STANDARDS FOR HEALTH IT: MEANINGFUL USE AND BEYOND

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 30, 2010

Serial No. 111–112

Printed for the use of the Committee on Science and Technology

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

U.S. GOVERNMENT PRINTING OFFICE

58–489PDF WASHINGTON : 2010

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 SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chair*

JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DAVID WU, Oregon
BRIAN BAIRD, Washington
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
STEVEN R. ROTHMAN, New Jersey
JIM MATHESON, Utah
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
RUSS CARNAHAN, Missouri
BARON P. HILL, Indiana
HARRY E. MITCHELL, Arizona
CHARLES A. WILSON, Ohio
KATHLEEN DAHLKEMPER, Pennsylvania
ALAN GRAYSON, Florida
SUZANNE M. KOSMAS, Florida
GARY C. PETERS, Michigan
JOHN GARAMENDI, California
VACANCY

RALPH M. HALL, Texas
F. JAMES SENSENBRENNER JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
MICHAEL T. McCAUL, Texas
MARIO DIAZ-BALART, Florida
BRIAN P. BILBRAY, California
ADRIAN SMITH, Nebraska
PAUL C. BROUN, Georgia
PETE OLSON, Texas

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chair*

DONNA F. EDWARDS, Maryland
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
HARRY E. MITCHELL, Arizona
GARY C. PETERS, Michigan
JOHN GARAMENDI, California
BART GORDON, Tennessee

ADRIAN SMITH, Nebraska
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
PAUL C. BROUN, Georgia

RALPH M. HALL, Texas

HILARY CAIN *Subcommittee Staff Director*
MEGHAN HOUSEWRIGHT *Democratic Professional Staff Member*
TRAVIS HITE *Democratic Professional Staff Member*
MATT McMAHON *Democratic Professional Staff Member*
JULIA JESTER *Republican Professional Staff Member*
VICTORIA JOHNSTON *Research Assistant*

CONTENTS

September 30, 2010

STANDARDS FOR HEALTH IT: MEANINGFUL USE AND BEYOND

THURSDAY, SEPTEMBER 30, 2010

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:18 a.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

Subcommittee on Technology and Innovation's

Hearing on

Standards for Health IT: Meaningful Use and Beyond

Thursday, September 30, 2010
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witness List

Dr. David Blumenthal
National Coordinator for Health Information Technology,
Office of the National Coordinator, U.S. Department of Health and Human Services

Ms. Kathleen M. Roberts
Associate Director for Federal and Industrial Relations,
Information Technology Laboratory, National Institute of Standards and Technology

Ms. Joyce Sensmeier
Vice President, Informatics, Healthcare Information and Management Systems Society

Dr. Dick Gibson
President, Oregon Health Network

Ms. Deven McGraw
Director of the Health Privacy Project, Center for Democracy and Technology

Ms. Deb Bass
President and CEO, Bass & Associates, Inc.

HEARING CHARTER

COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
U.S. HOUSE OF REPRESENTATIVES

Standards for Health IT: Meaningful Use and Beyond

THURSDAY, SEPTEMBER 30, 2010
10:00 A.M.—12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

I. PURPOSE

The integration of information technology (IT) with health care has the potential to improve patient care and lower escalating health care costs. Standards that enable interoperability among products developed by different vendors, as well as standards to ensure the privacy and security of electronic health care information, are central to realizing the benefits of health IT. In 2009, with the passage of the *American Recovery and Reinvestment Act*, Congress created programs and incentives to help speed the adoption of health IT, including measures to ensure the establishment of technical standards.

The purpose of this hearing is to examine the progress by the Department of Health and Human Services, the National Institute of Standards and Technology, and non-governmental health IT stakeholders in establishing standards for health IT, providing guidance for their implementation, and creating a mechanism to certify that health IT products comply with the established standards. Witnesses will also discuss future priorities for ensuring the interoperability of health IT systems, and the privacy and security of electronic health information.

II. WITNESSES

- **Dr. David Blumenthal**, *National Coordinator for Health Information Technology, Office of the National Coordinator, U.S. Department of Health and Human Services*
- **Ms. Kathleen M. Roberts**, *Associate Director for Federal and Industrial Relations, Information Technology Laboratory, National Institute of Standards and Technology*
- **Ms. Joyce Sensmeier**, *Vice President, Informatics, Healthcare Information and Management Systems Society*
- **Dr. Dick Gibson**, *President, Oregon Health Network*
- **Ms. Deven McGraw**, *Director of the Health Privacy Project, Center for Democracy and Technology*
- **Ms. Deb Bass**, *President and CEO, Bass & Associates, Inc.*

III. BRIEF OVERVIEW

Despite the potential benefits of health IT and electronic health records (EHRs) in lowering health care costs and improving patient care, the health care industry has been relatively slow to incorporate information technology into the delivery of medical services. The lack of established standards for health IT has been a key challenge hindering wider adoption of this technology. Standards ensure that information can be exchanged seamlessly between software and hardware devices developed by different vendors or put on the market at different times.

Through the *HITECH Act* [Title XIII of the *American Recovery and Reinvestment Act* (ARRA), P.L. 111–5], Congress created programs and incentives to encourage health IT adoption. In addition, the Act provided a mechanism to establish technical standards, and further provided that any health IT products purchased with ARRA funds must comply with standards established by the Department of Health and Human Services (HHS). With guidance from several advisory committees, HHS issued a final rule in July of this year identifying the standards that would support

the first stage of Medicare incentive payments for health IT products (termed "meaningful use" requirements).

The initial standards established by HHS provide an important baseline of functionality for health IT products. However, many standards-related issues have not yet been fully addressed. To ensure the seamless exchange of health information among authorized entities and realize the full benefit of health IT, the health care community will need robust standards and related products for interoperability. In addition, the standards process will require coordination to ensure that standards developers are able to support the needs of the health care community as health IT technology evolves. Finally, baseline national privacy and security policies could help health IT developers and users alike maximize the benefits of the technology.

IV. BACKGROUND

The Role of IT in Health Care

Studies and statistics show that a lack of ease in information exchange and communication contributes to medical errors and duplicative tests, and other wasteful practices. For instance, one study found that nearly one out of every five doses of medication given in typical hospitals or skilled nursing facilities was somehow in error. Most often, the medication was delivered at the wrong time, but other times the dosage was wrong or the incorrect medication was administered altogether. The study, in the *Archives of Internal Medicine*, further explained that these errors were harmful to the patient in 7 percent of cases (40 per day in a 300 patient facility)[1]. Other studies have found that miscommunication between doctors, patients, and others involved in patient care was a major factor in 80 percent of medical errors.[2] Health IT could help medical professionals, and their patients, manage complex or chronic conditions, identify harmful drug interactions or possible allergies, and provide other care support tools.

Adoption of health care IT is also widely seen as a way to stem the rising costs of health care. According to a report issued by the National Academies, an estimated half-trillion dollars per year is associated with "overuse, underuse, misuse, duplication, system failures, unnecessary repetition, poor communication, and inefficiency."[3] Although estimates vary on the actual savings that could be expected from health IT, a study published in *Health Affairs* estimated that a fully interoperable, national health IT network could save $77.8 billion a year, equal to 5 percent of annual U.S. health care spending.[4] In addition to reducing costs associated with medical errors, health IT could enable other cost-saving measures such as prompting physicians to prescribe generic drugs or making tests results more readily available, thus avoiding duplicative tests.

Adoption of IT by the Health Care Industry and Technical Standards

The health care industry has been slow to adopt health IT, despite its potential impact. A study published in June of 2008 found that only 4 percent of U.S. physicians had a fully functional electronic health records (EHRs) system, which the authors defined as an EHR system with broad range of capabilities including clinical order entry and clinical decision support. Thirteen percent of those surveyed in the study used a basic EHR, which the study described as one with a minimum set of functionalities, such as recoding laboratory data and clinical notes and electronic prescribing.[5]

One of the key barriers to wider adoption of health IT has been the lack of robust, widely-accepted technical standards. To realize the benefits of health IT, systems must be interoperable, allowing data systems, medical devices, and software from different vendors to share EHRs, as well as electronic physician orders for lab tests and drug prescriptions, electronic referrals to specialists, electronic access to information about current treatment recommendations and research finding, and other capabilities. In addition to the need for standards to ensure that disparate systems

---

[1] Barker, *et al*. 2002 Medication Errors Observed in 36 Health Care Facilities, *Archives of Internal Medicine*.

[2] Woolf, *et al*. 2004 A String of Mistakes: The Importance of Cascade Analysis in Describing, Counting, and Preventing Medical Errors, *Annals of Family Medicine*.

[3] Report by the National Academies, 2005 *Building a Better Delivery System: A New Engineering/Health Care Partnership*

[4] Walker, *et al*. 2005 The Value of Health Care Information Exchange and Interoperability, *Health Affairs*.

[5] DesRoches, *et al*. 2008 Electronic Health Records in Ambulatory Care—A National Survey of Physicians, *The New England Journal of Medicine*

are interoperable, standards are needed to meet data security and privacy requirements to enable compliance with federal and state patient privacy laws.

The Science and Technology Committee held hearings on health IT in the 109th and 110th Congresses. During those hearings, witnesses identified the lack of common standards as one of the challenges facing greater health IT adoption. Witnesses claimed that, without these standards, health care providers would not have a reasonable guarantee that the systems they purchase will be able to exchange information with systems that are currently in use, or that may be installed in the future. At the hearing held in September of 2007, witnesses agreed that NIST should assist HHS in efforts to establish standards for health IT. NIST is the Federal Government's lead agency for supporting the development of technical standards and conformance testing, and has a long history of working with the private-sector, federal agencies, and other stakeholders to develop consensus-based standards in fields such as electronic commerce, manufacturing, and information security.

HITECH Act

Congress passed the *HITECH Act* as part of the *American Recovery and Reinvestment Act* (ARRA) in 2009. The *HITECH Act* established programs and incentives to boost the rate of adoption of health IT systems. It also codified the Office of the National Coordinator for Health Information Technology (ONCHIT)[6] and strengthened provisions pertaining to privacy and security of electronically stored and exchanged health information in federal law. The *HITECH Act* gave ONCHIT the role of overseeing the establishment of standards and a certification process for health IT technology, guided by recommendations from two Federal Advisory Committees—the Health IT Policy Committee and the Health IT Standards Committee—on the "implementation of a nationwide health IT infrastructure."

The *HITECH Act* charged the HIT Policy Committee with providing recommendations on areas in need of standards, implementation specifications, and certification criteria. The Act further charged the Health IT Standards Committee with "develop[ing], harmoni[zing], and recogni[zing]" standards and related material, and providing recommendations on these for consideration by ONCHIT and HHS. The *HITECH Act* directs the ONCHIT to ensure that federal funds expended toward health IT technology go toward certified EHR technology that incorporates the standards and capabilities developed by the Policy and Standards Committees, and promulgated by HHS.

The *HITECH Act* also directs NIST to test the standards, implementation specifications, and certification criteria that emerge from the ONCHIT standards process. Additionally, the *HITECH Act* charges NIST with developing a conformance testing infrastructure, including creating technical test beds, and provided NIST with $20 million to develop this infrastructure. Conformance testing is necessary to ensure that the health IT products meet all of the requirements of the standards and that the standards are correctly implemented. To date, HHS has approved three testing and certification bodies and product certification is expected to begin shortly. In addition to supporting HHS with health IT testing and certification, NIST has assisted HHS with establishing security standards and guidance for health IT products.

Since the passage of the *HITECH Act*, much of the work of the two advisory committees has focused on providing recommendations to the ONCHIT regarding "meaningful use." Under the *HITECH Act*, medical providers are entitled to apply for Medicare incentive payments beginning in 2011 if they adopt EHRs for their patients and meet certain requirements. Finalized in July of this year, these include 15 "core set" requirements and 10 "menu set" options. Meaningful users must meet the 15 core requirements and at least 5 of the menu set options. Core set requirements include using an EHR to record smoking status for 50 percent of patients 13 years of age or older and to maintain an active medication list for 80 percent of patients. The core set includes only one requirement related to data exchange—users must perform at least one test of an EHR's capacity to electronically exchange information. The menu set options include using health IT systems to generate a listing of patients with a specific condition or to perform at least one test data submission of immunization data to immunization registries. As specified in the *HITECH Act*, requirements will be added for future stages of meaningful use.[7]

---

[6] Federal efforts to encourage widespread health IT adoption began in 2004 when President Bush signed an executive order creating the Office of the National Coordinator for Health IT (ONCHIT) within HHS, and stated the goal of widespread EHR adoption within 10 years. ONCHIT initiated a number of activities, including work on standards and certification.

[7] Providers who become meaningful users of EHRs beginning in 2011 are entitled to Medicare incentive payments. For providers adopting EHRs in 2014, no incentive payments will be pro-

Continued

In addition to specifying the basic functionality for certified EHRs, the final rule also included the standards, implementation specifications, and certification criteria required to be met by all certified EHRs.

National Health Information Network

In 2005, HHS began developing a National Health Information Network (NHIN). It was conceived of as a "network of networks" that would allow for the secure exchange of health information among health care providers. In 2007, HHS awarded contracts totaling $22.5 million to nine health information exchanges (HIEs) to begin trial implementation of the NHIN.

ONCHIT has continued work on developing standards and policies for a national health information exchange, whose core capabilities include the ability to look up, retrieve, and securely exchange health information; the ability to apply consumer preferences for sharing information; and the ability to apply and use the NHIN for other business capabilities as authorized by the health care consumer. ONCHIT has continued work on the NHIN, and is now also working on the NHIN Direct project, which will include standards, policies, and services to enable the transport of medical records between authorized providers.

Privacy and Security

A number of state and federal laws and regulations cover the confidentiality of personal health information. On the federal level, the privacy and security of medical information is protected by the *Health Information Portability and Accountability Act* (HIPPA). The *HITECH Act* expanded upon the HIPAA requirements with stricter enforcement mechanisms, requirements for breach notification, and the expansion of the privacy and security regulations to cover business associates of the health care provider.[8] The *HITECH Act* also required HHS to issues guidance on "technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals." Covered entities that follow the guidance issued by HHS but still suffer a security breach are not subject to the breach notification requirements or the stricter penalties enacted in the *HITECH Act*.

The meaningful use requirements give guidance on technologies and methodologies (such as encryption) to protect data. They also require users of health IT systems to perform a risk analysis to determine the nature and likelihood of threats, and to base their security measures on this analysis while considering the cost and complexity of needed security infrastructure.

V. ISSUES & CONCERNS

The standards adopted by HHS for meaningful use are an important step in establishing recognized standards for health IT systems and EHRs. However, while the standards provide a layer of commonality among health IT products, the final rule included only minimal provisions concerning interoperability.

At the same time, throughout the country, medical providers and states are developing electronic health information exchange networks, as well as pursuing other health IT projects. The Federal Government is also pursuing the NHIN and NHIN Direct projects. It is unclear whether, and to what extent, the standards-related components of these efforts are being coordinated to ensure interoperability in the future.

HHS has recently released an initial standards and interoperability framework. This framework will presumably guide the coordination of future standards activities, including harmonization, development, testing, and priority setting. However, HHS has not yet clearly described how it will maintain the transparency and stakeholder input that is an important component of the standards setting and development process. In addition, the framework does not specify how HHS will continue to work with NIST on health IT standards.

The *HITECH Act* strengthened privacy and security protections for patient information by requiring breach notification of readable data and implementing stricter penalties for the disclosure of personal health information. However, there is little

---

vided. By 2015, providers not using EHRs will be penalized through reductions on Medicare payments. Additional requirements will be added in later stages of meaningful use. Note, there is a corresponding timeline for providers who become meaningful users under the Medicaid incentive program.

