000 individuals, resulted from the theft of desktop computers. Finally, one breach involving the health information of over 175,000 individuals resulted from a system error that misprinted several thousand documents.

Additionally, OCR has received over 36,000 reports of breaches involving fewer than 500 individuals. The majority of these reports involve misdirected communications and affected just one individual each. Often, the clinical or claims record or other health information of one individual is mistakenly mailed or faxed to another individual.

Resolution Agreements and Civil Money Penalties

The HITECH Act significantly strengthened the Department's ability to take enforcement actions against entities for HIPAA violations by revising and greatly increasing the civil money penalty amounts that may be imposed for violations. Prior to the HITECH Act, the Department had authority to impose on a covered entity a civil money penalty of up to only $100 for each violation, with a calendar year limit of $25,000 for all identical violations. The HITECH Act provided a stronger and more flexible the penalty scheme by creating four categories of violations that reflect increasing levels of culpability – from circumstances where the entity did not know of the violation to circumstances of willful neglect, and by attaching to each tier amounts that significantly increase the minimum penalty amount for each violation. Now, covered entities are subject to penalties that range from $100 to $50,000 or more per violation, with a calendar year limit of $1.5 million for identical violations. Our experience has been that the increased penalty amounts available to the Department have reinvigorated covered entities'

attention to compliance. The Department has authority to use these amounts not only for purposes of imposing civil money penalties but also for determining and negotiating settlement payments with covered entities that have agreed to resolve issues of noncompliance by entering into resolution agreements with the Department.

A resolution agreement is a contract between the Department and a covered entity to settle potential violations and is accompanied by a corrective action plan in which the covered entity agrees to perform certain obligations, such as retraining staff, and to make reports to the Department, generally for a period of three years. During the period, the Department monitors the covered entity's compliance with its obligations. These agreements are reserved to settle investigations with more serious issues and outcomes and generally include payment of a settlement amount. To date, HHS has entered into six resolution agreements. When a case cannot be resolved informally through corrective action, HHS seeks to impose a civil money penalty. Thus far, HHS has imposed a civil money penalty using the increased penalties amounts provided for by the HITECH Act on one covered entity. These cases are instructive for the health care industry because they involve some of the most common compliance issues that we see in our investigations.

For instance, OCR entered into resolution agreements -- in July 2008 with Providence Health and Services (Providence) and in February 2011 with General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass Gen) -- after individuals' health information was stolen from or lost by employees taking the information offsite from the covered entity's premises. Providence and Mass Gen are important examples of the continuing problems that entities have with ensuring that proper safeguards and controls are in place with respect to employees removing and transporting patient information from the covered entity's facility. Providence paid a settlement amount of $100,000 and instituted a plan to revise policies and procedures, train employees, and to encrypt electronic health information on laptop computers and electronic media that are to be taken off the premises by employees. Mass Gen paid $1 million and instituted a plan to revise policies and procedures for employees taking patient information off-site, and training employees on these policies.

OCR also consistently encounters cases that illustrate the ongoing problem with proper disposal of patient information, whether it is in electronic or paper form. OCR entered into resolution agreements -- in January 2009 with CVS Pharmacy, Inc. (CVS), and in July 2010 with Rite Aid Corporation (Rite Aid) -- and obtained payments of $2.25 million and $1 million, respectively, to settle allegations of improper disposal of prescription bottles and other patient information. The investigations were carried out jointly with the Federal Trade Commission, which was investigating potential violations of the Federal Trade Commission Act. In the coordinated action, CVS and Rite Aid also signed consent orders with the FTC to settle the cases. In these cases, CVS and Rite Aid improperly disposed of patient information in unlocked dumpsters behind their retail stores, which were accessible to the public. We continue to work with covered entities to educate them about their responsibilities under the HIPAA Rules to safeguard patient information, including through disposal, and on the importance of ensuring employees know of the proper way to dispose of patient information.

Further, access to patient health information for marketing purposes continues to be a major concern of consumers, and is an issue that the HITECH Act specifically addresses. In December 2010, OCR entered into a resolution agreement with Management Services Organization Washington, Inc. (MSO) to resolve allegations of improper disclosure of patient information for marketing purposes. MSO was required to pay a settlement amount of $35,000. This case was coordinated with the Office of the Inspector General at HHS and with DOJ, which had been investigating MSO for violations of the Federal False Claims Act.

I spoke earlier about the frequency with which OCR encounters problems with hospital employees who inappropriately access information in the hospital's electronic data systems. In July of this year, the University of California at Los Angeles Health System (UCLA) entered into a resolution agreement with OCR and agreed to pay $865,500 to resolve allegations of UCLA employees repeatedly, and without permissible reasons, looking at the electronic health records of two different celebrity patients, as well as numerous other UCLA patients. The corrective action plan required UCLA to, among other things, conduct regular and robust trainings for all employees and implement policies to sanction offending employees.

Finally, one of our most important cases involved the fundamental HIPAA right of an individual to obtain a copy of his or her health information, and the blatant disregard of that right by a covered entity. In February of this year, with DOJ's approval and using the HITECH Act's strengthened penalty scheme, OCR issued a $4.3 million civil money penalty against Cignet Health of Prince George's County, MD (Cignet). Cignet refused to provide 41 patients with copies of their medical records when the patients requested them. Further, Cignet repeatedly failed to cooperate with OCR to resolve the issue, evidencing willful neglect with respect to compliance. OCR places a high priority on the ability of individuals to exercise their rights under HIPAA, and will not tolerate entities that refuse to provide individuals with their rights or cooperate with our investigations.

Other Enforcement Activities

State Attorneys General

OCR continues to leverage important relationships with the Department of Justice and with the Federal Trade Commission in its HIPAA enforcement work. In addition, OCR has been working with the State Attorneys General to coordinate enforcement. The HITECH Act gives State Attorneys General authority to enforce the HIPAA protections by bringing civil actions on behalf of State residents for violations of the HIPAA Rules. The State Attorneys General are authorized to seek injunctive relief or damages in the amount of up to $100 per violation, with a calendar year limit of $25,000 for identical violations. To assist them in their enforcement and to promote a productive and effective enforcement relationship with them, OCR conducted a series of HIPAA training seminars in four cities across the country, with representatives from over 45 States and territories, and the District of Columbia, in attendance. We continue to coordinate with the State Attorneys General, and in the past few months, have provided technical assistance on enforcement to the State Attorneys General in California, Connecticut, Illinois, Massachusetts, Michigan, Rhode Island, South Carolina, Texas, Washington, and Wyoming.

Audits

The HITECH Act authorizes HHS to conduct periodic audits to ensure that covered entities and business associates are complying with the HIPAA Privacy and Security Rules. As a result,

OCR, through the use of contract services, has begun to develop a pilot audit program and will be assessing its effectiveness. Audits will give OCR an ability to assess privacy and security protections and compliance issues on a systemic level, and to identify potential vulnerabilities to help entities prevent problems before they occur. This will complement the incident-based work that we currently conduct with respect to our investigations.

Other Initiatives to Safeguard Health Information

Many other efforts, in addition to OCR's enhanced enforcement activities, are underway to secure and protect highly sensitive patient health information as we move closer to the goal of the wide-spread adoption of electronic health record systems. One such initiative is the National Strategy for Trusted Identities in Cyberspace, signed by the President in April 2011, which calls for the development of a network of secure, interoperable digital credentials. Such digital credentials will enable patients and health care providers to access their electronic health records in a secure manner, and limit instances of inappropriate access as well as medical identity theft. Improving authentication is a key element to achieving the security requirements under the HIPAA Rules and realizing the full potential of the benefits that electronic health records can bring to society.

Closing

As you can see from my testimony, OCR is committed to ensuring the American public enjoys the full protections and rights afforded to them by the HIPAA Rules and to fostering a culture of compliance among the covered entities and business associates to whom individuals have entrusted their personal health information. These efforts also add to the public confidence that the investments being made in electronic health records, and the use of information to improve health, will be done in a way that also safeguards their privacy.

Mr. Chairman, this completes my prepared remarks and I will gladly answer any questions you or other members of the Committee may have at this time.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Deven McGraw**
Director, Health Privacy Project
Center for Democracy & Technology

Before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

YOUR HEALTH AND YOUR PRIVACY: PROTECTING HEALTH INFORMATION IN A DIGITAL WORLD

November 9, 2011

Chairman Franken and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today.