[8] Relevant business associates include business partners of the provider that may provide various services, such as accounting or management, wherein individually identifiable health information is disclosed.

federal guidance beyond HIPAA for implementing these stricter privacy and security measures. For example, no guidance exists on the federal level on whether individuals must opt-in to or opt-out of an electronic health exchange, or on the granularity, or degree, of patient consent needed to disclose certain types of health information. These are policy questions, often subject to individual state rules, but they impact the technology solutions that will be needed by health care providers. In addition, while the security measures adopted for EHRs allow for flexible implementation, they may prove challenging to implement, particularly among small practices.

Chairman WU. The hearing will now come to order. Thank you all very much for being here today.

I would like to recognize that there is a group of high school students from Beijing, China, with us today. Thank you very much for being here, and I hope that you find this experience edifying for your future studies.

And I thank the witnesses for being here and for traveling, in some instances, long distances.

In the Internet age, most of us take for granted being able to rapidly and seamlessly share information with someone across town, in another state or on the other side of the world. We also take for granted the ubiquitous integration of information technology in our workplace and in many other aspects of our lives.

In contrast, the health care industry is still surprisingly paper-based and is largely unaided by information technology. Medical treatment in this country often involves state-of-the-art technology. However, physicians and other health care providers have been slow to adopt health IT systems and electronic health records—or EHRs—and are still keeping track of our medical information the same way it has been kept historically.

The use of information technology has real-world implications for the cost and quality of health care. Currently, providers may order a duplicative test because previous test results from another provider are not readily at hand, or they may miss a harmful drug interaction because a patient's full prescription drug record is not available. According to most estimates, a fully interoperable health IT system could save us billions of dollars in health care costs each year. In addition, greater use of information technology could prevent some of the medical errors that, as reported by the National Academies, are responsible for the deaths of approximately 98,000 people each year.

A key barrier to broader integration of health IT systems has been the lack of technical standards to support interoperability and protect data and privacy. Many physicians, particularly those in small practices where most Americans get their health care, are hesitant to take on the considerable expense of a health IT system that without common standards may not work with the systems of a neighboring health care provider or may become prematurely obsolete.

This is the third hearing the Science and Technology Committee will have held on health IT standards since the 109th Congress. I am very eager to hear about the progress we have made on standards, especially since the implementation of the HITECH Act. In that Act, Congress included a directive to the federal agencies before us today to establish health IT standards and develop related measures to enable different manufacturers and vendors to produce software and other devices that will work with other products on the market today, as well as tomorrow.

Given the complexity of our healthcare system, with its myriad of players and large number of state and federal laws governing personal medical information, the HITECH Act charged the Office of the National Coordinator with a very difficult task. From all reports, the National Coordinator has done an admirable job meeting tight deadlines and navigating the needs of many stakeholders.

NIST has also played an important role, lending to HHS its extensive expertise in standards, testing, and certification.

However, as I am sure we will discuss today, we still have a long way to go in promoting interoperability, coordinating the many health IT projects underway, governing the standards development process and providing direction on privacy and security. Modernizing our health care system with information technology is imperative for lowering health care costs and improving patient care, and I look forward to hearing the thoughts and recommendations of the witnesses today on how we will successfully meet these challenges.

Chairman WU. Now I would like to recognize the Ranking Member, Mr. Smith, for his opening statement.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

Good morning. I would like to welcome everybody to today's hearing on healthcare information technology.

In the Internet age, most of us take for granted being able to rapidly and seamlessly share information with someone across town, in another state, or on the other side of the world. We also take for granted the ubiquitous integration of information technology in our workplace and in many other aspects of our daily lives.

In contrast, the health care industry is still surprisingly paper-based and largely unaided by information technology. Medical treatment in this country often involves state-of-the-art technology. However, physicians and other health care providers have been slow to adopt health IT systems and electronic health records—or EHRs—and are still keeping track of our medical information the same way they were 50 years ago.

The use of information technology has real-world implications for the cost and quality of health care. Currently, providers may order a duplicative test because previous test results from another provider are not readily at hand, or they may miss a harmful drug interaction because a patient's full prescription drug record is not available. According to most estimates, a fully interoperable health IT system could save us billions of dollars in health care costs each year. In addition, greater use of information technology could prevent some of the medical errors that, as reported by the National Academies, are responsible for the deaths of approximately 98,000 people each year.

A key barrier to broader integration of health IT systems has been the lack of technical standards to support interoperability and protect data and privacy. Many physicians, particularly those in small practices where most Americans get their health care, are hesitant to take on the considerable expense of a health IT system that, without common standards, may not work with the systems of a neighboring health care provider or may become prematurely obsolete.

This is the third hearing the Science and Technology Committee will have held on health IT standards since the 109th Congress. I am very eager to hear about the progress we have made on standards, especially since the implementation of the HITECH Act. In that act, Congress included a directive to the federal agencies before us today to establish health IT standards and develop related measures to enable different manufacturers and vendors to produce software and other devices that will work with other products on the market today, as well as tomorrow.

Given the complexity of our healthcare system, with its myriad of players and large number of state and federal laws governing personal medical information, the HITECH Act charged the Office of the National Coordinator with a very difficult task. From all reports, though, the National Coordinator has done an admirable job meeting tight deadlines and navigating the needs of many stakeholders. NIST has also played an important role, lending to HHS its extensive expertise in standards, testing, and certification.

However, as I am sure we will discuss today, we still have a ways to go in promoting interoperability, coordinating the many health IT projects underway, governing the standards development process, and providing direction on privacy and security. Modernizing our health care system with information technology is imperative for lowering health care costs and improving patient care, and I look forward to hearing the thoughts and recommendations of the witnesses today on how we will successfully meet these challenges.

Mr. SMITH. Thank you, Mr. Chairman, for calling today's hearing on development and implementation of standards and testing for interoperability of health information technology. With the enactment of the HITECH Act and other measures since our last full Committee hearing on this issue in September 2007, a follow-up hearing on this topic is certainly appropriate and appreciated.

Interoperability of health IT is vital to ensuring one of the greatest benefits of electronic medical records: the ability of multiple practitioners in different locations to access a patient's medical records. This access helps avoid adverse interactions, duplicative testing and other medical errors while improving coordination of care.

To maximize the potential of health IT, it is vital these benefits be available not just in a metropolitan area or a single state but across state lines. For example, in my own Congressional district, it is not uncommon for those in need of higher-level health care to seek it in Colorado, South Dakota, Kansas or Wyoming rather than from another in-state location such as the larger cities of Lincoln and Omaha. It is vital that electronic medical records be available both close to home and out of state.

For this reason, and among others, it is appropriate that NIST and other federal agencies play a role in developing interoperability standards and testing for such technologies. NIST in particular is a trusted arbiter of standards development and testing and has the proven expertise to assist the Department of Health and Human Services in developing testing methods to ensure technology is interoperable as promised.

Additionally, we must ensure interoperability standards protect private and taxpayer dollars from being wasted on technologies which are not proven to be interoperable—not as a barrier to future innovations, which could further improve the quality and coordination of patient care.

Thank you again, Mr. Chairman and witnesses. In particular, I would like to welcome our witness Deb Bass, who is Executive Director of the Nebraska Health Information Initiative based in Omaha. I look forward to a constructive session. Thank you.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Thank you, Chairman Wu, for calling today's hearing on the development and implementation of standards and testing for interoperability of health information technology. With the enactment of the HITECH Act and other measures since our last full committee hearing on this issue in September 2007, a follow-up hearing on this topic is indeed appropriate and appreciated.

Interoperability of health IT is vital to ensuring one of the greatest benefits of electronic medical records—the ability of multiple practitioners in different locations to access a patient's medical records. This access helps avoid adverse interactions, duplicative testing, and other medical errors while improving coordination of care.

To maximize the potential of health IT, it is vital these benefits be available not just in a metropolitan area or a single state, but across state lines. For example, in my own congressional district it is not uncommon for those in need of higher level care to seek it in Colorado, South Dakota, Kansas, or Wyoming, rather than from another in-state location such as Lincoln or Omaha. It is vital electronic medical records be available both close to home and out of state.

For this reason, among others, it is appropriate NIST and other federal agencies play a role in developing interoperability standards and testing for such technologies. NIST, in particular, is a trusted arbiter of standards development and testing, and has the proven expertise to assist the Department of Health and Human

Services in developing testing methods to ensure technology is interoperable as promised.

However, we must ensure interoperability standards protect private and taxpayer dollars from being wasted on technologies which are not proven to be interoperable—not as a barrier to future innovations which could further improve the quality and coordination of patient care.

Thank you again, Mr. Chairman and witnesses. In particular I'd like to welcome one of our witnesses, Deb Bass, who is Executive Director of the Nebraska Health Information Initiative, based in Omaha. I look forward to a constructive session.

Chairman WU. Thank you very much, Mr. Smith.

If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

And now it is my pleasure to introduce our witnesses. Dr. David Blumenthal is the National Coordinator for Health Information Technology at the Office of the National Coordinator for the United States Department of Health and Human Services. Ms. Kathleen M. Roberts is the Associate Director for Federal and Industrial Relations at the Information Technology Laboratory for the National Institutes of Standards and Technology. Ms. Joyce Sensmeier is the vice President of Informatics for the Healthcare Information and Management Systems Society. Dr. Dick Gibson is the President of the Oregon Health Network. Ms. Deven McGraw is the Director of the Health Privacy Project for the Center for Democracy and Technology. Ms. Deb Bass is the President and CEO of Bass and Associates.

You will each have five minutes for your spoken testimony. Your written testimony will be included in the record for the hearing. And when you all complete your testimony, we will begin with questions and each Member will have five minutes to question the panel. Dr. Blumenthal, please begin.

STATEMENT OF DAVID BLUMENTHAL, NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, OFFICE OF THE NATIONAL COORDINATOR, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Dr. BLUMENTHAL. Mr. Chairman, Ranking Member Smith, distinguished Subcommittee Members, thank you for the opportunity to testify today on behalf of the Department of Health and Human Services.

The HITECH Act represents an historic and unparalleled investment in health information technology. It lays the groundwork necessary to pursue the President's goals related to improved health care quality and efficiency and will help transform the way health care is both practiced and delivered.

We have made considerable progress in the relatively short time since the HITECH Act's passage. Our recent accomplishments include the establishment of two new federal advisory committees, the completion of three rulemakings together with the Centers for Medicare and Medicaid Services necessary to establish Meaningful Use, Stage 1, strengthening coordination throughout the Executive Branch on health information technology, and the responsible obligation of nearly all of the $2 billion that we were authorized to spend under the American Recovery and Reinvestment Act.

My remarks today will highlight progress that ONC has made thus far related to interoperability, privacy and security as well as our standards and priorities for future stages of Meaningful Use. Interoperability and privacy and security are themes that are present throughout the HITECH Act. Thus, many of our policy and programmatic efforts focus on those themes.

Established by the HITECH Act, the HIT Policy and Standards Committees both regularly issue recommendations on how best to fulfill our statutory responsibilities. Both committees include a diverse membership with representatives of various perspectives from both the public and private sectors. The Policy Committee's work on privacy and security exemplifies its major contribution, and I want to note that Ms. McGraw has been a major contributor through the Policy Committee to that work.

The privacy and security of electronic health information form the bedrock necessary to build trust. To ensure that we have timely privacy and security recommendations related to our HITECH programs, the HIT Policy Committee formed an interdisciplinary privacy and security Tiger Team of experts comprised of members from the HIT Policy and Standards Committees as well as from the National Committee on Vital and Health Statistics. The Tiger Team has already provided valuable guidance to ONC and HHS.

Like its sister committee, the HIT Standards Committee plays a critical role in guiding ONC. Since its inception, the HIT Standards Committee has issued recommendations to ONC on the standards and implementation specifications that should be considered to support Meaningful Use Stage 1 and the development and maintenance of specific vocabularies to improve interoperability.

With the advice of these committees and extensive external consultation, we completed last July three independent rulemakings that were necessary to implement Meaningful Use Stage 1. These rules cumulatively reflect over 2,000 public comments from stakeholders across the health care system.

The first rule was the EHR incentive program and defined Meaningful Use Stage 1. ONC and the Centers for Medicare and Medicaid Services worked collaboratively to strike a balance that reflected both the urgency of adopting EHR technology and the challenges that adoption will pose to health care providers. Our approach attempts to move the health system upward toward improved quality and effectiveness but at a speed that reflects both the capacities of providers who face multiple real-world challenges and the maturity of the technology itself.

The second rule defined EHR standards, implementation specifications, and certification criteria adopted by the Secretary to support Meaningful Use. The initial standard set several specific interoperability and security capabilities that certified EHR technology must incorporate including e-prescribing according to specific standards, exchanging standardized patient summary records, authenticating users, generating audit logs and encrypting health information according to standards specified by NIST.

In the third rule, ONC established a temporary certification process. We have now authorized three certification bodies. In developing our certification programs, we consulted extensively with our

colleagues at NIST, which has been an invaluable partner in all our efforts to implement the HITECH Act.

We anticipate that future stages of Meaningful Use will build on the foundation we have now established and will require progressively more rigorous electronic health information exchange requirements. In order to develop those requirements, we have again asked the HIT Policy Committee to make recommendations on what Meaningful Use stages 2 and 3 should encompass.

We anticipate that the Standards Committee will then begin to focus on the standards implementation specifications and certification criteria that will be necessary for future stages of Meaningful Use. We also expect the Standards Committee to issue recommendations that focus on strengthening security capabilities of EHR technologies and on standards for electronic health information exchange in support of meaningful use. Interoperability will be critical to our success in stages 2 and 3. We recognize that greater specificity with respect to standards is necessary to reach our goals and we will be working on adopting additional implementation specifications, achieving agreement on vocabulary and code sets for particular exchange purposes and comprehensive privacy and security capabilities for EHR technology.

ONC and CMS have accomplished a great deal up to now but much remains to be done. We look forward to working with the House and Science and Technology Committee on this important endeavor, and it has been my privilege to testify before you today and I look forward to answering any questions you may have.

[The prepared statement of Dr. Blumenthal follows:]

PREPARED STATEMENT OF DAVID BLUMENTHAL

Chairman Wu, Ranking Member Smith, distinguished Subcommittee members, thank you for the opportunity to submit testimony on behalf of the Department of Health and Human Services (HHS) on our progress and priorities related to interoperability and the security of electronic health records and health information technology (HIT) systems since the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

The HITECH Act represents an historic and unparalleled investment in HIT, lays the groundwork necessary to pursue the President's goals related to improved health care quality and efficiency, and will help transform the way health care is both practiced and delivered. The provisions of the HITECH Act are best understood not as investments in technology *per se*, but as efforts to improve the health of Americans and the performance of their health care system.

Interoperability and privacy and security are themes that are present throughout the HITECH Act. Consequently, many of our policy and programmatic efforts also focus on those themes. We have made remarkable progress in the relatively short time since the HITECH Act's passage. Our recent accomplishments include: the establishment of two new federal advisory committees, the HIT Policy Committee and HIT Standards Committee; the completion of the three rulemakings necessary to establish meaningful use Stage 1 for the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs; strengthened coordination throughout the Executive Branch on HIT; and the responsible obligation of nearly all of the $2 billion we were authorized under the American Recovery and Reinvestment Act of 2009 through the creation of several programs that will have a lasting impact on the HIT landscape. As we take stock of our successes and complete the challenges in front of us, we recognize that much work still remains in order to reach our goals for the future.

The first half of my testimony focuses on the progress that the Office of the National Coordinator for Health Information Technology (ONC) has made thus far related to interoperability and privacy and security, generally, while the second half discusses the work we are currently pursuing with respect to standards in order to support the latter stages of meaningful use.