The Center for Democracy and Technology ("CDT") is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

We are at an important juncture in the effort to build a health care ecosystem powered by information technology. The nation is at the beginning of a five-year commitment to achieve widespread adoption and use of electronic medical records by health care providers. The health care system suffers from unsustainable costs and uneven or poor quality, and increased digitization and more robust sharing of health information is widely seen as key to reversing these trends. At the same time, the public consistently expresses concern about the privacy and confidentiality of digital health records. Changes to federal health privacy laws enacted by Congress in 2009 have not been implemented due to regulatory delays, and breaches of electronic health data are far too common.

Failure to build and maintain public trust in the collection and sharing of electronic health information will doom efforts to leverage health information technology (health IT) to promote innovation in the health care sector. In this testimony we discuss some of the key privacy and security challenges that will need to be addressed in

order to provide a firm foundation for realizing the benefits of health IT.

Introduction

Survey data consistently show the public supports health IT but is very concerned about the risks health IT poses to individual privacy.[1] In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and
- 55% were concerned about insurers gaining access to this information.[2]

Health IT has a greater capacity to protect sensitive personal health information than is the case with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing among health care system entities for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption and similar technologies can reduce the risk to sensitive data when a system is breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, the perpetrators will be detected and punished.

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. Tens of thousands of health records can be accessed or disclosed through a single breach. In early October of this year, private medical data for nearly 20,000 emergency room patients at Stanford University Hospital were breached by a billing

---

[1] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005); study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006); Consumer Engagement in Developing Electronic Health Information Systems, AHRQ Publication No. 09-0081EF (July 2009). In the most recent survey conducted by the Markle Foundation, more than 80% of both the public and doctors surveyed said that requiring protections and safeguards for patient privacy was important. http://www.markle.org/publications/1443-public-and-doctors-agree-importance-specific-privacy-protections-health-it (January 2011).

[2] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006).

contractor.[3] Just the month before, Science Applications International Corporation (SAIC) reported a breach of personal medical information from 4.9 million military clinic and hospital patients due to a theft of back-up tapes from an SAIC employee's car.[4] Sadly, such incidents are all too common, with 364 breaches of greater than 500 patient records having been reported to HHS since implementation of federal breach notification rules covering health care entities in 2009.[5] The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[6]

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[7] Without appropriate protections for privacy and security in the healthcare system, people will engage in "privacy-protective" behaviors to avoid having their personal health information used inappropriately.[8] Such privacy-protective behaviors include failing to seek care for sensitive medical conditions, asking health care providers to leave sensitive information out of the medical record, and traveling outside of the area to seek care.[9] According to a 2007 poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be disclosed.[10] A September 2011 study by the New London Consulting commissioned by FairWarning®, a vendor of breach detection software, found that:

- 27.1% of respondents stated they would withhold information from their care provider based on privacy concerns.

---

[3] http://www.nytimes.com/2011/10/06/us/stanford-hospital-patient-data-breach-is-detailed.html?src=twrhp.

[4] Id.

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[6] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[7] See Janlori Goldman, "Protecting Privacy to Improve Health Care," Health Affairs (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), http://www.chcf.org/topics/view.cfm?itemID=12502 (Promoting Health/Protecting Privacy).

[8] Id.

[9] Id.

[10] Harris Interactive Poll #27, March 2007. Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors. National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

- 27.6% said they would postpone seeking care for a sensitive medical condition due to privacy concerns.
- Greater than 1 out of 2 persons said they would seek care outside of their community due to privacy concerns, and 35% said they would drive more than 50 miles to seek care.[11]

The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[12]

Contrary to the views expressed by some, privacy is not the obstacle to great adoption of health IT. In fact, appropriately addressing privacy and security is key to realizing the technology's potential benefits. **Simply stated, the effort to promote widespread adoption and use of health IT to improve individual and population health will fail if the public does not trust it**.

It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult —and more expensive—than building it at the start. Now, in the early stages of health IT adoption, is the critical window for addressing privacy.

We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

To build and maintain the public's trust in health IT, we need the "second generation" of health privacy — specifically, a comprehensive, flexible privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. Such a framework should be based on three pillars:

- Policies to implement core privacy principles, or fair information practices;[13]

---

[11] http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-US-PATIENT-SURVEY.pdf

[12] Protecting Privacy, supra note 7.

- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.[14]

This requires building on – and in some cases modifying – the privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA) so that they address the challenges posed by the new e-health environment. It also requires enacting new rules to cover access, use and disclosure of health data by entities outside of the traditional health care system and stimulating and rewarding industry implementation of best practices in privacy and security.

In a digital environment, robust privacy and security policies should be bolstered by innovative technological solutions that can enhance our ability to protect data. This includes requiring that electronic record systems adopt adequate security protections (like encryption; audit trails; access controls); but it also extends to decisions about infrastructure and how health information exchange will occur. For example, when health information exchange is decentralized (or "federated"), data remains at the source (where there is a trusted relationship with a provider) and then shared with others for appropriate purposes. These distributed models show promise not just for exchange of information to support direct patient care but also for discovering what works at a population level to support health improvement. We will achieve our goals much more effectively and with the trust of the public if we invest in models that build on the systems we have in place today without the need to create new large centralized databases that expose data to greater risk of misuse or inappropriate access.

We are in a much better place today in building that critical foundation of trust than we were three years ago. The privacy provisions enacted in the stimulus legislation – commonly referred to as HITECH (Health Information Technology for Economic and Clinical Health Act) or ARRA (American Recovery and Reinvestment Act) – are an important first step to addressing the gaps in privacy protection. However, more work is needed to assure effective implementation of those privacy provisions and address issues not covered by (or inadequately covered by) the changes in HITECH.

In the testimony below, we call for:

- Prompt release by the Administration of final regulations to implement the HIPAA Privacy and Security Rule changes mandated by HITECH;
- Strengthened accountability through greater transparency about enforcement of privacy and security rules;

---

[13] Although there is no single formulation of the fair information practices or FIPs, CDT has urged policymakers to look to the Markle Foundation's Common Framework, which was developed and endorsed by the multi-stakeholder Connecting for Health Initiative. See http://www.connectingforhealth.org/commonframework/index.html.

[14] See "Policy Framework for Protecting the Privacy and Security of Health Information," http://www.cdt.org/paper/policy-framework-protecting-privacy-and-security-electronic-health-information (May 2008); "Beyond Consumer Consent: Why We Need a Comprehensive Approach to Privacy in a Networked World," http://www.connectingforhealth.org/resources/20080221_consent_brief.pdf (February 2008).

- Baseline privacy and security legal protections for personal health information not covered by HIPAA;
- Appropriate limits on downstream uses of health information by contractors or "business associates;"
- Strengthened accountability for implementing strong security safeguards, like encryption; and
- Protections against re-identification of HIPAA de-identified data.

Addressing Health IT Key Privacy and Security Concerns

Issuance of final regulations to implement the HIPAA Privacy and Security Rule changes mandated by HITECH

Congress enacted a number of important modifications to the HIPAA Privacy and Security Rules to strengthen their protections as the nation moves rapidly to the widespread adoption of electronic health records. Such modifications included:

- Extension of accountability for complying with the HIPAA Privacy and Security rules to contractors (business associates and their subcontractors);
- Requirements to notify individuals and HHS in the event of a breach of health information;
- Strengthening prohibitions on using a patient's personal health information for marketing purposes without the patient's express authorization;
- Clarifying that patients have the right to an electronic copy of any medical information about them that is stored electronically;
- Prohibitions on the sale of personal health information;
- A new right for patients to prohibit the sharing of personal health information with insurers when the patient pays out-of-pocket for care; and
- Stronger enforcement provisions, including higher civil monetary penalties; mandates on HHS to audit entities covered by HIPAA and to pursue violations indicating willful neglect of the law; clarity that individuals can be prosecuted for criminal violations of HIPAA; and express authorization of state attorneys general to enforce HIPAA.

A proposed rule to implement most of the above provisions was issued in July 2010; the comment period closed September 13, 2010. (The exception is the rule requiring notification of individuals in the event of a breach, which was required by Congress to be promulgated in interim final form no later than 180 days after enactment of

HITECH.[15] That interim final rule was made effective as of September 23, 2009, although HHS is expected to respond in the main HITECH rulemaking to comments submitted to that interim final rule.) More than a year later, the final, "omnibus" rule to implement most of these HITECH changes has not yet been issued by HHS, and the latest prediction of release is not until early 2012. In the meantime, providers are actively adopting electronic health records with federal tax dollars authorized by Congress without the benefit of the privacy protections that Congress recognized were important to build public and stakeholder trust in health IT. Congress established an effective date for most of the HIPAA changes mandated by HITECH of 12 months post enactment, or February 2010.[16]

We have seen that it is possible to have regulations released when the Department of Health and Human Services (HHS) believes them to be high priority. The Centers for Medicare and Medicaid Services moved quickly in adopting the rules governing the new Medicare Shared Savings Program under the Affordable Care Act. The comment period for that proposed rule closed on June 6, 2011 – and just over four months later, the final rules were issued. HHS and the Administration should prioritize the release of these rules and ensure that they are issued without further delay.