Building on HITECH

The HIT Policy and Standards Committees

Established by the HITECH Act, the HIT Policy and HIT Standards Committees both contribute a great deal to our activities and regularly issue recommendations on how to best fulfill our responsibilities and implement the ambitious agenda set forth by the HITECH Act. Both Committees include a diverse membership, with representatives of various perspectives from both the public and private sectors. The HIT Standards Committee, for example, combines standards experts from the private sector with Federal government leaders from OSTP, NIST, DoD, VA, and CMS.[1]

As we continue to implement the HITECH Act, we are acutely aware that it is paramount to implement appropriate policies to keep electronic health information private and secure. Privacy and security form the bedrock necessary to build trust. Patients and providers must feel confident in the processes, policies, and standards in place related to HIT and the electronic exchange of health information. Thus, to ensure that we have timely privacy and security recommendations related to the HITECH programs for which we are responsible, the HIT Policy Committee formed an interdisciplinary "Privacy and Security Tiger Team" of experts comprised of members from both the HIT Policy and Standards Committees. Members from the National Committee on Vital and Health Statistics (NCVHS) also serve on the Tiger Team to ensure the efforts of these committees are coordinated.

Building on the work of the Tiger Team, the HIT Policy Committee has, in accordance with its mandate in the HITECH Act, recently submitted recommendations regarding data segmentation technologies to ONC, as well as recommendations on obtaining patient consent in various contexts. In upcoming months, the Tiger Team in coordination with the HIT Policy Committee will continue to prioritize and address additional privacy and security issues including: the privacy and security requirements for participants in health information exchange activities who are not subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules; credentialing assurance levels; individual access; transparency; security safeguards; and de-identified data.

Like its sister committee, the HIT Standards Committee plays a critical role in guiding ONC. In August 2009, and again in March 2010, it issued recommendations to ONC on the standards and implementation specifications that should be considered to support meaningful use Stage 1. It has also formed workgroups which focus on clinical operations, clinical quality, and implementation. Most recently, the HIT Standards Committee established a vocabulary task force under the clinical operations workgroup to address vocabulary subsets and value sets as facilitators and enablers of meaningful use. In April, 2010, the HIT Standards Committee made recommendations to ONC based on the work of the clinical operations workgroup and taskforce. These recommendations broadly addressed several areas related to the identification, development, review, testing, and maintenance of vocabularies, value sets, and code sets, as well as the establishment of an authoritative vocabulary infrastructure.

Finally, in response to their charge under Section 1561 of the Patient Protection and Affordable Care Act, the HIT Policy and Standards Committees recently made recommendations to ONC for the Secretary's consideration regarding interoperable and secure standards and protocols that facilitate enrollment of individuals in Federal and State health and human services programs. On September 17, the Secretary adopted this first set of recommendations and they were published on ONC's website.[2]

Meaningful Use Stage 1

This past July marked the completion of the three interdependent rulemakings that were necessary to implement "Meaningful Use Stage 1," the first stage of the Medicare and Medicaid EHR Incentive Programs. The first rulemaking establishes the requirements that eligible health care providers[3] will need to satisfy in order to qualify for incentive payments. The second specifies the technical capabilities and standards that certified EHR technology will need to include to support these health care providers. And the third creates the processes for EHR technology to be tested

---

[1] OSTP: Office of Science and Technology Policy; NIST: National Institute of Standards and Technology; DoD: Department of Defense; VA: Department of Veterans Affairs; CMS: Centers for Medicare & Medicaid Services

[2] *http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3161*

[3] "Eligible health care providers" is used to mean: "eligible professionals, eligible hospitals, and critical access hospitals"

and certified, thus providing confidence and assurance to eligible health care providers that the certified EHR technology they adopt will perform as expected. These rules, cumulatively, reflect over 2,000 public comments from stakeholders across the health care system, and illuminate the initial pathway to achieving an integrated and electronically connected health care system.

In developing the policies for meaningful use Stage 1, the ONC and CMS worked collaboratively to strike a balance that reflected both the urgency of adopting EHR technology to improve our health care system and the challenges that adoption will pose to health care providers. Our approach attempts to move the health system upward toward improved quality and effectiveness in health care, but at a speed that reflects both the capacities of providers who face a multitude of real-world challenges and the maturity of the technology itself.

In order to ensure that eligible health care providers can obtain EHR technology capable of assisting their achievement of meaningful use Stage 1, the Secretary adopted an initial set of standards, implementation specifications, and certification criteria for EHR technology (the Initial Set). Much like meaningful use Stage 1, the Initial Set creates a foundation from which we expect to continue to build in order to enhance the interoperability and security of EHR technology. The Initial Set specifies several interoperability and security capabilities that certified EHR technology must include in order to support meaningful use Stage 1. With respect to interoperability, it specifies that certified EHR technology must be capable of submitting information to public health agencies in standard formats, that specific standards must be used for electronic prescribing, and it specifies certain standards (content exchange and vocabulary) that must be used when patient summary records are exchanged and when patients are provided electronic copies of their health information. With respect to privacy and security, the Initial Set requires that certified EHR technology must be capable of automatically logging-off a user, access control, authentication, generating audit logs, checking the integrity of information that is electronically exchanged, and encrypting health information (according to standards specified by NIST).

To ensure proper incorporation and use of the adopted standards and implementation specifications EHR technology must be tested and certified according to the certification criteria adopted by the Secretary. In that regard, we issued, at the end of June, a final rule establishing the temporary certification program for health information technology that outlines how organizations can become ONC–Authorized Testing and Certification Bodies (ONC–ATCBs). Once authorized by the National Coordinator, the ONC–ATCBs will test and certify that EHR technology is compliant with the standards, implementation specifications, and certification criteria adopted by the Secretary. To date, three organizations have now been granted ONC–ATCB status by the National Coordinator. We are also working on a final rule for a permanent certification program that we expect to publish later this year and that will be fully operational in early 2012. We expect that this program will be more rigorous than the temporary certification program and will achieve greater incorporation of international standards and best practices through requirements such as accreditation and surveillance. In developing our proposals for both the temporary and permanent certification programs and, in accordance with the HITECH Act, we consulted extensively with our colleagues from NIST. During this time, we established an even closer working relationship with the experts at NIST and we anticipate continuing to work with them, as the certification programs mature. NIST has been an invaluable partner in all our efforts to implement the HITECH Act.

Strengthened Coordination

On a number of fronts, we have actively sought to strengthen coordination within the Executive branch on complementary activities where the use of adopted standards and implementation specifications may be appropriate. In this regard, the Federal HIT Task Force was created to facilitate implementation of the President's HIT agenda through better coordination among Federal agencies. As noted, under the aegis of this HIT Task Force, we are working with the President's Cybersecurity Coordinator, Mr. Howard Schmidt, to take full advantage of security lessons learned from other Federal programs. We are also supporting our colleagues at the Department of Defense and the Department of Veterans Affairs on their implementation of the Virtual Lifetime Electronic Record (VLER) project, and continuing our work with the Federal Health Architecture (FHA).

Additionally, ONC has maintained a close working relationship with HHS' Office for Civil Rights (OCR) and consulted with OCR as it developed the proposed modifications to the HIPAA Privacy, Security, and Enforcement Rules required by the HITECH Act to strengthen the privacy and security protections for health informa-

tion and to improve the workability and effectiveness of the HIPAA Rules. The proposed regulatory provisions would, among other things, expand individuals' rights to access their information and restrict certain disclosures of protected health information to health plans; extend the applicability of certain Privacy and Security Rules' requirements to the business associates of covered entities; establish new limitations on the use and disclosure of protected health information for marketing and fundraising purposes; and prohibit the sale of protected health information without patient authorization. This proposed rulemaking will strengthen the privacy and security of health information, and is an integral piece of the Administration's efforts to broaden the use of HIT in health care today.

HITECH Programs

Through implementing the new authorities provided by the HITECH Act, we have committed to fostering the support, collaboration, and ongoing learning that will mark our progress toward electronically connected, information-driven medical care. Several new programs will contribute to this progress, including:

- *The State Health Information Exchange Cooperative Agreement Program*—A grant program to support States or State Designated Entities in rapidly building capacity for exchanging health information across the health care system both within and across states.
- *The Beacon Community Program*—A grant program for communities to build and strengthen their HIT infrastructure and exchange capabilities. These communities will demonstrate the vision of a future where hospitals, clinicians, and patients are meaningful users of health IT, and together the community achieves measurable improvements in health care quality, safety, efficiency, and population health.
- *The Health IT Workforce Program*—A multi-pronged approach designed to support the education of HIT professionals, including new and expanded training programs, curriculum development, and competency testing.
- *The Strategic Health IT Advanced Research Projects (SHARP) Program*—A grant program to fund research focused on achieving breakthrough advances to address well-documented problems that have impeded adoption: 1) Security of Health Information Technology; 2) Patient-Centered Cognitive Support; 3) Healthcare Application and Network Platform Architectures; and, 4) Secondary Use of EHR Data.
- *The Health Information Technology Extension Program*—A grant program to establish Health Information Technology Regional Extension Centers to offer technical assistance, guidance, and information on best practices to support and accelerate health care providers' efforts to become meaningful users of EHRs.

Supporting Standards Needs beyond Meaningful Use Stage 1

We anticipate that future stages of meaningful use will build on the foundation we have now established and will require progressively more rigorous electronic health information exchange requirements. In order to develop those requirements, we have again asked the HIT Policy Committee to make recommendations on what meaningful use Stages 2 and 3 should encompass. The HIT Policy Committee and its Meaningful Use workgroup have received testimony and held numerous hearings on topics such as care coordination, patient/family engagement, and eliminating disparities in health care. This fall the Meaningful Use workgroup will be holding additional public meetings, and will be closely monitoring implementation of meaningful use Stage 1 to inform its recommendations to the HIT Policy Committee. As before, and in response to the meaningful use policy priorities identified by the HIT Policy Committee, we anticipate that the HIT Standards Committee will also begin to focus on the standards, implementation specifications, and certification criteria that will be necessary for future stages of meaningful use. We also expect the HIT Standards Committee to issue recommendations that focus on strengthening the security capabilities of EHR technology and on standards for electronic health information exchange in support of meaningful use.

In order to support future stages of meaningful use as well as our other initiatives, we determined that a comprehensive standards and interoperability framework was needed, and we are currently in the process of establishing that framework. The "Standards and Interoperability Framework" is intended to help us coordinate our standards development efforts, and to facilitate the development, adoption, and use of high-quality standards and implementation specifications. We believe by using the Standards and Interoperability Framework, we can develop and

maintain a well organized set of standards that can be reused across different use cases, and allow for greater coordination among public and industry stakeholders.

Interoperability will be critical to our success in Stages 2 and 3 of meaningful use. In the Initial Set, we adopted several standards for the electronic exchange of health information, but we recognize that greater specificity is necessary to reach our goals. In that respect we will be working on adopting additional implementation specifications; achieving agreement on vocabularies and code sets for particular exchange purposes; and comprehensive privacy and security capabilities for EHR technology.

Conclusion

The HITECH Act provides for an unprecedented amount of funding to improve the quality and efficiency of health care through HIT, and its historic investment will undoubtedly help transition our current antiquated, paper-dominated health care system into a high-performing 21st century health care system. With a nationwide infrastructure of HIT in place, that provides the capability of secure interoperable health information exchange through consensus built standards, patients, providers, and the public will experience the true value added for improving health care delivery. It is my privilege to testify before you today and I look forward to answering any questions you might have.

BIOGRAPHY FOR DAVID BLUMENTHAL

David Blumenthal, MD, MPP serves as the National Coordinator for Health Information Technology under President Barack Obama. In this role he is charged with building an interoperable, private and secure nationwide health information system and supporting the widespread, meaningful use of health IT.

Dr. Blumenthal received his undergraduate, medical, and public policy degrees from Harvard University and completed his residency in internal medicine at Massachusetts General Hospital. Prior to his appointment to the administration, Dr. Blumenthal was a practicing primary care physician; director, Institute for Health Policy; and the Samuel O. Thier Professor of Medicine and Professor of Health Policy at the Massachusetts General Hospital/Partners HealthCare System and Harvard Medical School.

Dr. Blumenthal is a renowned health services researcher and national authority on health IT adoption. With his colleagues from Harvard Medical School, he authored the seminal studies on the adoption and use of health information technology in the United States. He is the author of over 200 scholarly publications, including most recently, "Heart of Power: Health and Politics in the Oval Office," which tells the history of U.S. Presidents' involvement in health reform, from FDR through George W. Bush.

A member of the Institute of Medicine and a former board member and national correspondent for the New England Journal of Medicine, Dr. Blumenthal has held several leadership positions in medicine, government, and academia including Senior Vice President at Boston's Brigham and Women's Hospital; Executive Director of the Center for Health Policy and Management and Lecturer on Public Policy at the Kennedy School of Government; and as a professional staff member on Senator Edward Kennedy's Senate Subcommittee on Health and Scientific Research.

He was the founding chairman of AcademyHealth and served previously on the boards of the University of Chicago Health System and of the University of Pennsylvania Health System. He is recipient of the Distinguished Investigator Award from AcademyHealth, and a Doctor of Humane Letters from Rush University.

Chairman WU. Thank you very much, Dr. Blumenthal.

Ms. Roberts, please proceed.

STATEMENT OF KAMIE ROBERTS, ASSOCIATE DIRECTOR FOR FEDERAL AND INDUSTRIAL RELATIONS, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Ms. ROBERTS. Chairman Wu, Ranking Member Smith and Members of the Subcommittee, I am Kamie Roberts, Associate Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology. Thank for the opportunity to appear before you today to discuss our role in standards for health information technology.

Both the President and Congress have recognized that health IT is a national priority, and NIST expertise on standards and interoperability is key to the fulfillment of the goals of health IT, such as higher quality and more efficient care, seamless, secure and private movement of data between health care providers without compromise or loss of information, and fewer errors and redundant tests, to name a few.

Over its history, NIST has been successful in applying emerging IT standards in many national priority domains and leveraging collaborations with industry and other federal efforts. Health IT is no exception. NIST has been collaborating with industry and others to improve the health care information infrastructure since the 1990s.

I would like to quickly note that as with any standards effort in the United States, there are strengths and challenges in health IT standards activities. The health IT standards development effort in the United States is strengthened by the robust, open process in which public and private sector collaborations are addressing the end goal of interoperable EHRs and health IT systems. The many varied partners bring their own strengths to the deliberations. At the same time, with health IT as a national priority, many standards development organizations are working to provide the standards-based solutions needed, which can sometimes lead to conflicting, overlapping or redundant standards.

A further challenge is the need to accelerate standards to keep up with the fast pace of technology advances.

NIST plays a critical role by providing technical expertise early and throughout the standards development process by leveraging industry-led, consensus-based standards development and harmonization efforts. NIST is helping ensure that the requisite infrastructural standards, such as clinical information exchange and security are complete and unambiguous.

NIST testing activities, including developing test tools and associated testing infrastructure, reduce the cost to help develop IT systems, first, through the early use of testing, which can accelerate standards development efforts, and second, as vendors implement systems, test tools provided by NIST help ensure that standards are implemented correctly.

Under the temporary health IT certification program, testing organizations authorized by the Office of the National Coordinator will use the NIST tests to evaluate EHR software and systems so doctors' offices, hospitals and other health care providers have confidence in the systems that they purchase. In addition, NIST is advising ONC on the process by which testing organizations will be authorized to test and certify the EHR systems.

There is much to be done in the realm of health IT standards, so we have to set priorities. Current priority areas include security standards, usability standards, and medical device interoperability standards. NIST also advances other high-priority health IT standards as needed.

NIST is actively engaged with private industry, academia, and other federal agencies including our colleagues in the Networking and Information Technology Research and Development Committee in coordination of longer-term health IT standards activities to en-

sure that future technologies can be integrated into the nationwide health care infrastructure.

NIST has a diverse portfolio of activities supporting our Nation's health IT effort. With NIST's extensive experience and broad array of expertise, both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to achieve the goal of improving health care delivery through information technology.

Thank you for the opportunity to testify today on NIST's activities in health IT standards. I would be happy to answer any questions you may have.

[The prepared statement of Ms. Roberts follows:]

PREPARED STATEMENT OF KAMIE ROBERTS

Chairman Wu, Ranking Member Smith, and Members of the Subcommittee, I am Kamie Roberts, Associate Director of the Information Technology Laboratory at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in standards for health information technology (IT).

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

As health IT has become a top priority around the nation, it is clear that standards and interoperability are key to the fulfillment of the goals of health IT:

- higher quality and more efficient care;
- seamless, secure, and private movement of data between healthcare providers without compromise or loss of information;
- access to medical histories (including diagnoses, diagnostic tests, laboratory tests, and medication lists) at the point of care and in emergency settings;
- fewer errors and redundant tests;
- more efficient and effective reporting, including surveillance and quality monitoring; and
- quick detection of adverse drug reactions and epidemics.

NIST has been successful in applying emerging IT standards in many national priority domains and leveraging collaborations with industry and other federal efforts; health IT is no exception. NIST has been collaborating with industry and others to improve the healthcare information infrastructure since the 1990s. Our IT researchers have an internationally respected reputation for their knowledge, experience, and leadership. As in all NIST endeavors, we are highly recognized and respected for our neutrality. Since 2005, NIST has worked closely with the Department of Health and Human Services' Office of the National Coordinator for Health IT (HHS/ONC). The role of NIST was further articulated in the 2008–2012 Federal Health IT strategic plan and the American Recovery and Reinvestment Act (ARRA) to:

- Advance healthcare information enterprise integration through standards and testing
- Consult on updating the Federal Health IT Strategic Plan
- Consult on voluntary certification programs
- Consult on health IT implementation
- Provide pilot testing of standards and implementation specifications, as requested.

The health IT standards development effort is strengthened by the robust, open process in which private-public sector collaborations are addressing the end goal of interoperable electronic health records and health IT systems, where the various

partners participate according to their strengths. At the same time, with health IT as a national priority, many standards development organizations are working to provide the standards-based solutions needed, which can sometimes lead to overlapping or redundant standards. A further challenge is the need to accelerate standards to track the fast pace of technology advances. NIST recognizes this need and through close collaborations with the health IT community, priority areas are being identified and early use of testing is helping to accelerate the development of complete, unambiguous standards.

NIST Role in Health IT Standards

To accelerate health IT standards, NIST is providing technical expertise and leveraging industry-led, consensus-based standards development and harmonization efforts. NIST plays a critical role by participating early in the development process and by helping ensure that the requisite infrastructural standards (such as clinical information exchange, security, and usability) are complete and unambiguous. For example, NIST is collaborating with organizations including, Health Level Seven (HL7), IEEE, International Organization for Standardization (ISO), and Integrating the Healthcare Enterprise, to refine current standards and develop standards that are needed in the future, such as standards for the next stages of meaningful use criteria (in 2013 and 2015). NIST is also engaged with other Federal agencies that have responsibility for health IT standards.

NIST testing activities, including developing test tools and associated testing infrastructure, reduce the cost to develop health IT systems by providing developers with an innovative, flexible and virtual testbed to confirm that their systems can exchange clinical information with other systems. In addition, it is important that vendors test their implementation of standards-based health systems; without testing it is impossible to know if a standard is implemented correctly.

As a further extension of the NIST testing activities, NIST, in collaboration with HHS/ONC, is helping develop a program for the voluntary certification of health IT systems as being in compliance with applicable certification criteria to meet meaningful use, that is, performing specifically defined functions. This effort is two pronged: (1) develop the test procedures necessary to certify the systems, and (2) define the process by which testing organizations will be authorized to test and certify the Electronic Health Record (EHR) systems. To address the first prong, NIST published, in August 2010, a set of HHS/ONC-approved procedures for testing EHR systems. During the development of these test procedures, NIST collaborated with HHS/ONC to ensure that the relevant standards and certification criteria were consistent and effectively represented within the test procedures. The approved NIST-developed test procedures evaluate components of EHR systems such as their encryption, how they plot and display growth charts, and how they control access so that only authorized users can retrieve information.

Under the voluntary health IT certification program, testing organizations authorized by HHS/ONC will use the NIST test procedures to evaluate EHR software and systems so doctor's offices, hospitals and other healthcare providers have confidence in the systems they purchase. As defined in ARRA, the Federal government will provide Medicare and Medicaid incentive payments to healthcare providers who meaningfully use EHR systems which meet HHS/ONC certification standards and criteria.

In addition, NIST is advising HHS/ONC on the process by which testing organizations will be authorized to test and certify the EHR systems. This includes advising on all aspects of developing the temporary and permanent certification programs and collaborating with HHS/ONC during the implementation and operational phases of the certification programs. In addition, HHS/ONC has stated its intention to use NIST's National Voluntary Laboratory Accreditation Program (NVLAP) to perform the accreditation of testing laboratories under the permanent certification program.

Standards Priorities

Working in collaboration with relevant standards development organizations, Federal agencies, professional societies, and industry, NIST provides technical expertise to enable the acceleration of industry-led, consensus-based standards development and harmonization to help ensure a complete, unambiguous set of health IT standards for clinical information exchange functions such as finding patients, discovering patient information, retrieving patient information, sending patient information, and allowing information to be sent, such as lab test results. Current priority areas include security standards, usability standards, and medical device and terminology

standards. NIST also advances other high priority health IT standards as appropriate.

Security

To help safeguard health information, NIST is developing a harmonized set of security principles and guidelines for use in emerging secure health information exchanges. NIST developed a systematic approach that organizations can use to design the technical security architecture necessary for the secure exchange of health information. This approach applies common government and commercial practices to the health information exchange domain. Utilizing this approach will assist organizations in ensuring protection of health data is addressed throughout the system development life cycle, and that organizations apply these protection mechanisms in technologies to enable the exchange of health information. Other key activities in health IT security include:

- Using security automation specifications, NIST is working with HHS's Office of Civil Rights to develop baseline security configuration checklists and toolkits that will help implement and assess the effectiveness of technical and non-technical safeguards in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
- Conducting outreach and awareness on security challenges, threats, and safeguards including presentations at industry conferences, workshops, Federal Advisory Committee meetings, and other Federal agencies on the application of security standards and guidelines to support health IT implementations.

Usability

Usability is a critical factor in health IT systems and must be considered in future meaningful use criteria. Usability enables health IT systems that are safe, effective, and efficient. Building upon our foundational work in usability, NIST is performing cutting-edge research for usability standards within the healthcare domain. NIST is collaborating closely with industry, academia, and other government agencies, including HHS/ONC, , the Agency for Healthcare Research and Quality (AHRQ), the Food and Drug Administration (FDA), and the National Institutes of Health (NIH) to provide guidance in the development of health IT usability standards and measurements. To pursue these goals, in November 2009, NIST released a usability roadmap, designed to deliver specific, objective health IT usability standards and define rigorous testing methods to assess compliance. This summer, to further refine the roadmap, NIST co-sponsored a health IT usability workshop with HHS/ONC and AHRQ to prioritize, align, and coordinate short, medium, and long-term strategies to improve usability of EHR systems. To help carry out the work defined in the roadmap, a public-private multi-year program of research will develop a principled framework for measuring the usability of health IT systems, resulting in established usability and accessibility standards for systems to prevent critical errors and promote effective and efficient use by all end users (doctors, nurses, administrators, patients, and others). Closely related to usability, accessibility, if implemented in a well-defined way, has the potential to remove the barriers to using health IT systems for the 20% of our population who experience some form of disability. Promoting the use of accessibility standards on a voluntary basis will achieve a nationwide impact that is truly "welcoming" to all people.

Medical Device Interoperability Standards

Medical devices have the ability to communicate with many other devices of various makes, models, and modalities. Acute point-of-care settings, such as a patient's bedside, require each class of medical device to use the same terminology to seamlessly and reliably communicate physiological data. As EHR systems are adopted, it is important that data from medical devices be easily and fully integrated into a patient's EHR. NIST researchers are collaborating with medical device and EHR experts to develop point of care medical device and EHR standards that meet this need.

In addition, terminology standards are an important area of focus needed to facilitate device interoperability. Terminology standards provide the necessary means to enable interoperability of data. For example, different device manufacturers sometimes utilize different terminology within their devices. Based on this, interoperability between these devices or between a device and an EHR is impossible. NIST, in collaboration with ISO and IEEE, developed a system to enhance medical device interoperability through standard terminology mapping; this system is being used across the health IT enterprise.

Beyond Meaningful Use

NIST is actively engaged with private industry, academia, and other Federal agencies, including those in the Networking and Information Technology Research and Development (NITRD) community, in coordination of longer-term health IT standards development, research, and outreach activities. For example:

- There is an ever-growing need to provide remote and home healthcare for aging, underserved (e.g., rural), and chronically ill populations, which can be facilitated by leveraging existing and emerging health IT standards and testing. Telemedicine includes capabilities where wellness checkups and monitoring, diagnoses, and treatment can occur any place and any time.
- Pervasive healthcare explores the use of emerging technologies such as body sensors, implants, and medical equipment for routine monitoring of chronic conditions. Current research includes analyzing the impact of interference from such devices and exploring the potential of applying energy from human movement to power the devices.
- Standards and guidelines are required so that medical records can be retrieved regardless of the format and medium in which they were first created or stored. This preservation will allow doctors to create the medical records of children today, and enable access to those same medical records when those children are adults.
- Standards and terminologies need to be extended to accommodate changing technologies and advances in biomedical knowledge.
- Information needs to be retrieved from notes in EHRs where data is not formatted or structured. EHR systems contain a wealth of information in the notes on a patient's history, symptoms, reactions, etc. Research into the retrieval and analysis of this textual information based on specific search criteria will enable use of key data by the practitioner.
- Advances are needed in image quality for healthcare applications to help ensure, for example, that the colors viewed on a digital image by a medical practitioner are representative of the actual colors when viewed in person.

NIST activities and collaboration in areas such as these will ensure that future technologies can be integrated into the nationwide healthcare infrastructure. NIST's pilot projects and/or programs doing basic research in these emerging technologies have potential for immediate and big impact applications in healthcare. Using NIST core competencies to expand research in these areas is in direct support of the goals of health IT.

NIST has a diverse portfolio of activities supporting our nation's health IT effort. With NIST's extensive experience and broad array of expertise both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to achieving the goal of improving healthcare delivery through information technology.

Thank you for the opportunity to testify today on NIST's activities in health IT. I would be happy to answer any questions that you may have.

BIOGRAPHY FOR KAMIE ROBERTS

Kamie Roberts is the Associate Director for Federal and Industrial Relations of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST). As Associate Director, Roberts provides a focal point for interactions with industry, government and international communities in key ITL program areas. She is responsible for the management of technical and administrative staff serving the needs of the ITL and NIST management, including but not limited to coordination of NIST Health Information Technology strategy and telemedicine research activities, ITL strategic planning, and IT standards liaison.

During 2009, Roberts served as the Acting Division Chief of the Software and Systems Division in ITL. The division develops software testing tools and methods that improve quality, conformance to standards and correctness. The division also participates with industry in the development of forward-looking standards. Key focus areas include health information technology, software quality, computer forensics, voting systems and test method research.

From October 1996 to June 1998 and again from April 2002 to June 2006, Roberts served as the Acting Deputy Director of the Information Technology Laboratory. She was responsible for the day-to-day administration, financial, and personnel manage-

ment of the laboratory and assisted in the direction of the scientific and technical activities of the Laboratory divisions.

Roberts served in the Office of Enterprise Integration, ITL, NIST, coordinating Department of Commerce activities in the area of enterprise integration. Roberts also served as special assistant to the NIST Director in the Director's role as Chair of the Committee on Applications and Technology of the Administration's Information Infrastructure Task Force. Previously, Roberts was on detail as technical staff to the Director of NIST in the position of Program Analyst. Prior to December 1994, Roberts performed research in the areas of distributed systems, transaction processing, X.25 networking standards and integrated services digital network standards.

Roberts received a B.S. degree in Mathematics with a minor in Computer Science from Clarion University of Pennsylvania in 1986 and received a Masters Degree in Computer Science at George Washington University in 1998. Since 1986, she has been a Computer Scientist at the National Institute of Standards and Technology (NIST).

Last updated: 11/17/2010

Chairman WU. Thank you, Ms. Roberts.

Ms. Sensmeier, please proceed.

STATEMENT OF JOYCE SENSMEIER, VICE PRESIDENT, INFORMATICS, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY

Ms. SENSMEIER. Thank you, Chairman Wu, Ranking Member Smith and Subcommittee Members. My name is Joyce Sensmeier and I serve as Vice President of Informatics at HIMSS, where I oversee the clinical informatics, standards, interoperability, privacy and security initiatives for the Society. It is a pleasure to be with you today before the Subcommittee and alongside these distinguished panelists.

I present these comments on behalf of HIMSS, a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology and management systems for the betterment of health care. HIMSS represents more than 30,000 individual members of which two-thirds work in health care provider, governmental, and not-for-profit organizations. HIMSS also includes over 470 corporate members and more than 85 not-for-profit and provider organizations that share our mission. Supporting the adoption and meaningful use of health IT is a key focus for HIMSS membership, and as a nurse and a clinician with several decades of experience, I am deeply committed to improving patient safety and outcomes. It is in that vein that we have addressed the two questions posed by the Subcommittee.

The first question is related to the progress ONC has made since passage of the HITECH Act. Prior to passage of HITECH, and for many decades, standards development organizations used open, consensus-based, volunteer-driven processes working in silos developing health IT standards. With the passage of the HITECH Act, a new process for oversight of health IT standards has been implemented. While forward progress is being made, we would like to identify three specific areas of concern.

First, data transport and basic security are focus areas where selected standards are missing yet necessary for achieving interoperability. For example, until the recommended transport standards are identified, EHR vendors will be forced to support all available transport methods or risk developing software that may not meet future interoperability needs. This lack of guidance in the first

stage of Meaningful Use and the standards criteria creates marketplace confusion and wastes existing resources, ultimately delaying progress.

Second, we would like to express concern regarding the selection of multiple standards for the same criterion such as the selection of two clinical summary standards, CCR [Continuity of Care Record] and CCD [Continuity of Care Document]. When two standards are selected, vendors and providers must choose to either support one or instead support both, which is costly, resource-intensive and minimizes health information exchange across organizations. It is our recommendation that only one standard be selected for each criterion in futures Stages of Meaningful Use.

Our third area of concern is the timing of identifying and selecting the standards in subsequent rules. Timing is critical to ensure the industry can appropriately incorporate these standards into the product development and implementation cycle. Thousands of EHR systems are currently being developed and upgraded by vendors and implemented by health care providers. To ensure optimal software development and testing and safe implementation, the final rules for Meaningful Use and standards should be available 18 months before the next stage.

The second question relates to the strengths and weaknesses of the current health IT standards identification and development process. HIMSS was pleased that the final rule established standards criteria for supporting stage 1 of Meaningful Use and specifically that structured lab test results and appropriate implementation guidance were added. HIMSS urges CMS, ONC and NIST to ensure that all contractual engagements in the standards harmonization are coordinated and leverage the public domain work products of standards harmonization bodies such as HITSP [HIT Standards Panel] and Integrating the Healthcare Enterprise, IHE. We also request that they complement rather than duplicate each agency's efforts when creating testing procedures, tools, services and reference implementations and that they embrace a transparent and open consensus process with the private sector.

We also recommend that HHS publish implementation guidance for all selected standards, publish standards for data transport, financial transactions, security and health information exchange as soon as possible, publish the process and schedule for harmonizing standards, and set up one repository such as the National Library of Medicine for licensure and access to all standards and implementation guides. HIMSS is pleased to see these final rules being implemented in order to put into action the legislative and Executive Branch intent to transform health care using IT.

I thank you for this opportunity, and I would be happy to answer questions, and we look forward to providing our members' expertise to help transform health care in the United States.

[The prepared statement of Ms. Sensmeier follows:]

PREPARED STATEMENT OF JOYCE SENSMEIER

Good morning. My name is Joyce Sensmeier and I serve as Vice President of Informatics for HIMSS, where I oversee the clinical informatics, standards, interoperability, privacy and security initiatives for the Society. It is a pleasure to be with you today before this Subcommittee and alongside these distinguished panelists.