Strengthen Accountability/Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but until recently, those rules have never been adequately enforced.[17] From 2003 (the date when HIPAA regulations went into effect for most entities) through 2010, the Office for Civil Rights (OCR) within HHS, charged with enforcing the HIPAA privacy regulations, did not levy a single civil monetary penalty against a HIPAA-covered entity, even though that office found numerous violations of the rules.[18] The Justice Department had levied some penalties under the criminal provisions of the statute, but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limited the application of the criminal provisions to covered entities, forcing prosecutors to turn to other laws in order to criminally prosecute certain employees of covered entities who have criminally accessed, used or disclosed a patient's protected health information.[19]

A lax enforcement environment sends a message to entities that access, use and

---

[15] Section 13402(j) of HITECH.

[16] Section 13423 of HITECH.

[17] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008), http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

[18] Id. HHS has extracted monetary settlements (most recently from large chain pharmacies) for what were largely violations of the HIPAA Security Rule. In materials connected with these settlements, HHS made it clear that the amounts being paid in settlement of the alleged violations were not civil monetary penalties.

[19] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences.

disclose personal health information that they need not devote significant resources to compliance with the rules. Without strong enforcement, even the strongest privacy and security protections are but an empty promise for consumers and patients.

In HITECH, Congress took a number of important steps to strengthen HIPAA enforcement:[20]

- State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA, which puts more hands on the enforcement deck.
- Contractors or business associates to entities covered by HIPAA are now directly responsible for complying with key HIPAA privacy and security provisions and can be held directly accountable for any failure to comply.
- Civil penalties for HIPAA violations have been significantly increased. Under HITECH, fines of up to $50,000 per violation (with a maximum of $1.5 million annually for repeated violations of the same requirement) can now be imposed.[21]
- HHS is required to impose civil monetary penalties in circumstances where the HIPAA violation constitutes willful neglect of the law.
- The U.S. Department of Justice (DOJ) can now prosecute individuals for violations of HIPAA's criminal provisions.
- The HHS Secretary is required to conduct periodic audits for compliance with the HIPAA Privacy and Security Rules. (The HIPAA regulations provide the Secretary with audit authority, but this authority has rarely – if ever – been used.)

The HITECH provisions are a major advancement in enforcement of federal health privacy law, and there was an uptick in enforcement activity in early 2011. OCR issued its first civil monetary penalty of $4.3 million on February 21, 2011, against Cignet Health of Maryland for failing to provide patients with requested copies of their medical records and not cooperating with OCR's investigation.[22] In the same week, they reached a $1 million monetary settlement and executed a corrective action plan with Massachusetts General Hospital for failing to secure health data (paper copies of HIV patient records were left on the subway).[23] In 2011, OCR also began training

---

[20] See Sections 13409-13411 of ARRA.

[21] Of note, the increased penalties went into effect on the day of enactment – February 17, 2009. State Attorneys General are limited to the previous statutory limits - $100 per violation, with a $25,000 annual maximum for repeat violations.

[22] http://cdt.org/blogs/harley-geiger/first-hipaa-civil-monetary-penalty.

[23] http://www.fiercehealthcare.com/story/patient-info-lost-subway-earns-mgh-1-million-hipaa-fine/2011-02-25.

state attorneys general on HIPAA enforcement;[24] OCR also requested a $5.6 million increase for its FY2012 budget in order to more effectively comply with enforcement mandates.[25] It is unclear whether this increased recent activity will translate into a sustained, consistent pattern of enforcement activity from OCR.

In addition, OCR rarely provides routine guidance, such as answers to frequently asked questions, to clarify how the rules apply to new circumstances or new technologies. Building public trust in health IT will require a greater understanding on the part of patients and industry stakeholders about health privacy law and policy. HHS should provide regular and proactive communication to both industry and consumers about rights under the law, compliance, best practices, and frequently asked questions. Where uncertainty or misinformation about the law is an obstacle to facilitating the exchange of data that needs to occur to improve our health care system, it should be HHS' job to resolve that.[26]

To strengthen accountability and further build public trust in health IT, CDT has three recommendations: (1) as noted above, increase the amount of informal guidance on compliance with Privacy and Security Rules; (2) increase transparency about HIPAA violations and enforcement activity by OCR and DOJ; and (3) deem providers found to be in *significant* violation of HIPAA (either criminally responsible or found to be in willful neglect of the law) ineligible to receive subsidies under the federal health IT incentive program.

With respect to the second recommendation, OCR issues reports on an annual basis that contain summary statistics such as the number of HIPAA complaints received that year, the general category of the complaint, the number of complaints that were dismissed, the number that were resolved through voluntary corrective action, and the number that were further investigated and pursued. These statistics are helpful but tell us very little about the areas of HIPAA noncompliance that need further attention; they also tell us very little about whether the agency with oversight over HIPAA is doing a good job. Congress should consider requiring greater transparency about enforcement activity from both HHS and DOJ. Such transparency could include more details about the types of violations being reported, more detail about complaints that are handled through seeking voluntary corrective action (which could be done with a random sample if reporting on all such dispositions would be overly burdensome), more detail about the size and type of entities that are the subject of complaints, and more information about the disposition of complaints that are referred by OCR to DOJ for criminal prosecution – all of which could be accomplished without revealing the name of the provider or institution who is the subject of an investigation that may not result in fines or charges.

---

[24] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/sagmoreinfo.html.

[25] http://healthcare.cmtc.com/2011/03/office-for-civil-rights-seeks-additional-funding-for-data-breach-policing/.

[26] http://www.ihealthbeat.org/Perspectives/2009/HHS-Holds-Keys-to-Next-Generation-of-Health-Privacy.aspx%5D

With respect to the third recommendation (declaring a significant HIPAA violation to be a disqualification for health IT subsidies), the Health IT Policy Committee recommended that HHS institute such a policy before the health IT financial incentive program went into affect in 2011.[27] If the purpose of seeking greater enforcement of HIPAA is to build public trust in the use of health IT, it is hard to justify providing taxpayer funds for use of health IT to an entity in significant violation of our nation's privacy laws.

Ensure Appropriate Limits on Downstream Uses of Data by Contractors/Business Associates

HIPAA is not a health data privacy law; instead, the privacy and security regulations under HIPAA cover only certain entities in the health care system – health care providers, insurers, and healthcare clearinghouses – reflecting a limit to the statutory reach of HIPAA.[28] However, HHS also understood that HIPAA covered entities would need to be able to share data with contractors to support routine operations. Under the HIPAA Privacy Rule, entities that contract with HIPAA covered entities to perform particular services or functions on their behalf using protected, identifiable health information (or PHI) are required to enter into "business associate" agreements.[29] The agreements are required to establish both the permitted and required uses and disclosures of health information by the business associate[30] and specify that the business associate "will not use or further disclose the information other than as permitted or required by the contract or as required by law."[31]

This combination of provisions suggests that HHS intended to place limits on what a business associate can do with health information received from a covered entity. However, other provisions of the business associate rules are less clear that business associates must be restricted in how they can use and disclose information received from a covered entity. For example, the Privacy Rule provides that covered entities may not authorize the business associate to access, use or disclose information for activities that the covered entity itself could not do under HIPAA, *except* that the contract may permit the business associate to use and disclose protected health information for the "proper management and administration of the business associate" and for "data aggregation" services related to the covered entities' operations.[32] Thus, if an activity to "manage" a business associate would be prohibited by HIPAA, the business associate agreement is still permitted to authorize

---

[27] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911073_0_0_18/PSWG%20Recommendation%20Letter_Regs_final.pdf; see also https://www.cdt.org/blogs/deven-mcgraw/hhs-releases-rules-electronic-health-records.

[28] Section 1172 of the Social Security Act; 45 CFR 164.104.

[29] 45 CFR 164.502(e)(1) & (2).

[30] Id.