Background

I present these comments today on behalf of HIMSS, a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded 50 years ago, HIMSS and its related organizations have offices in Chicago, Washington, DC, Brussels, Singapore, Leipzig, and other locations across the U.S. HIMSS represents more than 30,000 individual members, of which two-thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 470 corporate members and more than 85 not-for-profit organizations that share our mission of transforming healthcare through the effective use of IT and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, and research initiatives designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care.

I have been deeply involved in the harmonization and adoption of health IT standards during my decade at HIMSS. With co-sponsor, the Radiological Society of North America, I led HIMSS' effort to develop and manage Integrating the Healthcare Enterprise (IHE), a global initiative that drives the adoption of health IT standards for clinical needs. I also led HIMSS' involvement with the Healthcare Information Technology Standards Panel, or HITSP, a federal standards harmonization initiative, while also collaborating with another organization to form the Alliance for Nursing Informatics, a collaboration of 27 distinct nursing informatics organizations that I co-chair.

I became Board Certified in Nursing Informatics in 1996, and am an adjunct faculty member at Johns Hopkins University in Baltimore. This year, I am honored to be recognized as a Fellow of the American Academy of Nursing, a credential held by more than 1,600 nursing leaders throughout the world.

On behalf of HIMSS members, we commend Congress and President Barack Obama for their vision and commitment to transform our national healthcare delivery system through the use of IT.

HIMSS and HITECH

I was asked to come before the Subcommittee today to share HIMSS perspective on the progress of federal efforts in the standards arena to support the first stage of Meaningful Use. in this testimony, we will aim to address the specific questions posed by the Subcommittee.

The American Recovery and Reinvestment Act of 2009 (ARRA) includes billions of dollars in Medicare and Medicaid incentive payments to providers and hospitals for the "Meaningful Use" of certified health IT products, which are addressed in the Health Information Technology for Economic and Clinical Health (HITECH) Act portion of the statute. The HITECH Act requires the Department of Health and Human Services (HHS) to take regulatory action in several areas, including electronic health record (EHR) incentives for eligible professionals and hospitals (Meaningful Use), standards and certification criteria, a Certification Program, and privacy and security.

The HITECH Act also requires the Secretary of HHS to establish certification criteria and standards for achieving Meaningful Use. HHS and the Office of the National Coordinator for Health Information Technology (ONC) established a Final Rule on the Standards, Implementation Specifications, and Certification Criteria that are being used to support Meaningful Use for the start of the incentive payment programs in 2011.

The HHS/ONC Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Interim Final Rule were published in the *Federal Register* in January 2010. After receiving more than 400 responses from HIMSS and other organizations, ONC released its Final Rule on July 28, which included the resolution of technical challenges related to some of the standards and implementation specifications. The Final Rule went into effect on August 27, 2010.

Response to Subcommittee Questions

Supporting the adoption and Meaningful Use of health IT is a key focus for the HIMSS membership. It is in that vein that we have addressed the questions posed by the Subcommittee. We were asked by this Subcommittee to particularly address two issues, the first of which is:

"What progress has ONC made since the passage of the HITECH Act in meeting the need for interoperability and information security standards for electronic health records and health IT systems?"

Prior to the passage of the HITECH Act, and for many decades, standards development organizations (SDOs) used an open, consensus-based, volunteer-driven process, working in silos to develop health IT standards. While this is important work that is being leveraged by healthcare entities today, each SDO has its own priorities, goals and objectives. As a result, while many standards are available, there are multiple gaps, redundant efforts, and limited adoption in live health IT systems.

Also, standards are often not implemented consistently enough across individual organizations or products to enable interoperability. By necessity, hospitals and clinical practices invent one-off integration "solutions" when implementing IT products, which is a major impediment to interoperability. Implementation guides or specifications are also necessary to ensure that standards are implemented in the same manner to allow multiple systems to share data. These implementation specifications are typically developed by SDOs, such as Health Level 7 (HL7) or SNOMED, and standards-profiling organizations, such as IHE.

Prior to enactment of the HITECH Act, U.S. health information exchange priorities were set by the American Health Information Community (AHIC), the Federal Advisory Committee established by HHS. These priority use cases were given to HITSP through a $22-million, five-year contract awarded to the American National Standards Institute (ANSI), which was funded by HHS and managed by ONC. In an open, consensus-based process involving 966 member organizations and more than 900 volunteer stakeholders, HITSP technical committees selected and harmonized standards to address the interoperability of the use cases. This stakeholder engagement was widespread across both federal and private sectors, and a number of the HITSP specifications, which are available in the public domain, are in the process of being tested and implemented. During its tenure, HITSP developed over 130 interoperability specifications that were subsequently accepted, recognized, and/or adopted by HHS.

With the passage of the HITECH Act, a new process for oversight of the health IT standards process has been implemented. During this transition period, a degree of momentum in the advancement, harmonization and implementation of health IT standards has been lost. The healthcare community was previously aligning with the HITSP process, and vendors and health information exchanges were adopting its recommended standards and specifications. Today, the HIT Standards Committee determines priorities and recommends standards to support the Meaningful Use criteria. While the Committee's efforts are not overtly based on an open, consensus-based process, it has designated task forces and work groups to execute specific tasks, and these groups invite testimony to incorporate feedback from the healthcare community. The regulatory process stemming from the HITECH Act includes designated comment periods to accommodate public feedback, which allows "real world" experience and subject matter expertise to inform the final regulations. Compliance with the standards identified in the Standards and Meaningful Use final rules will be verified by the National Institute of Standards and Technology (NIST) testing procedures and the EHR certification process.

These inputs have informed the Standards, Implementation Specifications and Certification Criteria, as well as the Stage 1 Meaningful Use final rules, which incorporate a beginning set of standards and several implementation guides to enable interoperability. Leveraging the open, consensus-based work products of HITSP and using implementation guides from standards profilers such as IHE is essential for quickly, efficiently and cost effectively advancing health IT efforts to allow providers to realize the incentives. This type of reuse was accomplished with selection of HITSP/C32 as the implementation specification for the Continuity of Care Document (CCD) and the Continuity of Care Record (CCR) clinical summary content standards for Stage 1 Meaningful Use, and thus, is a positive example of leveraging previous work and ensuring the interoperability of those standards when implemented. However, there are significant gaps in standards for interoperability in Stage 1 Meaningful Use.

We would like to identify three specific areas of concern regarding standards selection for Stage 1 Meaningful Use. First, data transport and basic security are focus areas where selected standards are missing, yet necessary for achieving interoperability. We understand that Stage 1 is not intended to force interoperability on a healthcare community that is not technically ready to meet the requirement. However, identifying the accepted transportation method will have a dramatic impact on preparedness for Stage 2. For example, it is important to designate standards for documenting the content of clinical summaries, but if we don't know how to trans-

mit these summaries or acknowledge their receipt, we will have limited interoperability. Until the recommended transport standards are identified, EHR vendors will be forced to support all available transport methods or risk developing software that may not meet future interoperability needs. This lack of guidance creates marketplace confusion and wastes existing resources, ultimately delaying progress.

Second, we would like to express concern regarding the selection of multiple standards for the same criterion, such as selection of two clinical summary content standards—CCR and CCD. When two standards are selected, vendors and providers have to choose to support one standard, or instead, support both, which is very costly, resource intensive, and minimizes interoperability capabilities across organizations. It is our recommendation that only one standard is selected for each criterion in future stages of Meaningful Use.

Our third area of concern is the timing of identifying and publishing the selected standards in subsequent rules, which is critical to ensure that the industry can appropriately incorporate the standards into the product development and implementation cycle. Thousands of EHR systems are currently being developed and upgraded by vendors and implemented by healthcare providers. Recent statistics show that sales of hospital EHR systems nearly doubled from 2008 to 2009.[i] To ensure optimal software development, testing, and safe implementation by providers, the final rules for Meaningful Use and certification criteria should be available 18 months before the next stage of Meaningful Use commences.

ONC has published a Standards and Interoperability Framework and has recently completed the long-awaited contracting process for promoting interoperability and Meaningful Use. The goal of this framework is to create a collaborative, coordinated, incremental standards process that is led by the industry in solving real-world problems. The selected contractors will each be working to complete specific components of the framework, including use case development, standards harmonization, implementation specifications, tools and services. It is ONC's stated intent to leverage the health IT community, professional organizations, government agencies and standards organizations to ensure that all of their work comes down to a harmonized set of standards and implementation specifications. It is essential that ONC and its contractors deliver on this promise, and use an open, transparent, coordinated process to engage the community and leverage their collective efforts in order to maximize industry involvement and "buy in" to the effort.

Going forward, a centralized and coordinated process is needed for engaging SDOs and harmonization organizations, such as IHE, in meeting the needs for interoperability and information security standards for EHRs. While government can be an enabler for this standards coordination process, a neutral and uniform approach is necessary to ensure that the principles of transparency, openness, stakeholder representation, healthcare leadership, industry engagement, impartiality and balance, due process, consensus, relevance, and effectiveness are maintained. A timely evaluation of the optimal process for standards coordination is needed to address this urgent and important need.

In this testimony, we have previously suggested that the open, consensus-based and public domain work products of HITSP and IHE should be leveraged to quickly, efficiently and cost effectively advance standards for health IT. To this end, IHE is a global non-profit entity that has, over the past decade, developed a framework for standards-based interoperability of health IT systems that is being adopted and implemented worldwide. Each IHE integration "profile" describes a clinical requirement for systems integration and outlines a standards-based solution to address it. IHE profiles address critical interoperability issues related to information access for care providers and patients, clinical workflow, security, administration, transport and information infrastructure. IHE profile development includes multiple opportunities for public comment review and feedback. Vendors that implement IHE specifications participate in annual testing events hosted in a structured and supervised environment, to ensure compliance, and publish integration statements for their IHE-compliant products prior to real-world implementation.

A number of THE transport profiles, such as Cross Community Access (XCA), support the exchange of health information and documents across communities and are being implemented in the Nationwide Health Information Network and various regional health information exchanges in the U.S. and worldwide. Reuse of these profiles in the U.S. standards identification and development process will build on a foundation of proven implementation guides that will accelerate standards adoption and save valuable time and resources.

The second issue that we were asked to address is:

"What are the strengths and weaknesses of the current health IT standards identification and development process, and what should the top standards-related priorities be for future health IT activities?"

HIMSS was pleased that the Final Rule established standards criteria for supporting Stage 1 of Meaningful Use including:

- Removal of All or Nothing
- General relaxation of the requirements, specifically, implementation of drug-drug and drug-allergy interaction checks
- Maintenance of an active medication list
- Addition of structured lab test results
- Removal of LOINC code requirement
- Removal of requirement to submit electronically in Stage 1
- Change to a core and menu objectives approach
- Addition of a requirement to generate patient lists by specific conditions
- Expanded clinical quality reporting measures
- Moved requirements to check insurance eligibility and submit claims to Stage 2
- Added guidance to expand capability to submit electronic syndromic surveillance data to public health agencies
- Clarified numerous privacy and security criteria
- Moved more aggressive requirements to Stage 2
- Added appropriate implementation guidance

As discussed previously, we were disappointed that HHS did not further leverage HITSP and other harmonization work, such as IHE. Millions in federal taxpayer dollars and thousands of volunteer hours by committed subject matter experts were expended on harmonization efforts. Recognizing this work would have accelerated Meaningful Use adoption. HIMSS urges the Centers for Medicare and Medicaid Services (CMS), ONC and NIST to ensure that all contractual engagements for standards harmonization and coordination efforts:

- Incorporate HITSP and IHE work products and test tools
- Complement (versus duplicate) each agency's efforts when creating testing procedures, testing tools & services, and reference implementations
- Embrace transparent and open consensus processes with the private sector

The HITECH Act set the vision for transforming the healthcare setting and these final rules are key components in implementing that vision. To achieve HITECH's vision, we recommend that HHS address the following:

- Publish implementation guidance (such as IHE and HITSP interoperability specifications) for all selected standards
- Publish data transport, financial transactions, security and health information exchange standards as soon as possible
- Publish the process and schedule for harmonizing standards and developing implementation specifications
- Set up one repository (such as the National Library of Medicine) for licensure and access to all standards and implementation guides
- Publish, as soon as possible, federal health IT best practices guidelines

Finally, HIMSS urges HHS to publish criteria pertaining to Stage 2 Meaningful Use at least 18 months before the beginning of Stage 2. This will enable sufficient time to develop, test, and deploy software conforming to these standards and implementation guides so that all eligible users can become meaningful users. Beyond the specific concerns associated with the Standards, Implementation Specifications, and Certification Criteria for Meaningful Use Stage 1, HIMSS is concerned that Meaningful Use and interoperability will be hindered without addressing two key areas, a patient identity solution and security of personal health information.

In response to this question, I would also like to highlight an important work product of one of HIMSS' many multi-stakeholder member workgroups—the Patient Identity Integrity Workgroup. Last year, this workgroup published a landmark white paper describing the challenges and costly efforts healthcare organizations face every day in their efforts to ensure the integrity (accuracy and completeness) of data attached to or associated with an individual patient, including the correct

pairing or linking of all existing records for that individual within and across information systems.

Obviously, patient identity integrity is of central importance to achieving quality of care, patient safety, and cost control. In addition, the primary goal for nationwide health information exchange is to allow authorized users to quickly and accurately exchange health information in an effort to enhance patient safety and improve efficiency. Achieving this goal is dependent on the ability to link or match multiple, disparate records relating to a single individual.

This white paper describes nine key influencers for improving data integrity in this area. One key influencer listed is the need for standards for patient identification data and format, and another has to do with the need for a study of the current technical solutions available to uniquely identify a patient. Using the results from the study, we can anticipate the exponential exacerbation of problems and errors with patient data matching in the health information exchange environment and evaluate potential solutions. We can do this by having *current* data on available technical capabilities as we formulate an "informed patient identity solution," a position discussed in the white paper and endorsed by the HIMSS Board of Directors.

Finally, I would like to highlight an annual HIMSS Security Survey that examines in-depth information from healthcare organizations regarding security implementation practices and technology uses. The HIMSS Security Survey, now in its third year, analyzes the responses of IT and security professionals from healthcare provider organizations across the U.S. regarding the policies, processes and tools in place at healthcare organizations to secure electronic patient data. The study covers a multitude of topics regarding organizations' general security environment, including access to patient data, access tracking, and audit logs, use of security in a networked environment and medical identity theft.

Last year, we probed our respondents with regard to their preparedness and approach for meeting new privacy and security requirements contained in ARRA, and we were privileged to provide testimony to the HIT Standards Committee as to the results and trends uncovered in this study.[ii] This year, we have partnered with the Medical Group Management Association (MGMA) to include an even larger population of ambulatory and medical group practices. The results of this year's study will be available in early November, and we would be happy to provide those results to the Subcommittee.

Closing

HIMSS is pleased to see these final federal rules and the ONC Standards and Interoperability Framework and related contracts being implemented in order to put into action legislative and executive branch intent to transform healthcare using IT. Through our robust member structure, we will continue to evolve our positions to reflect the current needs of health IT professionals to improve healthcare quality, safety, efficiency, and access for all. HIMSS believes that by linking credible health IT principles emanating from our members' needs and experiences, we will help our nation successfully transform healthcare using effective IT.

Celebrating our 50-year history of serving the healthcare community, HIMSS remains deeply committed to working with federal and state leaders in a bipartisan manner to improve the quality, safety, and efficiency of healthcare for all through the appropriate use of IT and management systems. HIMSS members appreciate and understand the cultural and technical challenges that healthcare providers face in meeting the requirements for Meaningful Use.

In closing, I'd like to highlight a few health IT initiatives within HIMSS that aim to recognize best practices in the use of health IT and measure the level of EHR adoption throughout the U.S. These initiatives will be critical reference points in evaluating the success of the HITECH Act in transforming the way we do healthcare. To recognize healthcare's excellence in using IT to improve access, safety, quality and efficiency, the HIMSS Nicholas E. Davies Awards of Excellence[iii] recognizes management, functionality, technology and value—the pillars of health IT success. Objectives of the Davies program include promoting the vision of EHR systems through concrete examples; understanding and sharing documented value of EHR systems; providing visibility and recognition for high-impact EHR systems; and sharing successful EHR implementation strategies.

The awards focus on four healthcare settings: organizations, ambulatory sites, public health, and community health organizations. Since 1994, the Davies program has honored 71 healthcare organizations, private practices, public health systems, and community health organizations that have implemented health IT, specifically EHRs, in their respective locations. I invite members of the Subcommittee to visit HIMSS' State HIT Dashboard[iv] to locate Davies winners in or near your Districts. Mr. Chairman, I'm pleased to report that there are two Davies winners in your

home state of Oregon: Kaiser Permanente Northwest in Portland,[v] and the Indian Health Service in Warm Springs.[vi]

Next, I would like to highlight the HIMSS Analytics' EMR Adoption Model℠ (EMRAM).[vii] Knowing the baseline of current adoption of health IT is critical to understanding the realities at U.S. hospitals and the federal government's EHR adoption goals. According to quarterly health IT implementation census data from HIMSS Analytics, the use of health IT among healthcare providers has steadily increased over the past four years.

Using a census survey, HIMSS Analytics' EMRAM tracks adoption of EMR applications within all 5,217 U.S. civilian hospitals and health systems and scores hospitals based on their progress towards meeting the criteria for various stages within the Model. There are eight stages for hospitals, ranging from 0 to 7, as they move to a completely electronic environment (Stage 7); at the pinnacle of the model, paper charts are no longer used in the delivery of patient care.

As of June 2010 [viii]:

- 16.3 percent of U.S. hospitals (850 of 5,217) have achieved "Stage 4" or higher of the Adoption Model. This is up from 3.7 percent in December 2006.
- Another 50.2 percent of U.S. hospitals (2,621 of 5,217) have achieved "Stage 3."

As it has for the past six years, HIMSS Analytics will continue to gather data and release quarterly updates of its census-based survey, shedding light on EHR adoption levels.

Driving the appropriate use of health IT will improve patient safety and the quality, accessibility, and cost-effectiveness of healthcare. Thanks to our informed and committed member volunteers, HIMSS will be a leader in the transformation. HIMSS looks forward to working with the legislative and executive branches in helping to ensure that the components of the HITECH Act are appropriately implemented. HIMSS actively equips its members with the knowledge and tools they need to successfully navigate these regulations, including FAQs, white papers, and educational webinars.[ix]

Again, it was a pleasure to be with you today before this Subcommittee and alongside these distinguished panelists. I would be happy to answer questions that members of the Subcommittee may have and look forward to providing our members' expertise to help you transform healthcare in the U.S. Thank you for this opportunity.

[i] *CIS Purchase Decisions: Riding the ARRA Wave. Klas. August 2010. Available at*: *http://www.klasresearch.com/Store/ReportDetail.aspx?ProductID=589*
[ii] *http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf*
[iii] *http://www.himss.org/davies*
[iv] *http://www.himss.org/statedashboard*
[v] *http://www.himss.org/davies/pastRecipients—org.asp*
[vi] *http://www.himss.org/davies/pastRecipients—ph.asp*
[vii] *http://www.himssanalytics.org/hc—providers/emr—adoption.as*p
[viii] *http://www.himssanalytics.org/stagesGraph.html*
[ix] *http://www.himss.org/economicstimulus*

BIOGRAPHY FOR JOYCE SENSMEIER

Joyce Sensmeier is Vice President of Informatics for HIMSS, the largest U.S. not-for-profit healthcare association focused on providing global leadership for the optimal use of information technology. HIMSS represents more than 31,000 individual members, 470 corporate members and 30 not-for-profit organizations that share its cause-based mission.

Sensmeier joined HIMSS as the Director of Professional Services in 2000. In her current role she is responsible for the areas of clinical informatics, standards, interoperability, privacy and security. Sensmeier became Board Certified in Nursing Informatics in 1996, earned the Certified Professional in Healthcare Information and Management Systems in 2002, and achieved HIMSS fellowship status in 2005. She is an adjunct faculty member in the School of Nursing at Johns Hopkins University in Baltimore. She previously served at Palos Community Hospital in Palos Heights, Illinois as a nursing coordinator leading clinical information system implementations.

Sensmeier has made contributions to enabling health information exchange through standards profiling and harmonization initiatives. She led advancement of Integrating the Healthcare Enterprise (IHE), an international standards profiling organization which, over the past decade, has achieved both regional and international adoption of its public domain technical framework. She is President of IHE USA, and previously served as the Standards Implementation Technical Manager for the Healthcare Information Technology Standards Panel (HITSP).

An internationally recognized speaker and author of multiple book chapters, articles and white papers, Sensmeier was recognized in 2010 as a fellow with the American Academy of Nursing, a credential held by 1,600 nursing leaders throughout the world. She is co-founder and co-chair of the Alliance for Nursing Informatics, a collaboration of 27 distinct nursing informatics organizations that represents a unified voice for nursing informatics professionals.

Sensmeier received a BSN from Elmhurst College and a Masters degree in Nursing Administration from St. Xavier University, both in Illinois.

Chairman WU. Thank you.

Dr. Gibson, please proceed.

STATEMENT OF RICHARD GIBSON, PRESIDENT, OREGON HEALTH NETWORK

Dr. GIBSON. Chairman Wu, Ranking Member Smith, good morning and thank you for the opportunity to discuss health information technology standards. My name is Richard Gibson. I am a practicing family physician and former emergency physician and have nearly 20 years of experience in health information technology.

On the status of current standards, the Meaningful Use final rule has been well received by providers. We applaud the Office of the National Coordinator and the Centers for Medicare and Med-

icaid Services for seriously considering the many comments received over the past nine months. They have been extraordinarily responsive in making rules as straightforward and as pragmatic as possible while still moving the country forward to electronic health records that promise to improve the quality and consistency of health care.

Concerning the standards-related priorities for the future, my comments will go to the area of helping small practices in the short term to connect to each other directly while we await the more complete and widespread health information exchange.

We need a standard for transmitting provider text notes. Providers expect to be able to review the text reports produced by other providers. Historically, these text reports have been produced by transcribing notes that physicians dictated, say, for an office visit, a consultation note, a surgical procedure and the like. We need a specific continuity-of-care document or continuity-of-care record for these text documents to be most useful for patient care.

We need a standard for exporting and importing patient information directly between EHRs and directly provider to provider. Meaningful Use stage 1 does not require EHRs to have the ability to export and import patient information directly to and from other EHRs. As clinicians move to electronic health records, we need to enable our EHRs to transfer patient information as easily as fax machines accomplish that transfer now. The office staff needs to be able to press a button to send information to the next physician. This concept and the next two have been promulgated by Wes Rishel at Gartner and have led to the NHIN [Nationwide Health Information Network] Direct Project.

We need a standard directory for health Internet addresses. After a provider decides to refer the patient to another physician, the provider or her staff member could go onto the Internet and search for the provider's authenticated health Internet address. This could be entered into the sending physician's electronic health record, which would send an encrypted packet of information directly to the receiving physician's electronic health record. Later, states will need a record locator service so that emergency departments can pull data from the patient's previous providers.

We need a standard for document transfer that can accommodate providers still on paper records. It will be years before all providers have electronic health records. We need a standard that sends patient information like an e-mail attachment so that providers on paper records can still print the information. Once they do get an EHR, the same attachment could be imported into that EHR.

We need an EHR functionality requirement for quality measure reporting. Smaller practices under the current rules would likely need to seek the help of consultants to produce an acceptable quality measures report. This reporting needs to be a core EHR function specified by a consistent nationwide requirement so that providers in any practice can again press a button to produce submission-ready reports on a chosen measure.

We need a national model for privacy and patient consent. In Portland, we often see patients from southwest Washington. Having significantly different privacy laws between Washington and Oregon would lead to uncertainty, missed information and the un-

necessary duplication of diagnostic testing. We need a federal effort to convene, sponsor, and mandate development of model rules and laws that each state could take through its own legislative process. We need to set appropriate expectations on provider access controls to patient information. In our largely fee-for-service health care system, one cannot exactly predict which doctor or nurse may take care of them on any given occasion. Our model needs to set the expectation in the patient's mind that it is not possible to predict precisely who will need access to their record in the course of their care.

Finally, we need a model for the complete health record being available to the provider. Although the provider can infer some of the patient's diagnoses from a medication list and allergy list alone, it is crucial that providers see all the medications and allergies when they prescribe. Without this guarantee, patients could be hurt. Similarly, providers need access to the full laboratory and imaging reports when they are trying to make a diagnosis. Redacting these data because they imply a certain restricted diagnosis is unsafe and could ultimately result in physical harm to the patient.

Chairman Wu and Ranking Member Smith, thank you for the opportunity to testify on these important issues. I would be happy to answer any questions you may have.

[The prepared statement of Dr. Gibson follows:]

PREPARED STATEMENT OF RICHARD GIBSON

Chairman Wu and Members of the Subcommittee, good morning and thank you for the opportunity to discuss health information technology standards, current status and future needs. My name is Richard Gibson. I am President of Oregon Health Network. I am a practicing, board-certified family physician, and a former board-certified emergency physician. I have nearly 20 years' experience in health information technology, including working with several major hospital systems and Oregon health information exchange planning efforts.

SUMMARY OF RECOMMENDATIONS

During my testimony I will offer my opinion on the current status of recent standards, discuss challenges to EHR adoption, and make the case for the following new national standards:

- A standard for transmitting provider text notes.
- A standard for exporting and importing patient information directly between EHRs and directly provider-to-provider.
- A standard directory for Health Internet Addresses.
- A standard for document transfer that can accommodate providers on paper records.
- A standard EHR functionality requirement for quality measure reporting.
- A national model for privacy and patient consent, access control, and availability of the entire health record.

STATUS OF CURRENT STANDARDS

Meaningful Use Final Rules Are Well Received

The delivery of the Final Rule on the CMS EHR incentive program has been well received by the provider community. As far as Stage l of the Meaningful Use objectives and measures, the uncertainty is now over. This is been enormously helpful to providers. We applaud the consideration that the Office of the National Coordinator and CMS have shown to the many comments received over the past six months. This office has been extraordinarily responsive in making rules as straightforward and pragmatic as possible while still moving the country forward to electronic health records that actually improve the quality and consistency of healthcare. We very much appreciate the obvious collaboration between the Office

of the National Coordinator and the Centers for Medicare and Medicaid Services and would encourage continued coordination among all federal agencies working in health information technology to achieve the needed improvement goals in public health, mental health, and long term care through health information exchange.

In particular, the use of Core Requirements and Menu Set Requirements for Meaningful Use, in place of the "all or nothing" approach was very helpful in giving providers and EHR vendors some flexibility in meeting Stage 1 Meaningful Use criteria. It is also very helpful to providers and vendors to set the expectation that Stage 1 Menu Set Requirements will become Core Requirements in Stage 2. Vendors and providers now know what to plan for over the next several years. The Meaningful Use Final Rules have provided structure and organization in electronic health records, previously characterized by a disorganized marketplace where individual products could not communicate effectively with each other.

The HITECH Act Has Ushered Great Progress

EHR vendors now have a clear roadmap for the next two years of what will be required of their software as a minimum for clinician adoption. They know what workflows need to addressed by the EHR. The vendors know the capabilities required of their EHR software in order for it to be certified. Some current EHR products may not be able to achieve certification. Clinicians now know that financial support is available if they use certified EHRs and demonstrate their meaningful use. Clinicians understand how their use of EHR will be measured. The HITECH Act has done as much as it can to remove uncertainty in clinicians' minds about whether or not to pursue an EHR. Enough of the EHR incentive variables are now known for providers, hospitals, and health systems to make reasoned choices about when and how they will acquire an EHR. The HITECH Act has brought focus and consistency to EHR adoption. It is now clear what needs to be done, even if it is not quite as clear how long it will take.

CONCERNS ABOUT ADOPTION OF ELECTRONIC HEALTH RECORDS

Adoption of EHRs is a Prerequisite for Interoperability

We have an enormous effort still ahead of us. Before going on to the specific standards that are the topic of today's hearing, we need to acknowledge that the standards have relatively little application unless individual healthcare providers have electronic health records in the first place. Most of the more than 400,000 Eligible Professionals still need to acquire an electronic health record, and most of that effort will be in small physician offices. CMS has estimated the five-year cost of acquiring an electronic health record for an eligible professional to be $94,000. EHR incentive plans through Medicare and Medicaid will cover 47 to 67% of that estimated cost. As a general rule, EHRs still do not allow providers to see more patients in a day, spend more quality time with their patients, or guarantee better or more consistent health outcomes for their patients. In short, even with the generous EHR incentive program, there still may not be a sufficient financial rationale for individual providers or small practices to invest in electronic health records.

Implementing an EHR is Stressful for the Provider

Implementing electronic health records in small physician offices is not like purchasing a copy machine or a fax machine. In addition to the great capital expense, the EHR is markedly disruptive to both the clinical and administrative functions of the office. Every provider, medical assistant, receptionist, and billing staff member needs to change the way they do their work. Even with excellent training, it usually takes 2–12 months before providers are fully comfortable on their new tools. On a new EHR, each office visit takes longer—this means increased waiting times for patients or a fewer number of patients per day for the provider. It is not uncommon for providers on a new EHR, after a full 8–10 hour day of seeing patients, to finish their charts on the computer at home for three or four hours in the evening. Even those providers who believe in the patient care benefits of an EHR are exhausted by the process in the first year.

EHRs Viewed Unfavorably by Many Providers Because of Administrative Documentation

Many providers who do not yet have EHRs in their office have commented to me how much they dislike the output received from many other physician office EHRs or from hospital EHRs. They specifically complain about how many pages these EHR reports require and how difficult it is to find the small bit of useful clinical information within. Upon investigation, most of this low-value verbosity comes from

physicians documenting specific history and physical exam findings required to support their billing. Also, as medicolegal requirements ratchet up, clinicians feel a need to document with a date-time stamp every single finding and every single item of data that they have reviewed. The existing cumbersome EHR reports impair the clinical process and can put the patient at risk by making important information obscure. Clinicians criticize the EHR for this clumsy reading even though the cause lies with our current payment and administrative systems, and not the EHR itself, which is otherwise widely agreed to be highly legible. Most clinicians would prefer to go back to simpler charting that more closely reflects their thought process. These EHR changes will need to await payment reform.

IT Professionals with Multiple Skills Needed for EHR Implementation

Another challenge in implementing electronic health records in small provider offices is the lack of technical expertise and support for the office. The providers are busy with a full schedule seeing patients. Medical assistants are putting patients in rooms or they are continuously on the phone with patients. Front office staff members are trying to make appointments and handle incoming calls. The billing staff is overwhelmed with insurance paperwork. Most providers and staff, especially those in small practices, don't have time to become fluent in the use of the new system, much less become expert in training others to use the system. Typical small physician implementations start two to three months before the expected launch date of the software. All current paper-based workflows need to be examined and re-designed for the new software. This requires analysts who are not only familiar with software but familiar with the healthcare office process. Bringing the majority of the 400,000 Eligible Professionals up to speed on an EHR in the next several years will be challenged by a lack of IT implementation professionals.

EHR Technical Requirements Can Be Challenging for Smaller Practices

Small physician practices are already spending 40–60% of their net revenue on overhead. Space in small physician offices is at a premium and providing a physically locked computer space within the physician office is difficult. Physician offices do not typically have the technical expertise to manage the computers in the clinical areas as well as the office computer network and the larger computers that act as servers and tape backup for the EHR software. Hosting provider EHRs on centralized servers supporting multiple practices may address this concern, but many of the currently used office EHRs are not yet ready for this step-up in technology. Many small towns do not have local computer hardware professionals to support physician offices. The Regional Extension Centers (RECs) exist to assist physicians in this context but even with generous funding, the RECs will be challenged to meet the enormous demand in the next several years.