[31] 45 CFR 164.504(e)(2)(ii)(A)

[32] 45 CFR 164.504(e)(2)(i).

the business associate to perform this activity. In addition, business associate agreements may permit the business associate to use protected health information to "carry out its legal responsibilities."[33]

Privacy advocates have long suspected that some business associate agreements do not tightly restrict a business associate's use of personal health information. One large national business associate has been accused of using data they receive from covered entities to support other business objectives.[34] Recently CDT has reviewed an electronic health record vendor agreement that authorizes the vendor/business associate to use information from the EHR for any purpose not prohibited by HIPAA (e.g., not just acting on behalf of the provider). We also have heard anecdotal reports of a business associate agreement with a medical device manufacturer also authorizing the manufacturing to use information from the device for its own business purposes. The extent of this problem is not known, because, to the best of our knowledge, OCR does not audit business associate agreements – and if such audits are occurring, the results have not been publicly shared.

In HITECH Congress took a significant step toward strengthening oversight for business associates by making them directly accountable to federal and state regulators for failure to comply with HIPAA or the provisions of their business associate agreements.[35] In the proposed rule to implement the HITECH changes, HHS proposed extending this accountability to subcontractors of business associates, taking positive steps toward maintaining a consistent level of accountability for privacy and security protections as personal health data moves downstream.[36] CDT strongly applauds these actions.

However, CDT remains concerned that the HIPAA Privacy Rule is still not sufficiently clear with respect to the important role of business associate agreements in placing clear limits on how business associates and their subcontractors can use and disclose patient data received from covered entities. The reports of business associates using health information to develop additional lines of business not directly related to the services they have been asked to perform by their covered entity business partners are: (1) an indication that HIPAA is not being adequately enforced, and/or (2) evidence that some business associate agreements are too permissive with respect to additional uses of information. In this testimony CDT calls for stronger enforcement of HIPAA, and this should include stronger oversight of business associates and business associate agreements. Further, in comments to HHS, CDT has urged revising the Privacy Rule to require business associate agreements to expressly limit the business associate's access, use and disclosure of

---

[33] 45 CFR 164.504(e)(4)(i).

[34] See http://www.alarmedaboutcvscaremark.org/fileadmin/files/pdf/an-alarming-merger.pdf, pages 14-16.

[35] ARRA, section 13404.

[36] 75 Fed. Reg. 40867-40924, at 40885 (July 14, 2010).

data to only what is reasonably necessary to perform the contracted services.[37] Failure to appropriately account for and control downstream uses of data will jeopardize trust in health IT.

Establish protections for health data not covered by HIPAA

As noted above, HIPAA covers only covered entities and the contractors/business associates who provide services on their behalf. But health information is being increasingly shared on the Internet and stored in mobile devices, largely due to an explosion of health and wellness products and services that are aimed at, and largely used by, consumers. To keep pace with changes in technology and business models, additional legal protections are needed to reach new actors in the e-health environment and address the increased migration of personal health information out of the traditional medical system.

According to the Pew Research Center's Internet & American Life Project, a whopping 80% of Internet users look for health information on-line.[38] This represents 59% of total U.S. population, since not everyone is on-line. Searching for health information is the third most popular on-line pursuit (behind e-mail and use of a search engine), with searches for symptoms and treatments the most common. About 50% of those searching for health information on-line say they are looking "on behalf of someone else."[39] Individuals are increasingly participating in social networking sites dedicated to sharing health concerns.[40] Today there are 9,000 consumer health apps available in the Apple store, and research2guidance estimates that about 500 million people will be using mobile health apps by 2015.[41] Consequently, Internet search providers, app developers, and mobile service providers have access to, and/or are storing and sharing, sensitive health information – and none of them are covered by federal health privacy and security rules.[42]

Personal health records (PHRs) provide opportunities for consumers to store and share electronic copies of their health information and are being offered by Internet companies like Microsoft,[43] No More Clipboard,[44] or by employers, such as through

---

[37] http://www.cdt.org/comments/cdt-comments-hhs-proposed-rule (hereinafter, CDT Comments).

[38] http://www.pewinternet.org/Reports/2011/HealthTopics.aspx.

[39] Id.

[40] http://cdt.org/blogs/harley-geiger/social-networking-sites---they're-not-just-revolutions-anymore. A list of some of these sites, also called "e-patient communities," can be found at http://epatientdave.com/communities/.

[41] http://www.research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/.

[42] Some may be covered as "business associates" if they are providing a service on behalf of an entity covered by HIPAA – but most of these entities provide services directly to consumers.

[43] http://www.microsoft.com/en-us/healthvault/.

the Dossia Consortium.[45] Only seven percent of individuals report using a PHR — but that number has doubled since 2008.[46] PHRs also are not covered by the HIPAA regulations unless they are being offered to consumers by HIPAA covered entities or business associates acting on the covered entity's behalf. (Kaiser offers a PHR to its enrollees, and this PHR is covered by HIPAA because it is offered to individuals by a covered entity (Kaiser).) In HITECH, Congress mandated breach notification for PHR vendors – but beyond that law, consumer privacy is protected only by the PHR offeror's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information). If these policies are violated, the FTC may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.[47]

HHS recently released a model privacy notice, intended to help consumers compare the privacy policies of entities offering PHRs.[48] HHS describes it as a "nutrition label" for privacy policies. We applaud this effort and the willingness of the PHR vendors mentioned above to volunteer to be part of this initiative. Although it may help consumers navigate an often-confusing PHR marketplace, it is no substitute for a comprehensive set of privacy and security policy protections that apply to health data stored and shared on the Internet.

The absence of any clear limits on how these entities can access, use and disclose information is alarming – and has motivated some to suggest extending HIPAA to cover PHRs and other consumer health tools. However, CDT cautions against applying a one-size-fits-all approach. The HIPAA regulations set the parameters for use of information by traditional health care entities and therefore permit access to and disclosure of personal health information without patient consent in a wide range of circumstances. As a result, it would not provide adequate protection for PHRs or other health applications, where consumers should be in more control of their records, and may do more harm than good. Further, it may not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to

---

[44] http://www.nomoreclipboard.com/.

[45] http://www.dossia.org//.

[46] http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.

[47] The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

[48] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_4108_1176_15440_43/http%3B/wci-pubcontent/publish/onc/public_communities/p_t/privacy_and_security/model_phr_privacy_notice_home_portlet/files/phr_model_privacy_notice_backgrounder___final.pdf.

take the lead in enforcing consumer rights and protections with respect to Internet and mobile health tools.

CDT applauds Congress for not extending HIPAA to cover all PHRs.[49] In HITECH, Congress did enact provisions requiring PHR vendors to notify individuals and the FTC in the event of a breach of personal information, and this was a positive step forward. Congress also directed HHS to work with the Federal Trade Commission (FTC) to come up with recommendations for privacy and security protections for PHRs. This PHR "study" was due February 2010 but has not yet been released.

The agencies need not start from scratch in developing their recommendations. In June 2008, the Markle Foundation released the Common Framework for Networked Personal Health Information outlining a uniform and comprehensive set of meaningful privacy and security policies for PHRs. This framework was developed and supported by a diverse and broad group of more than 55 organizations, including technology companies, consumer organizations (including CDT) and entities covered by HIPAA.[50] In addition, CDT in 2010 issued a report with further guidance to regulators on how the provisions of the Markle Common Framework could be implemented in law.[51] Establishing these protections will likely require Congress to extend additional authority to HHS and/or the FTC.

Congress also should ensure that bills to protect consumer privacy on the Internet include protections for health data. At present, most privacy legislation pending in Congress does not offer specific protections to health data. The Commercial Privacy Bill of Rights Act, sponsored by Senators Kerry and McCain, does apply privacy protections to "information related to a particular medical condition or health record."[52] Likewise, Senator Blumenthal's Personal Data Protection and Breach Accountability Act of 2011 would ensure that companies not covered by HIPAA would notify individuals in the event of a breach their sensitive health information.[53] These bills take an important step forward in safeguarding health information outside of HIPAA, and CDT hopes that other commercial privacy and data breach bills do the same. The sensitivity of medical data is too great to leave out the privacy protections needed for the evolving marketplace for commercial health information.

---

[49] Under ARRA, PHRs that are offered to the public on behalf of covered entities like health plans or hospitals would be covered as business associates. Section 13408.

[50] See http://connectingforhealth.org/phti/#guide. A list of endorsers can be found at http://www.connectingforhealth.org/resources/CCEndorser.pdf.

[51] "Building a Strong Privacy and Security Framework for PHRs," http://www.cdt.org/paper/building-strong-privacy-and-security-policy-framework-personal-health-records (July 2010).

[52] S.799, The Commercial Privacy Bill of Rights Act of 2011, Sec. 3(6)(B)(i).

[53] S.1535, Personal Data Protection and Breach Accountability Act of 2011, Sec. 3(15)(F)(iv).

Strengthen Accountability for Strong Security Safeguards

The Health Information Management Systems Society (HIMSS) releases an annual study of data security initiatives adopted by hospitals and outpatient care centers. The data from the 2011 survey was released just last week:

- Nearly one-quarter of respondents say their organization does not conduct annual risk assessments (which are required under the HIPAA Security Rule);
- Only about half say their organization has a chief security officer, chief information security officer, or another full-time staff member to handle data security responsibilities;
- 53% reported spending 3% or less of organizational resources on security; and
- 14% said at least one patient had reported a case of medical identity theft during the last year.[54]

The prospect of storing and moving personal health data electronically in an environment where security is a low institutional priority should give us all pause. We need – through certified electronic health record requirements and enhancements to the HIPAA Security Rule – stronger requirements with respect to data security, as well as more proactive education and guidance from regulators.

Under the HITECH EHR incentive program, the certification requirements for EHRs include a number of important security functionalities, including the ability to encrypt data in motion and at rest, the ability to generate an audit trail, and authentication and access controls.[55] However, there is no clear requirement, either in the criteria for eligibility for a stimulus payment or in the HIPAA Security Rule, to actually implement and routinely use these functionalities. OCR should provide guidance to providers with certified EHR systems with respect to implementing the security functionalities built into those systems; to date, no such guidance has been issued.

The new breach notification provisions of HITECH provide an incentive for health care providers to encrypt health information using standards approved by the National Institute of Standards and Technology (NIST). Specifically, entities are not required to notify individuals or HHS of a breach if the information that is breached is encrypted, and the encryption key has not been stolen or compromised. This safe harbor for encryption was enacted to provide a strong incentive for health care providers to encrypt. But we know from the statistics on breaches that have occurred since the notification provisions went into effect in 2009 that the health care industry appears to be rarely encrypting data. To the best of our knowledge, no one has done a comprehensive study of the reasons why the health care industry has not embraced the use of encryption.

---

[54] http://www.ihealthbeat.org/articles/2011/11/4/data-security-makes-up-small-portion-of-health-organization-it-budgets.aspx.

[55] http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf.

We note that at least two-thirds of the breaches that have been reported to HHS have been due to lost or stolen media (laptops, computers and thumb drives), none of which was encrypted at the time of the theft.[56] Because this represents the highest risk of exposure for PHI, CDT urges policymakers to focus on strengthening incentives for encryption – or requiring it – for media that are at high risk for theft or loss. For example, HIPAA rules could be strengthened to require encryption in these cases. As an alternative, encryption could continue to be "addressable" under the Security Rule (not required but strongly encouraged), and OCR could issue guidance on the factors OCR will use in evaluating decisions not to encrypt health data on media at risk of theft or loss. The cost of encryption varies depending on the amount of data to be protected and the encryption tool chosen – but most solutions for media at risk of theft or loss appear to be cheaper than the cost of a breach. Ponemon Institute has estimated the cost of a healthcare breach to be $294 per individual affected by the breach.[57] The mean breach size reported to HHS is about 38,000 individuals – at a cost of $294 per individual, that's a cost of over $11 million.[58]

Strengthen Protections Against Re-identification of HIPAA De-Identified Data

HIPAA's protections do not extend to health information that qualifies as "de-identified" under the Privacy Rule. As a result, covered entities may provide de-identified data to third parties for uses such as research and business intelligence without regard to HIPAA requirements regarding access, use and disclosure. In turn, these entities may use this data as they wish, subject only to the terms of any voluntary contractual provisions (or state laws that might apply). If a third party then re-identifies this data – for example, by using information in its possession or available in a public database – the re-identified personal health information would not be subject to HIPAA.[59] It could be used for any purpose unless the entity holding the re-identified data was a covered entity (or had voluntarily committed to restrictions on use of the data).

There is value to making data that has a very low risk of re-identification available for a broad range of purposes, as long as the standards for de-identification are rigorous, and there are sufficient prohibitions against re-identification. Neither condition is present today. A number of researchers have suggested it may be

---

[56] http://www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml.

[57] http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.

[58] From a webinar conducted by Dixie Baker, SAIC, Encryption: Making the Business Case, http://www.healthcareinfosecurity.com/webinarsDetails.php?webinarID=233.

[59] If a covered entity has a reasonable basis for knowing that the recipient of "de-identified" data will be able to re-identify it, the data does not qualify as de-identified. See 45 C.F.R. 164.514(b)(2)(ii).

relatively easy it is to re-identify some data that qualifies as de-identified under HIPAA.[60]

Congress recognized this, and ARRA requires HHS to do a study of the HIPAA de-identification standard; that study, due in February 2010, is significantly delayed. CDT has urged HHS to revisit the current de-identification standard in the Privacy Rule (in particular, the so-called "safe harbor" that deems data to be de-identified if it is stripped of particular data categories) to ensure that it continues to present *de minimis* risk of re-identification.[61] CDT recently held a workshop on HIPAA de-identification attended by industry stakeholders and consumer groups, and we will be releasing a set of specific policy recommendations in the coming months. We will share these with the subcommittee when they are ready.

Conclusion

To establish greater public trust in HIT and health information exchange systems, and thereby facilitate adoption of these new technologies, a comprehensive privacy and security framework must be in place. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. Thank you for the opportunity to present this testimony, and I would be pleased to answer any questions you may have.

---

[60] See, for example, Salvador Ocha, Jamie Rasmussen, Christine Robson, and Michael Salib, Re-identification of Individuals in Chicago's Homicide Database, A Technical and Legal Study (November 2008),

http://web.mit.edu/sem083/www/assignments/reidentification.html (accessed November 20, 2008).

[61] See http://www.cdt.org/healthprivacy/20090625_deidentify.pdf for a more comprehensive discussion of CDT's views on the HIPAA de-identification standard.

United States Senate

Committee on the Judiciary

Testimony before the Subcommittee on Privacy, Technology and the Law

Implementation and Enforcement of Privacy Rules

and the Electronic Health Record

November 9, 2011

Kari L. S. Myrold
Privacy Officer
Hennepin Healthcare System, Inc.
d/b/a Hennepin County Medical Center
Minneapolis, Minnesota

Introduction

Mr. Chairman, Ranking Member Coburn, distinguished members of the Subcommittee, thank you for this opportunity to testify on behalf of a hospital that has implemented an electronic health record and information privacy and security rules for that record. My name is Kari Myrold and I am here on behalf of Hennepin County Medical Center in Minneapolis as their Privacy Officer.

Organizational Overview

Hennepin County Medical Center (HCMC) is operated by the Hennepin Healthcare System, Inc., a public subsidiary corporation owned by Hennepin County. HCMC is a 477 bed safety net teaching hospital with numerous in-house and specialty clinics and six primary care clinics located throughout the metro area. HCMC has been recognized for 15 straight years on the *US News and World Report* list of top hospitals. HCMC is:

- Minnesota's premier Level 1 Adult Trauma Center and Level 1 Pediatric Trauma Center with many nationally recognized programs and specialties and approximately 100,000 Emergency Services visits annually;
- The third largest hospital in Minnesota, based on operating revenue;
- An essential teaching hospital for numerous students of many professions including doctors and over 1000 medical residents each year;
- A safety net hospital providing care for low-income, the uninsured and vulnerable populations; and
- A major employer and economic engine in Hennepin County.

Electronic Health Record History

In late 2002 HCMC embarked on a journey toward an electronic health record (EHR). HCMC chose to replace a number of "best of breed" applications that had been implemented throughout the

organization. These individual models did not interface with one another. HCMC wanted a fully integrated clinical and revenue cycle system for its hospital and clinics. This $68M capital investment was supported by a return on investment analysis demonstrating a seven year payback which is on schedule to deliver. HCMC was driven in this endeavor by a vision that included enhancing the experience of its patients, improving patient quality and safety, supporting research and education, and sustaining the financial viability of the organization.

Principles that guided HCMC along the way included designing an EHR that would support standardized workflow, creating an environment to enhance the patient and provider experience, and improving clinical and financial performance. Design also included an environment that would be patient-focused and actively engage patients in their care. It was also a desire of HCMC to standardize processes and tools throughout the enterprise and capture current data for measurement and continuous improvement. More importantly, HCMC wanted to be able to facilitate communication between caregivers for coordinated interdisciplinary care.