STANDARDS-RELATED PRIORITIES FOR THE FUTURE

A Standard for Transmitting Provider Text Notes

When providers care for patients as a team, they expect to be able to review the patient's relevant laboratory results, diagnostic imaging reports, diagnostic images, and text reports that have been produced by other providers. Historically these text reports were produced by transcribing notes that physicians dictated for an office visit, a consultation note, a surgical procedure, and the like. These text reports are crucial for the coordination and transfer of care among providers. One of the Meaningful Use Core Requirements for Eligible Professionals calls for the capability to exchange "Key Clinical Information" among providers and gives examples of such data. The Requirement leaves the interpretation of "key clinical information" up to the provider. The HITECH Act specifies that the content standard for a patient summary will be the Continuity of Care Document (CCD) or Continuity of Care Record (CCR). These two documents have 17 sections containing mostly lists but there is no standard CCD or CCR for the specific text documents most useful for patient care. Physician office EHRs and hospital EHRs need to be able to export and import CCDs or CCRs specifically created for these crucial physician-authored reports.

A Standard for Exporting and Importing of Patient Information Directly Between EHRs and Directly Provider-to-Provider

As noted above, health information exchange is predicated upon providers having electronic health records. Oregon is currently developing a statewide plan for the operation of local, regional, or statewide health information exchanges. There is discussion as to what health information should be exchanged and how that exchange

should be managed, for example, directly from provider to provider or from provider to central information exchange to another provider. There are pros and cons of these two ends of the spectrum. Three points need to be made here. First, even if one has a centralized health information exchange (HIE) the EHR still needs to export and import the common patient information such as laboratory reports, diagnostic imaging reports, diagnostic images, and provider text reports from the HIE. The HITECH Act already specifies the content standard for most of these data types but Meaningful Use Stage 1 does not require EHRs to use this function. Second, HIEs are not yet well established. Complex centralized patient data repositories serving as HIEs are likely to be expensive to build and maintain and it may take a number of years before most providers have access to an affordable HIE of this nature. Third, central clinical data repositories may not be as trusted by patients as direct exchange of information from one provider known by the patient to another provider known by the patient. EHRs that can directly export and import data are required even if HIEs are present, and such EHRs have the added benefit that they can be used among providers when an HIE is not available. The next round of regulations needs to require that EHRs can export and import these data types directly to and from other EHRs without requiring a central health information exchange.

It should be noted that importing clinical data from an outside EHR into one's own EHR will be very challenging technically and culturally. Typical use of a CCD or CCR has them displaying the outside information in the equivalent of a "Correspondence" section of the electronic record. This is certainly better than having no information at all, but if we wish physicians to order less duplicate testing, we will need to devise technical standards where the results of an outside diagnostic test appear in the EHR results table very close to the internally-obtained test results.

Most ambulatory care in this country is delivered by providers in the patient's local area. Providers in each specialty are likely to know their colleagues in the other specialties from whom they receive and to whom they send consultation requests. Much of the time these consultation requests are arranged by the provider or by one of his/her staff members. In a paper world this is conveniently handled by a phone call and/or faxing of the clinical documents. The Receiving Physician is very appreciative of having organized patient information from the Sending Physician ahead of the patient arriving in the Receiving Physician's office. As clinicians move to electronic health records, we need to enable our EHRs with the ability to transfer patient information as easily as fax machines accomplish that transfer now. The Sending Physician knows what data need to go ahead of the patient. All EHR vendors need to provide this export/import function at the point of care for use by office staff This concept and the next two have been promulgated by Wes Rishel at Gartner and have led to the NHIN Direct Project.

A Standard Directory for Health Internet Addresses

If providers are going to electronically export patient information for immediate use by another provider, they will need to have a system of Health Internet Addresses and provider directories. A Certificate Authority will need to be established that can guarantee the authenticity of a provider's Health Internet Address. After a provider decides to refer the patient to another physician, whether next-door or in another state, the provider or his/her staff member could go onto the Internet and search for the provider's authenticated Health Internet Address. This could be entered into the provider's EHR, which would send an encrypted packet of provider text reports (for example, Office Visit Notes), recent laboratory results, diagnostic imaging reports, and diagnostic images to the Receiving Physician's EHR, which would similarly import the patient information. Both provider offices would be assured of immediate transmittal and receipt and the authenticity of the providers' identities. A state, regional, or national body could provide a similar function by building a Master Provider Index. For the basic function of a provider pushing patient information to another provider, there is not a need for a centralized clinical data repository. In the longer run, we need a method where an emergency department, for example, could pull patient data from other providers and hospitals when the patient or family member is unable to say where he or she has been cared for previously. This would require the more complex function of a Record Locator Service, which would keep track of the disparate electronic sources of a patient's clinical data. A state or regional organization could furnish a Record Locator Service.

A Standard for Document Transfer That Can Accommodate Providers on Paper Records

It will be years before all providers have electronic health records. For the next few years, providers will need to be confident that they can manage patient information to support patient care whether the Sending Physician or the Receiving Physician, or both, or neither, is on an EHR. Imagine the Sending Physician has an EHR that produces a concise, thorough patient information document. The Sending Physician looks up the Receiving Physician's Health Internet Address and sends the document directly from her EHR like an attachment to an e-mail. The Receiving Physician, unbeknownst to the Sending Physician, does not have an EHR. No problem—he receives the document as an attachment to a secure e-mail, prints it out, reviews it, and includes it in his paper charts. Once he acquires a certified EHR, he will be able to import the document easily without resorting to printing. We need a transfer standard that is human readable and that is flexible in terms of the technology required on the receiving end.

A Standard EHR Functionality Requirement for Quality Measure Reporting

The Standards and Certification Criteria Final Rule is clear about what quality measures Eligible Professionals will submit as part of the Core Requirements. I appreciate the ONC making these measures consistent with the Physician Quality Reporting Initiative. Although the data elements for figuring the numerators, denominators, and exclusions of each measure are clear, many EHRs will have difficulty in getting their EHR software to produce these numbers automatically. Business intelligence tools built into most EHRs are currently immature. Smaller practices would likely need to seek the help of consultants in order to produce an acceptable report from their EHR. The necessary clinical data should be present in a certified EHR but smaller EHR vendors will be challenged to include adequately sophisticated report writing tools in their products that can be used directly by clinicians. Quality measure reporting needs to be a core EHR function specified by a consistent nationwide requirement, so that providers in any practice can press a button to produce submission-ready reports on a given measure.

A National Model for Privacy and Patient Consent

Currently Oregon is trying to establish health information exchange privacy and patient consent standards for use within the state. I applaud these efforts but think that EHR adoption would be much enhanced by having consistency in privacy and patient consent across all 50 states. In Portland we often see patients from Southwest Washington. In the course of a busy office day, clinicians need access to previous records. Having significantly different privacy laws in Washington versus Oregon would lead to uncertainty, missed information, and unnecessary duplication of diagnostic testing. Currently, providers may exchange health records for purposes of payment, treatment, and operations without explicit patient consent. If it is decided that a patient needs to specifically consent to have their provider send or retrieve their health information, then we need a standard so that any vendor's EHR can effectively communicate the obtained patient consent with any other vendor's EHR in any other state. We need a federal effort to convene, sponsor, and mandate development of model rules and laws that each state could take through its own legislative process. A "Uniform Privacy Code," as it were, like the Uniform Building Code, would provide interstate consistency and give EHR vendors confidence that their software would perform consistently wherever it is used.

Setting Appropriate Expectations on Provider Access Control to Patient Information

About six years ago at Providence Health and Services in Oregon, we looked at the access to the electronic chart for a typical four-day hospital stay. More than 65 different people had appropriate access to the patient's chart during and after their hospital stay. Depending on their role, some staff members had access to only a part of the patient's information. It is unpredictable which provider will need immediate access to a patient's chart at any given time. On a hospital floor, a physician might ask a colleague to take a look at her patient. The Receiving Physician walks right over to the computer and begins to examine the patient's information. Nurses frequently are called from one unit to another according to the ebb and flow of patient census and they need immediate access to the records of that unit's patients. The nature of fee-for-service healthcare makes it difficult to predict who will be taking care of the patient next. As an emergency physician, I would see people on Saturday night and refer them to the orthopedist to be seen first thing Monday morning. When they show up at the orthopedist's office, that doctor or her partner needs immediate access to the full electronic health record even though they have never seen

the patient before. Our model needs to set the expectation in the patient's mind that it is not possible to predict exactly who will need access to their record in the course of their care. To balance these relatively open provider access controls, I do believe we have an opportunity to involve the patient in reviewing the log of who looked at their records. Most confidentiality breaches in electronic health records are associated with people who have approved access to a given electronic health record system but use their access inappropriately in looking up information of a friend or colleague for whom they are not caring.

A Model for the Complete Health Record Being Available to the Provider

Access to the entire health record is important for providers taking care of patients. It is crucial that providers see the entire medication list, the entire allergy list, the entire problem list, pertinent laboratory results, and diagnostic imaging studies. Although the provider can infer some of the patient's diagnoses from the medication and allergy lists, it is crucial that providers see all the medications and allergies when they prescribe. Without this guarantee, the patient could be hurt when a physician prescribes a medication that interacts with one that they are already taking or to which they have developed an allergy in the past. Most physicians would be very uncomfortable practicing in an environment where some information about the patient in front of them may have been redacted. Similarly, providers need access to the complete laboratory reports and diagnostic imaging results when they're trying to make a diagnosis. Hiding these data because they imply a certain "restricted" diagnosis is unsafe and could ultimately result in physical harm to the patient. I acknowledge that most providers do not need to see the office visit notes from sensitive psychotherapy sessions and these parts of the records should be restricted to the mental health therapists only. Everyone else needs to see the full health record.

CONCLUSION

In summary, The HITECH Act and the Meaningful Use regulations have dramatically accelerated interest in electronic health records. The proposed standards have assured clinicians and EHR vendors of a level playing field where EHRs will ultimately be able to communicate with each other. The regulations appropriately require evidence not just of EHR implementation, but of improved intermediate healthcare outcomes. I respectfully request that the next round of standards builds on the progress of the current standards. Let national standards enable our small physician offices to communicate directly with each other using tools that can be mastered by the provider or office staff. We need a specific transfer standard for the most crucial provider-authored text notes. National regulations must require that EHRs can directly send and receive patient information initiated by the office staff at the point of care using the equivalent of e-mail attachments and Health Internet Addresses while we wait for more complex exchange methods to be developed. These tools can be used by physician offices still on paper records as they prepare to move to an EHR. Finally, we need a national privacy and patient consent model for states to use creating their own legislation so that patients and providers can be confident that clinicians always have all the information in front of them that they need to provide consistently superior care.

Chairman Wu and Members of the Subcommittee, thank you for the opportunity to testify on these important issues. I would be happy to answer any questions you may have.

BIOGRAPHY FOR RICHARD GIBSON

Richard Gibson is President of Oregon Health Network, a nonprofit using Federal Communications Commission funds to extend a medical-grade, high-bandwidth network to all Oregon hospitals, community colleges, and clinics for the underserved. He is a practicing family physician and former board-certified emergency physician. Previously he was Senior Vice President and Chief Information Officer for Legacy Health, an integrated delivery network in Portland, Oregon. Before that he was Chief Medical information Officer for Providence Health and Services, Oregon Region, also an integrated delivery network in Portland, Oregon.

Dr. Gibson practiced family medicine in Forks, Washington, a logging town of 3,000, four hours west of Seattle. He was an emergency physician in Port Angeles, Washington, a community of 20,000 three hours west of Seattle. He received a BS in Biology from Stanford University and an MD from Case Western Reserve University in Cleveland. He holds a PhD in Medical Informatics from the University of Utah and an MBA from The Wharton School.

Outside of practicing medicine, Dr. Gibson has spent his information technology career helping physicians, health systems, and independent software vendors acquire, develop, and implement electronic health records for use in physician office and hospital settings. He has advised the State of Oregon in electronic health records, health record privacy and security, health information exchange, and telemedicine.

Chairman WU. Thank you very much.

Ms. McGraw, please proceed.

STATEMENT OF DEVEN MCGRAW, DIRECTOR OF THE HEALTH PRIVACY PROJECT, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MCGRAW. Okay. Thank you. Chairman Wu, Ranking Member Smith and the staff. I really, very much appreciate the invitation to testify before you on the privacy and security challenges raised by widespread adoption of health IT.

What we do at CDT is develop and promote pragmatic privacy and security policy and technology solutions for a health system that we really hope will be increasingly characterized by electronic health information exchange to improve individual as well as population health, and I also chair the Health IT Policy Committee's privacy and security team that Dr. Blumenthal mentioned, and I appreciate the thanks. We are in a very good place, I think, for making some progress on these issues.

We know from survey data that the public is actually quite enthusiastic about what we are doing with health IT but they also express, in equal numbers, concern about privacy. You can't have one without the other. Essentially, privacy is not the obstacle to doing all this and getting it done; it is the enabler, and we need to consider it that way and pay it serious attention, and clearly this Subcommittee agrees or you wouldn't have asked me here today in a hearing that is largely about standards. And we will talk about security standards because that is where standards really come into focus, probably less so on the privacy side.

We do have the privacy and security regulations of HIPAA, and of course states have laws as well, and those are the baseline, but we are really changing the way we are going to be moving health information and setting up new infrastructures and so we have to consider what we need to layer on top of what we already have, and in addition, we are talking about health information technology, not just protecting health information, and so we need to think about the strong role that technology can actually play in helping us to accomplish a comprehensive and flexible framework of privacy and security protections that will build that trust layer that will enable us to go forward.

As I mentioned before, we are in a much better place than we were a few years ago when we were arguing about privacy. We are still arguing about it but we actually, the work that Congress did in the HITECH legislation has pushed us tremendously forward, and in addition, the financial incentives that are part of the HITECH incentive program give us additional policy levers to really push us into a better place with respect to privacy and security.

We still do have gaps to address, of course. You know, this is not something that is never done. We need to be continuously paying attention to this, and so I am going to talk a little bit about secu-

rity and I am going to give some credit to one of my panelists from HIMSS. They did a survey fairly recently of large health care organizations that indicated that security is far less of a priority than we would hope. Just to lay out some examples, fewer than half conduct the annual risk assessment that the HIPAA security rule requires. Fifty-eight percent of these organizations say they actually don't have security personnel, and 50 percent reported spending three percent or less of their resources on security. And again, this is a survey of large organizations and not small practices, although as you will see in HIMSS' written testimony, they are doing this survey next, I think. Those will probably be some very sobering numbers but they are a lesson for us. We really need to be quite serious about this. When you think about what the root is of the public's concern, a lot of it is about inappropriate access to records, for which security is a primary gatekeeper.

Now, we know that with respect to what an electronic health record has to have in order to be certified, there are functionalities that have to be present, and Dr. Blumenthal mentioned some of these—the ability to encrypt data, the ability to generate an audit trail, but there is actually no clear requirement to use the functionalities. The HIPAA security rule is very flexible. It says that some of them are addressable. Similarly, in Meaningful Use, you have to conduct a risk assessment and address any deficiencies, but here you have the functionalities in the record and we are not are being terribly clear with providers about using them. I think that is a major deficiency. We need to raise our expectations certainly with respect to small providers. You know, a piece of health data is sensitive no matter who is holding it, whether it is a large institution or a single physician practice. But in terms of the level of resources that the smaller physician practices can put into this, clearly we need something that is scalable and something that works for them now with a glide path to greater expectations down the road.

So I am reaching the end of my time. My written testimony has a number of other gaps that I have discussed there, including the HIPAA deidentification standard. We are seeing an increasing emphasis on access to and use of deidentified data for a range of purposes. Certainly when data is deidentified, stripped of identifiers, it is much more privacy protective, but we actually don't have a legal prohibition against reidentification that we can enforce, and that is something that Congress could actually do to really help secure trust. Again, the deidentified data issue is a big one. HHS is doing a study. I think after that comes out, we ought to talk seriously about what the right next steps are.