EHR vendor selection involved over one hundred full-time and temporary staff from interdisciplinary teams who drafted the design criteria; it took two years to go from design phase to a signed contract. HCMC used a phased approach for implementation, with six waves occurring from 2005 - 2007. Since that time, HCMC has continued to add functionality for specialties as well as becoming an early adopter of Epic's Care Everywhere® (health information exchange application), MyChart® (electronic patient chart access application), and most recently, Care Link® (a web-based application for community users). The addition of these modules allows for record sharing among providers and with our patients. The hardware and software upgrades along with regular maintenance are continuous.

HCMC has representatives on all of the major e-Health Committees in Minnesota, including HIE, Privacy and Security, and Standards. Through active involvement, HCMC is able to influence direction at the state level and collaborate with our peer organizations. HCMC is also active in the Minnesota Epic User Group and has numerous staff qualified to present at Epic conferences. The working relationship we have with our vendor has been very instrumental to our success.

Through performance and improvements in our EHR, HCMC has achieved Stage 6 (of 7) of the HIMSS Analytics EMR Adoption model; only 4% of hospitals nationwide have achieved this standing. We hope to achieve Stage 7 in 2012. In addition, and as testament to our EHR being able to capture data for measurement purposes, HCMC was an early attester to Stage 1 of Meaningful Use; only 10% of hospitals nationwide have achieved this so far.

Implementation of Privacy and Security Protections

One of the first examples to not only test the viability of HCMC's EHR, but also the privacy regulations, involved the collapse of the 35W bridge in Minneapolis on August 1, 2007. EHR was a critical help in treating our patients in a very difficult, mass casualty situation. This is what Marsha Zimmerman, HCMC's EHR Clinical Director, said about our use of the EHR after the collapse:

"The initial direction from some of the ED and ICU docs was to go back to paper, but they quickly determined that it was faster and easier to actually do their work on Epic. It also allowed us to do some first time access auditing of staff. "[1]

For a public entity, complying with federal data privacy requirements was an expansion of what Minnesota already had in place. As a public hospital, HCMC had to comply with the Minnesota Government Data Practices Act[2] already. For non-profit and other privately operated organizations federal privacy and security regulations posed a greater challenge. Minnesota also had in place the Minnesota Medical Records Act which provided protections for information privacy as well as patient's rights. [3]

When compliance with federal mandates in the Health Insurance Portability and Accountability Act (HIPAA)[4] became a reality for many organizations (April 14, 2003 for the Privacy Rule, and April 20, 2005 for the Security Rule), the way healthcare was transacted changed for the better. Although it will be a continuous climb to perfect the regulations for patients, providers and third parties, it was necessary.

Addressing Improvements to Privacy Issues Surrounding an EHR

1. Policies and Procedures for Privacy and Security Compliance

The time and effort that continues to be put into policy and procedure development by organizations is extraordinary, not to mention the amount of inconsistencies found when comparing one organization to another. When responding to an Office of Civil Rights (OCR) investigation, one of the items they review consistently is policies. They are quick to point out where a policy is lacking for compliance or enforcement purposes, but will also make helpful suggestions to improve upon an organizations effort. An initial effort to set forth model policies defining expectations would have been very helpful.

2. Business Associates

Because we are still awaiting the final rule on this topic from HHS, there is no shortage of parties still confused as to whether they are engaging in a business associate relationship. Once a determination is made that such a relationship exists, negotiating the terms of a "Business Associate Agreement" begins: Who determines if there is a breach? By what standards? Who notifies who? What

---

[1] Marsha Zimmerman, RN, MA, EHR Clinical Director HCMC (November, 2011)

[2] Minn. Stat. Chap.13

[3] Now known as the Minnesota Health Records Act, Minn.Stat.§144.291 - 298

[4] 42 C.F.R. 160, 162 & 164

recourse does any party have, including the multitude of patients that have had their privacy breached by a contracted party? Where do subcontractors fit in?

HCMC has stiff requirements for contracting parties that include: signing business associate agreements that limit the amount of information accessed, actually requesting the business associate to define what type of PHI they will be accessing or using and how they will be using it; requiring privacy training for EHR users; and, compliance with security requirements, including having a recent security assessment available for review.

A final rule containing additional guidance is necessary in order for all parties to better understand their roles, responsibilities and consequences.

3. Data Breach Notification

One of the key functions of having an EHR is the ability to be able to run audits for determining inappropriate uses or accesses of patient information. An EHR allows you to run reports by patient, provider, department, etc. The regulations and this new tool presented a culture change for caregivers in that they no longer were able to follow their patients due to the lack of a continuous caregiver relationship.

> "HCMC had a Security/Compliance/Legal workgroup during the implementation. We, early on, determined that we couldn't fight the rules/regulations since we weren't in charge of them, but we could design and implement a system that supported the rules and provided access to information for the staff that needed to have this information. I grew up in the Emergency Department as a nurse, and had, as did my medical and nursing peers, a concern about what happened to my patients when they left the ED. It was hard to transition to a new reality where we could no longer access a patient's to follow their care. HCMC also decided to have a balance between the EHR restricting and/or controlling access to functionality and an expectation that staff needed to only access the information they needed to do their job."[5]

While awaiting publication of a final rule on data breach notification by HHS, organizations have established independent harm analysis criteria for notification ranging from no analysis, to lengthy "objective" checklists, to holding breach team meetings in a multidisciplinary fashion in hopes of achieving consensus, to including peers of those whose privacy was breached on decision-making groups. Without guidance, there is inconsistency in application of the rules for notification.

In addition to the large breach postings it would be helpful to have a generic (non-identifying) publication of breaches that are below the 500 patient threshold indicating the types of breaches received, the process in evaluating such breaches, and how they are resolved.

---

[5] Marsha Zimmerman, RN, MA, EHR Clinical Director HCMC (November, 2011)

4. Organizational Costs of an EHR and Privacy & Security Rules:

While some organizations were adding Compliance and Information Professionals earlier, many in health care did not get started until the EHR movement picked up and enforcement of the Privacy and Security Rules became a reality. Since then, the C-Suite positions have expanded as have other related professional positions (Ex: CCO, CIO, CMIO, C/PO, C/ISO, EHR staff).

Selection of an EHR is only the beginning – annual maintenance fees, interfacing applications, upgrades, certifications for employees, training and continuing education, and infrastructure support and IT security are but a few of the added and ongoing expenses.

Breach costs – including insurance, investigations, remediation (credit monitoring), auditing and legal expenses are also of concern to providers.

5. Expansion of the definition of "covered entity"

With the expansion of EHR, there is an increasing ease of using "de-identified" data for quality, safety, research, and treatment improvements. HIPAA de-identified data is protected health information that has 18 specified identifiers removed, including demographic information as well as other unique identifiers. This is certainly known by those who are not now considered covered entities or business associates. Expanding the definition to include these future users, or those who sell or share such data without exception or consent, would further protect the privacy of patient data.

6. Encryption

Although designated as the one safety net for the protection of health information, there are far too many organizations still not finding it critical to implement encrypted systems. Cost, lack of IT resources to implement, maintain and control assets, and the perceived distant risk of a breach or lack of enforcement are perhaps some reasons why.

Closing

On behalf of HCMC, I thank you for providing us with this opportunity to share our story with regard to the use of an EHR in today's ever-challenging environment of information privacy and security. If we can be of further assistance in this or related areas please do not hesitate to call on us.

QUESTIONS FOR DEVEN MCGRAW, LEON RODRIGUEZ, AND KARI MYROLD SUBMITTED BY SENATOR AL FRANKEN

Written Questions for Deven McGraw
Senator Al Franken

(1) Can you describe the different rules and regulations that have yet to be issued in a final enforceable form under the HITECH Act?

(2) The HITECH Act required public reporting of breaches of unencrypted health information that affected 500 or more people. To date, there have been 364 separate major breaches of unencrypted health data since 2009 that have affected the health information of over 18 million Americans. The covered entities that suffered these breaches could have avoided public reporting by encrypting their data – but they didn't. Why aren't more entities encrypting their data?

Written Questions for Health and Human Services Office for Civil Rights Director Leon Rodriguez
Senator Al Franken

(1) HHS has received 64,000 complaints, 22,500 of which HHS could investigate. In your testimony, you suggest that the other 40,000 complaints involve entities that are not subject to HIPAA's rules.

The fact is, there are increasing numbers of entities in cyberspace that are getting a hold of medical data and that are not covered by HIPAA or the HITECH Act. There are health-centered social networking sites that allow people to create a profile describing their illnesses and connect with similar patients. There are private health records services that allow you to create your own electronic personal health record. And every time you conduct a search for health information online, your search engine will learn what you're searching about.

Isn't it true that there are a lot of entities that can get American's health information that are not subject to the privacy and security protections of HIPAA or the HITECH Act? Isn't it true that personal health record vendors are not subject to any of the protections of the HIPAA Privacy and Security rules?

(2) It is hard for Congress to know whether HHS is doing its job right when it levies 7 fines for about 22,500 complaints --- because we don't know enough about these complaints. We don't know the kinds of entities being complained about, the nature of the breaches at those entities, or how long it is taking HHS to consider and investigate each complaint.

If HHS were called upon to provide more detailed enforcement statistics, do you think that this is something that the Office of Civil rights could provide?

(3) One in five Internet users goes online to research health information or communicate with other people that have health concerns like theirs. For example, a person can log on to PatientsLikeMe.com, create a profile detailing their struggle with diabetes and connect with others to discuss treatment options of their experience. t is my understanding that apart from that website's privacy policy and the Federal Trade Commission fair trade practices, the health information on these websites is not protected by HIPAA or HITECH. Is that correct? Do you think that this sensitive health data is being protected in the way it should be?

(4) How has Congress provided funding for the use of electronic health records? It is my understanding that funds were made available in the bipartisan American Recovery and Reinvestment Act of 2009 and not in the Affordable Care Act. Is that correct?

Written Question for Kari Myrold
Senator Al Franken

(1) How is your work and that of other privacy officers in other hospitals affected when there are delays in the issuance of implementing regulations under HIPAA or the HITECH Act?

RESPONSES OF DEVEN MCGRAW TO QUESTIONS SUBMITTED BY SENATOR AL FRANKEN

Written Questions for Deven McGraw
Senator Al Franken

(1) Can you describe the different rules and regulations that have yet to be issued in a final enforceable form under the HITECH Act?

At the time when this question was asked (November 2011), the following final HITECH rules and regulations had not yet been issued:

1. Final rules regarding notification to patients and regulators of data breaches (interim final had been released in the Fall of 2010, but HHS had pledged to re-examine them in a "final" final rule);
2. Extension of accountability for complying with HIPAA Privacy and Security Rules to "business associates" (contractors of entities covered by HIPAA);
3. Patient's right to restrict disclosures to health plans of information regarding services that have been paid for in full by patient out-of-pocket;
4. Guidance on compliance with the HIPAA Privacy Rule's "minimum necessary" standard;
5. Changes to the HIPAA requirements to provide patients, upon request, with an accounting of disclosures of identifiable health information;
6. Prohibition on the sale of identifiable health information without prior patient authorization;
7. Right of patients to electronically access, or receive an electronic copy of, their health information when it is maintained in electronic form;
8. Prohibition on the use of a patient's identifiable health information for marketing purposes without authorization;
9. Right of patient to opt-out of having their information used by provider for that provider's fundraising activities;
10. Increased civil monetary penalties, and clarity with respect to criminal sanctions, for noncompliance with HIPAA;
11. Establishment of a methodology to enable patients affected by HIPAA noncompliance to receive a percentage of civil monetary penalties or settlements collected by HHS.

[Note: As of September 23, 2013, final rules have been issued for all of the above except items 4, 5 and 11.]

(2) The HITECH Act required public reporting of breaches of unencrypted health information that affected 500 or more people. To date, there have been 364 separate major breaches of unencrypted health data since 2009 that have affected the health information of over

18 million Americans. The covered entities that suffered these breaches could have avoided public reporting by encrypting their data – but they didn't. Why aren't more entities encrypting their data?

We do not fully understand why more entities are not encrypting their data – in particular, data that is stored in portable media that is susceptible to being lost or stolen (which accounts for a significant majority of the breaches that have been reported under the HITECH Act). Encryption solutions are no longer expensive and do not delay access to data (particularly in circumstances where data is being accessed on portable media, where an additional step to access data will not have a detrimental impact on patient care). All other industries handling sensitive data that we know of routinely use encryption to protect it from inappropriate access.

The only excuse that makes any sense is one of culture. The health care industry is not accustomed to encrypting data; consequently, getting health care providers to encrypt is tantamount to culture change. We do believe it will happen, particularly as breaches continue to embarrass providers. But it likely will take longer than is ideal.

Responses of Leon Rodriguez to Questions Submitted by Senator Al Franken

United States Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
Public Hearing
"Health Information Privacy Enforcement and Electronic Health Records"
November 9, 2011

Written Questions for Health and Human Services Office for Civil Rights Director Leon Rodriguez

Senator Al Franken

(1) HHS has received 64,000 complaints, 22,500 of which HHS could investigate. In your testimony, you suggest that the other 40,000 complaints involve entities that are not subject to HIPAA's rules.

The fact is, there are increasing numbers of entities in cyberspace that are getting a hold of medical data and that are not covered by HIPAA or the HITECH Act. There are health-centered social networking sites that allow people to create a profile describing their illnesses and connect with similar patients. There are private health records services that allow you to create your own electronic personal health record. And every time you conduct a search for health information online, your search engine will learn what you're searching about.

Isn't it true that there are a lot of entities that can get American's health information that are not subject to the privacy and security protections of HIPAA or the HITECH Act? Isn't it true that personal health record vendors are not subject to any of the protections of the HIPAA Privacy and Security rules?

There are many types of entities that handle or have access to individuals' health information but are not covered entities (health plans, health care clearinghouses, and most health care providers) or business associates as defined by HIPAA and its implementing regulations and, therefore, are not subject to the privacy and security protections of HIPAA or HITECH.[1] For example, life insurance companies and health-centered social networking sites are not subject to HIPAA. Furthermore, even some health care entities, such as health care providers who take cash only, are not subject to HIPAA because they do not engage in electronic transactions for which HIPAA provides a standard format, such as claims and billing transactions.

With respect to personal health records (PHRs), section 13408 of the HITECH Act requires that each vendor contracting with a covered entity to provide a PHR to patients be treated as a business associate for HIPAA purposes, and the Privacy Rule now explicitly defines such vendors

[1] Note that, while many of the non-jurisdictional complaints received by HHS involve entities not subject to the HIPAA Rules, some of the complaints HHS receives are not within the Department's jurisdiction because they do not present an eligible case for enforcement for other reasons, such as because they involve activities that do not violate the HIPAA Rules, allege violations that occurred prior to the compliance date, or are untimely or withdrawn.

as business associates. For example, where a covered entity hires a vendor to provide and manage a PHR service the covered entity wants to offer its patients or enrollees, and provides the vendor with access to protected health information to do so, the vendor is a business associate and, therefore, subject to HIPAA. However, a vendor that only offers a PHR directly to individuals, and not on behalf of a covered entity, would not be a business associate and, therefore, would not be subject to HIPAA.

Still, other privacy and security requirements may apply. For example, the Federal Trade Commission's (FTC) Health Breach Notification Rule, which is similar to the HIPAA Breach Notification Rule in many respects, requires certain businesses not covered by HIPAA to notify their affected customers and the FTC (and, in some cases, the media) if there's a breach of unsecured, individually identifiable electronic health information. The rule applies to non-HIPAA covered vendors of PHRs, PHR-related entities, and third-party service providers for a vendor of PHRs or a PHR-related entity.[2] In addition, the FTC's general truth-in-advertising requirements and consumer privacy protections require businesses to explain their privacy practices to consumers and fulfill any privacy promises made.

Finally, many states have enacted laws requiring certain businesses, such as those that handle personal health information, to protect the privacy of their customers' data and notify customers regarding breaches of their information.

(2) It is hard for Congress to know whether HHS is doing its job right when it levies 7 fines for about 22,500 complaints --- because we don't know enough about these complaints. We don't know the kinds of entities being complained about, the nature of the breaches at those entities, or how long it is taking HHS to consider and investigate each complaint.

If HHS were called upon to provide more detailed enforcement statistics, do you think that this is something that the Office of Civil rights could provide?

We currently are developing our reports to the Congress on Privacy Rule and Security Rule compliance and enforcement, and on Breach Notification activities. We will provide these reports to the Committee and post them on OCR's website as soon as possible.

We are continually seeking ways to improve the enforcement information made available through our website and are happy to hear about the type of enforcement data that would be most useful to the public. In addition to information about our enforcement process, OCR currently makes the following information available to the public through its website: A variety of enforcement data, including the number of complaints received by calendar year, the total number of complaints received to date since enforcement began for the Privacy Rule and the

[2] More information on how FTC's Health Breach Notification Rule applies to PHR vendors can be found at http://www.business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule.

Security Rule, the total number of investigations that are closed and reasons for closure (either with corrective action or because no violation was found), and the number of cases closed for administrative reasons without investigation. This information is updated on a monthly basis. In addition, we provide information about cases on a calendar year basis and by state. This information is updated on an annual basis. We also provide in our public enforcement data the types of entities against whom the most complaints are filed and the privacy and security issues raised most often in these complaints. Finally, we post on the website complete documentation of all Resolution Agreements and all civil money penalties assessed.[3]

With regard to breaches, we post on our website a sortable and downloadable listing of breaches that affected 500 or more individuals, including the name and state of the entity reporting the breach; the name of the business associate, if any, involved in the breach; the number of persons affected; the cause of breach; the date of the breach; and the location of the information that was compromised (*e.g.,* laptop computer, paper records). We update the breach website as breaches are reported. In addition, when OCR has completed its investigation of the breach, we update the website with a short synopsis of the breach and remedial action taken in response to the breach. Breaches affecting fewer than 500 individuals are only required to be reported to OCR annually, and we require the annual reports within 60 days of the end of the calendar year. Statistics available for these smaller breaches are included in our report to the Congress on our breach activity.[4]

(3) One in five Internet users goes online to research health information or communicate with other people that have health concerns like theirs. For example, a person can log on to PatientsLikeMe.com, create a profile detailing their struggle with diabetes and connect with others to discuss treatment options of their experience. It is my understanding that apart from that website's privacy policy and the Federal Trade Commission fair trade practices, the health information on these websites is not protected by HIPAA or HITECH. Is that correct? Do you think that this sensitive health data is being protected in the way it should be?

That is correct. The "patientslikeme" website is not considered a covered entity or business associate for HIPAA purposes. However, as you note, such entities may be subject to other privacy and security obligations or legal requirements, such as FTC's consumer privacy protections and state law requirements. Beyond those requirements, as long as a website's

---

[3] Information about OCR's HIPAA enforcement activities is available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.

[4] This report is available on our website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html. Our report on Privacy Rule and Security Rule compliance is available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/complianceretpmain.html.

information privacy practices are transparent to the public, consumers are able to choose whether to accept the potential risks or benefits of joining or using the website.

(4) How has Congress provided funding for the use of electronic health records? It is my understanding that funds were made available in the bipartisan American Recovery and Reinvestment Act of 2009 and not in the Affordable Care Act. Is that correct?

Yes. The American Recovery and Reinvestment Act of 2009 (ARRA) created the Meaningful Use program at the Centers for Medicare & Medicaid Services, and provided funding to award incentive payments to eligible professionals, eligible hospitals, and critical access hospitals as they adopt, implement, upgrade, or demonstrate Meaningful Use of certified electronic health record (EHR) technology. Further, ARRA provided funding to the Office of the National Coordinator for Health IT to invest in health information technology infrastructure activities including, among many other initiatives, electronic health information exchange across states, standards harmonization and development, regional extension centers to assist health care providers in using EHR technology, and health IT education and workforce development. The Affordable Care Act did not make specific funds available for the use of EHRs.

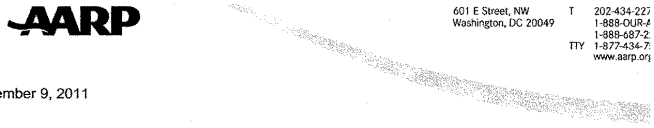
Responses of Kari Myrold to Questions Submitted by Senator Al Franken

Written question for Kari Myrold

Senator Al Franken

(1) How is your work and that of other privacy officers in other hospitals affected when there are delays in the issuance of implementing regulations under HIPAA or the HITECH Act?

Although the current interim regulations provide a pretty good picture of what *may* be required, the temporary status of the regulations creates a feeling of being in 'limbo'. The longer it takes, the more organizations will focus and apply their resources toward other priorities - "if it is not a priority to get the final rules out, why should it be a priority for us to address any changes we *might* have to make?" Organizations may tend to procrastinate while they wait to see what changes will be final. This results in a lack of compliance. Credibility is also lost with such delays. Final changes may affect personnel decisions and the purchasing of software applications or other tools to assist in implementation. The fact that another budget cycle just passed for many organizations means requests for additional resources may be out for another year. On the other hand, if organizations have made changes based on the interim rules they may find that they have wasted or misdirected resources once the regulations are final – policy implementation, form development and training are but a few examples. Finally, without final rules and the much needed guidance that should accompany the rules, there will continue to be confusion and inconsistent application of the regulations – application of the breach notification rule as stressed in my written testimony is one of the best examples.



601 E Street, NW
Washington, DC 20049

T 202-434-22
1-888-OUR-A
1-888-687-2
TTY 1-877-434-7
www.aarp.org

November 9, 2011

The Honorable Patrick Leahy
Chairman
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Honorable Charles Grassley
Ranking Member
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Honorable Al Franken
Chairman Subcommittee on Privacy,
Technology and the Law
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member, Subcommittee on Privacy,
Technology and the Law
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

Dear Senators Leahy, Grassley, Franken and Coburn:

On behalf of our millions of members, we are writing to reiterate AARP's long-held support for an effective, safe, and efficient health care system that relies on health information technology (HIT) to improve health care quality, safety, promote patient engagement, and stimulate greater efficiency in the health care system. We believe this integration should be accomplished without compromising the confidentiality of personal health information and data security, and in such a way as to reassure the public that individuals' personal health information will be protected from inappropriate uses.

HIT is a critical enabling tool to improve care and to support the efficient use of health care resources. We applaud Congress for action already taken in the Patient Protection and Affordable Care Act (ACA), the American Recovery and Reinvestment Act (ARRA), and other legislation that recognizes the value of HIT in health care and advances its use. The many advantages of HIT and data exchange include:

- Reduction of medical errors by helping to eliminate mistakes that arise from poor handwriting or lack of complete medical records;
- Decision support for clinicians and patients through access to information, prompts for best practices, educational information, etc;
- Facilitation of information-sharing at critical times in non-emergent situations to enhance opportunities for care coordination and integration across settings and between and among providers;

- Reduction of duplicate tests and procedures that are now commonly performed because records are not available when they are needed;
- Facilitation of data collection to measure performance and accelerate the development of interventions to address identified problems;
- Facilitation of data collection on race, ethnicity, and other patient characteristics that give rise to health care disparities. Without data, it will be impossible to assure equitable care for all;
- Support for public health initiatives by providing access to data to help avert public health threats;
- Elimination of redundant paperwork and the need for patients to repeat medical history and demographic data;
- Greater consumer engagement by giving patients and family caregivers access to information they need to support self-management; and
- Access to a wide array of technologies that help people stay in their own homes and out of institutions and also allow them to access needed health care services remotely through non face-to-face encounters with clinicians and other medical personnel.

Privacy

HIT can enhance privacy protections in many ways, but it also raises new concerns that we must address. Paper-based records allow anyone who can gain access to the files to see, copy and share sensitive information with little chance of detection. HIT establishes firewalls, requiring passwords and permission to gain access, and leaves an audit trail of who accessed or altered the data. However, electronic records also have potential for breaches, data-mining, and misuse of sensitive data that could undermine consumer confidence in HIT. If privacy protections are inadequate, consumers may withhold information or forego treatment to avoid embarrassment and discrimination. For HIT to thrive, consumers need significant assurances that adequate protections and deterrents are in place to safeguard their personal health information. Enforcement through appropriate sanctions must be rigorous.

While HIT can allow people with heightened privacy concerns to identify subsets of their records that they do not want shared, such as those for mental health, HIV/AIDS, reproductive health, and other sensitive data, the technology to provide absolute assurance that such data can be protected does not yet exist. AARP believes that there needs to be adequate attention to integrating strong privacy policies into the technology as it is developed. Protecting personal health information should not be an afterthought -- it must be integral to the technology itself.

Given the enormous potential to improve quality and efficiency, consumers should not be forced to choose between HIT and privacy. And, despite outstanding privacy concerns, there is broad support among a majority of the American public for advancing HIT. They understand the value it can bring to health care and their own lives. However, they want to be reassured that the value that HIT and data exchange brings also will promote trust and protect the privacy, security, confidentiality, and integrity of their health data.

AARP urges Congress to continue to recognize and support HIT's enormous potential to improve the safety, effectiveness, and efficiency of care without compromising the confidentiality of personal health information and data security. If you have any questions, please feel free to call me or have your staff contact Leah Cohen Hirsch on our Government Affairs staff at 202-434-3770.

Sincerely,

Joyce A. Rogers
Senior Vice President
Government Affairs