So I am going to close. I had a real ambitious oral statement here for five minutes. As I noted before, assuring privacy and security to the level where we have the trust of the general public in what we are trying to build here really is an ongoing commitment and the fact that you have put privacy and security on this agenda, even two years after HITECH when a lot of people are saying, "didn't we do this already?" shows that you agree, which is terrific.

So thank you again for the opportunity and I am happy to answer any questions that you might have.

[The prepared statement of Ms. McGraw follows:]

PREPARED STATEMENT OF DEVEN MCGRAW

Chairman Wu 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.

You have asked me to address, in particular, the main challenges for personal privacy and information security presented by health information technology (health IT), as well as the privacy and security gaps and priorities that remain to be addressed for future health IT activities. Not surprisingly, the main privacy and security challenges in health IT result from gaps in current law and a lax approach to enforcement, accountability and oversight. *My testimony below focuses on those gaps*. However, since the broad topic of the hearing deals with health IT "standards," I have referenced some comments endorsed by CDT urging a measured role for government in setting and enforcing standards for 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] Contrary to the views expressed by some, privacy is not the obstacle to 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.

To build and maintain this trust, 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:

- Implementation of core privacy principles, or fair information practices;[2]
- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.[3]

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

---

[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).

[2] 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*.

[3] 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).

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 two years ago. The privacy provisions enacted in the stimulus legislation—commonly referred to as HITECH or ARRA—are an important first step to addressing the gaps in privacy protection. However, more work is needed to assure effective implementation and address issues not covered by (or inadequately covered by) the changes in ARRA.

In my testimony below, I call for:

- Establishing baseline privacy and security legal protections for personal health records (PHRs);
- Ensuring appropriate limits on downstream uses of health information;
- Strengthening protections against re-identification of HIPAA de-identified data;
- Encouraging the use of less identifiable data through the HIPAA minimum necessary standard;
- Tightening restrictions on use of personal health information for marketing purposes;
- Strengthening accountability for implementing privacy and security protections; and
- Strengthening accountability for implementing strong security safeguards.

Health IT: Key Privacy and Security Concerns

Establish Baseline Protections for PHRs

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. Personal health records (PHRs) and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers, are not covered by the HIPAA regulations unless they are being offered to consumers by covered entities.[4] In the absence of regulation, 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.[5]

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. 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, where consumers should be in more control of their records, and may do more harm than good. Further, it may not be appropriate for the Department of Health and Human Services (HHS), which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

---

[4] HIPAA applies only to covered entities—providers, health plans, and health care clearinghouses. Section 1172 of the Social Security Act; 45 CFR 164.104. As explained in more detail below, ARRA extended the reach of some of HIPAA's regulations to business associates, which receive health information from covered entities in order to perform functions or services on their behalf.

[5] 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.

CDT applauds Congress for not extending HIPAA to cover all PHRs.[6] Instead, Congress 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.[7] 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.[8] Establishing these protections will likely require Congress to extend additional authority to HHS and/or the FTC.

Ensure Appropriate Limits on Downstream Uses of Data

As noted above, HIPAA applies only to "covered entities." However, 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.[9] Such agreements may not authorize the business associate to access, use or disclose information for activities that the covered entity itself could not do under HIPAA.[10] The agreements also are required to establish both the permitted and required uses and disclosures of health information by the business associate[11] 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."[12]

This combination of provisions demonstrates that HHS intended to place limits on what a business associate can do with health information received from a covered entity. However, one large national business associate has been accused of using data they receive from covered entities to support other business objectives,[13] and some privacy advocates have long suspected that such practices are more widespread.

In ARRA Congress took a significant step toward strengthening accountability 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.[14] HHS recently issued a proposed rule making it clear that accountability also extends 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.[15] CDT strongly applauds these actions.

However, CDT remains concerned that the HIPAA Privacy Rule is 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 either: (1) an indication that HIPAA is not being adequately enforced or (2) evidence that some business associate agreements are too permissive with respect to additional uses of information. In this testimony below CDT calls for stronger enforcement of HIPAA. 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 data to only what is reasonably

---

[6] 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.

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

[8] "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).

[9] 45 CFR 164.502(e)(1) & (2).

[10] 45 CFR 164.504(e)(2)(i).

[11] Id.

[12] 45 CFR 164.504(e)(2)(ii)(A)

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

[14] ARRA, section 13404.

[15] 75 Fed. Reg. 40867–40924, at 40885 (July 14, 2010).

necessary to perform the contracted services.[16] Failure to appropriately account for and control downstream uses of data will jeopardize building trust in health IT.

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 applicable 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.[17] 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 documented how easy it is to re-identify some data that qualifies as de-identified under HIPAA.[18]

Congress recognized this, and ARRA requires HHS to do a study of the HIPAA de-identification standard; that study, due in February 2010, is 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 points) to ensure that it continues to present *de minimis* risk of re-identification.[19] However, Congress need not wait for the issuance of the study. To ensure consumers are protected, Congress should enact provisions to ensure data recipients can be held accountable for re-identifying data.

Encourage Use of Less Identifiable Data

Although the HIPAA provisions for de-identifying data need to be revisited and strengthened, CDT also believes that privacy risks are lessened when data has been anonymized to the greatest extent possible. In particular, many non-treatment uses of health data—including quality, research and public health—can be effectively done with data where sufficient patient identifiers have been removed to make it anonymous to the recipient. Unfortunately, federal and state privacy laws do not sufficiently promote the use of less identifiable data. Instead, they permit (in the case of HIPAA) or require (in the case of many state reporting laws) the use of fully identifiable data (including patient names, addresses, phone numbers, etc.), providing little incentive to remove identifiers from data before its use.

Under the collection and use limitations of fair information practices, data holders and recipients must collect, use and disclose only the minimum amount of information necessary to fulfill the intended purpose of obtaining or disclosing the data. The HIPAA Privacy Rule incorporates these principles in the "minimum necessary" standard, which requires covered entities to use only the minimum necessary amount of data for most uses and disclosures other than treatment. This standard is intended to be flexible, but HHS has not issued any meaningful guidance on this standard. As a result, covered entities and their business associates frequently express concerns about how to implement it, and CDT suspects that few covered entities or business associates take affirmative steps to minimize the identifiability of data.

The Privacy Rule does provide for two anonymized data options—de-identification (as discussed above) and the limited data set, which can be used for research, public health and health care operations). These data sets provide greater privacy protection for individuals, but are not useful for all purposes due to the number of identifiers that must be removed before the data can qualify for either option.

---

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

[17] 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).

[18] 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).

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

ARRA attempts to strengthen the Privacy Rule's collection and use limitations by strongly encouraging covered entities to use a limited data set to comply with the minimum necessary standard, as long as limited data is sufficient to serve the purposes for the data access or disclosure.[20] This section of ARRA also requires the HHS Secretary to issue guidance on how to comply with the minimum necessary standard. In comments to HHS, CDT has asked HHS to be clear in its guidance that covered entities must address the identifiability of data in order to be in compliance with the minimum necessary standard.[21]

Tighten Rules Regarding Use of Patient Data for Marketing

The use of sensitive medical information for marketing purposes is one of the most controversial practices affecting health privacy. In health privacy surveys, use of data for marketing ranks as a top concern among respondents.[22] Consequently, protections against the unauthorized use of personal health information for marketing purposes are critical to building trust in new e-health systems.

The HIPAA Privacy Rule has provisions intended to limit the use of health data in marketing, but it historically was subject to a number of exceptions. There also has been little regulatory or legislative investigation of health marketing practices.

In ARRA, Congress took some steps to tighten the definition of "marketing" in the Privacy Rule. Under the new provisions, communications that are paid for or "subsidized" by third parties are marketing, and therefore require prior patient authorization—even if those communications would otherwise not be construed as marketing because they qualify for one of the existing exceptions. But even this new provision includes exceptions that could swallow the rule. For example, HHS has initially interpreted subsidized treatment communications to be outside the new ARRA rules requiring prior patient authorization. As a result, a covered entity can use a patient's data without consent to send her a letter urging her to switch to a different brand medication, even if that communication was paid for by the manufacturer of the medication.[23] Patients will experience these communications as marketing and mistrust any system that allowed this to happen without their authorization.

Strengthen Accountability/Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for noncompliance, but those rules have never been adequately enforced.[24] The Office for Civil Rights (OCR) within HHS, charged with enforcing the HIPAA privacy regulations, had not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office found numerous violations of the rules.[25] 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.[26]

A lax enforcement environment sends a message to entities that access, use and disclose protected 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. Further, HIPAA has never included a private right of action, leaving individuals dependent on government authorities to vindicate their rights.

---

[20] ARRA, Section 13405.

[21] See CDT Comments, supra note 16.

[22] In the 2006 Markle Foundation survey referenced in footnote 1, 89% of respondents said they were concerned about marketing firms getting access to their personal health information online, and 77% described themselves as "very concerned." *http://www.markle.org/downloadable_assets/research_doc_120706.pdf.*

[23] HHS did give patients the right to opt-out of receiving subsidized treatment communications, but an opt-out is not as protective of patient privacy as requiring prior consent.

[24] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008), *http://www.latimes.com/business/la-na-privacy9aor09.0.5722394.story*.

[25] Id. Although this story is two years old, to the best of our knowledge no civil monetary penalties have been assessed since that time. Over the last couple of years 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.

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

In ARRA, Congress took a number of important steps to strengthen HIPAA enforcement:[27]

- State attorneys general are now expressly authorized to bring civil enforcement actions under HIPAA, which puts more hands on the enforcement deck.
- As mentioned above, business associates 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 ARRA, 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.[28]
- 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 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 ARRA provisions are a major advancement in enforcement of federal health privacy laws, but enforcement is still lax. To strengthen accountability and further build public trust in health IT, CDT has two recommendations: (1) deem providers who are found to be in significant violation (either criminally responsible or found to be in willful neglect of the law) ineligible to receive subsidies under the federal health IT incentive program, and (2) provide individuals with a limited private right of action to enforce their HIPAA privacy rights.

With respect to the former (declaring a significant HIPAA violation to be a disqualification for health IT subsidies), it is hard to justify providing tax dollars as a reward for meaningful use of health IT to an entity in significant violation of our nation's privacy laws.

With respect to a private right of action for privacy and security violations, CDT recognizes that providing such a right for every HIPAA complaint—no matter how trivial—would be inappropriate and disruptive. However, Congress should give consumers some right to privately pursue recourse in specific circumstances. For example, policymakers could create compliance safe harbors that would relieve covered entities and their business associates of liability for violations if they meet the privacy and security standards but would allow individuals to sue if they could prove the standards had not been met. Another suggestion is to limit the private right of action to only the most egregious HIPAA offenses, such as those involving intentional violations or willful neglect.

Strengthen Accountability for Strong Security Safeguards

According to a recent survey of large health care organizations conducted by the Health Information Management Systems Society (HIMSS):

- Fewer than half (47%) conduct annual risk assessments (which are required under the HIPAA Security Rule),
- 58% have no security personnel, and
- 50% reported spending 3% or less of organizational resources on security.[29]

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 meaningful use incentive program, the certification requirements include a number of important security functionalities, including the ability to encrypt data in motion and at

---

[27] See Sections 13409–13411 of ARRA.

[28] 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.

[29] See testimony of Lisa Gallagher, Senior Director of Privacy & Security, HIMSS, *http://healthit.hhs.gov/portal/server.pt?open=512&objID=1817&parentname=CommunityPage&parentid=28&mode=2&in_hi_userid=11673&cached=true* (November 19, 2009).

rest, the ability to generate an audit trail, and authentication and access controls.[30] However, there is no clear requirement, either in the meaningful use criteria or in the HIPAA Security Rule, to actually implement and routinely use these functionalities. Providers are required under meaningful use to perform a security risk assessment and respond to any deficiencies discovered, but this falls short of a clear requirement to implement or have a plan for implementing the functionalities required for EHR certification. CDT is continuing to advocate with regulators for strengthened security requirements. Providers with fewer resources (such as small physician practices) may need to have security requirements scaled up over time; policymakers should, however, consider imposing greater obligations on the connecting infrastructure to better address gaps or potential weak links as these systems develop.

Promote a Measured Role for Government in Health IT Standards

Although most of this testimony concerns health IT privacy and security, CDT would like to take this opportunity to reference a set of collaborative comments drafted by the Markle Foundation and endorsed by a broad range of stakeholders, including CDT. The comments concern the role of standards in health IT and urge a limited role for government in certifying health IT.[31] CDT asks that these comments also be included in the Subcommittee hearing record.

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.

BIOGRAPHY FOR DEVEN MCGRAW

Deven McGraw is the Director of the Health Privacy Project at CDT. The Project is focused on developing and promoting workable privacy and security protections for electronic personal health information.

Ms. McGraw is active in efforts to advance the adoption and implementation of health information technology and electronic health information exchange to improve health care. She was one of three persons appointed by Kathleen Sebelius, the Secretary of the U.S. Department of Health & Human Services (HHS), to serve on the Health Information Technology (HIT) Policy Committee, a federal advisory committee established in the American Recovery and Reinvestment Act of 2009. She co-chairs the Committee's Privacy and Security "Tiger Team" and serves as a member of its Meaningful Use, Information Exchange, and Strategic Plan Workgroups. She also served on two key workgroups of the American Health Information Community (AHIC), the federal advisory body established by HHS in the Bush Administration to develop recommendations on how to facilitate use of health information technology to improve health. Specifically, she co-chaired the Confidentiality, Privacy and Security Workgroup and was a member of the Personalized Health Care Workgroup. She also served on the Policy Steering Committee of the eHealth Initiative and now serves on its Leadership Council. She is also on the Steering Group of the Markle Foundation's Connecting for Health multi-stakeholder initiative.

Ms. McGraw has a strong background in health care policy. Prior to joining CDT, Ms. McGraw was the Chief Operating Officer of the National Partnership for Women & Families, providing strategic direction and oversight for all of the organization's core program areas, including the promotion of initiatives to improve health care quality. Ms. McGraw also was an associate in the public policy group at Patton Boggs, LLP and in the health care group at Ropes & Gray. She also served as Deputy Legal Counsel to the Governor of Massachusetts and taught in the Federal Legislation Clinic at the Georgetown University Law Center.

Ms. McGraw graduated magna cum laude from the University of Maryland. She earned her J.D., magna cum laude, and her L.L.M. from Georgetown University Law Center and was Executive Editor of the Georgetown Law Journal. She also has a Master of Public Health from Johns Hopkins School of Hygiene and Public Health.

---

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

[31] *http://www.markle.org/downloadable_assets/20090430_meaningful_use.pdf* (see in particular, section 4) and *http://www.markle.org/downloadable_assets/20100510_collabcmts.pdf.*

Chairman WU. Thank you very much, Ms. McGraw.
Ms. Bass, please proceed.

STATEMENT OF DEB BASS, PRESIDENT AND CEO, BASS & ASSOCIATES INC.

Ms. BASS. Thank you. Chairman Wu, Ranking Member Smith, Committee Members, staff and guests, thank you for the opportunity to present on this very important topic. I am honored to be amongst such esteemed members of the health care community, my fellow testifiers, all who are contributing so much to the advancement of health care reform.

In preparing for this testimony, I spent considerable time reflecting on our experiences in Nebraska. There is a great deal of expert dialog on the topic. Certainly, hearings like this provide additional subject matter expertise that will surely benefit the ongoing development of standards for interoperability and information security and health care reform in general. It is clear that this Committee has significant data and information at its disposal to continue its pursuit to develop solid and workable standards.

I would like to focus my testimony on principles Nebraska has implemented in this arena and respectfully share with you the lessons that we have learned as we directly apply the success of those efforts for those at the Office of the National Coordinator who are developing these critical standards.

There are three areas that have contributed tremendously to Nebraska's success in implementing the federal health care initiatives of achieving Meaningful Use: One, extensive and persistent stakeholder engagement; two, physician engagement; three, sharing the knowledge among the States.

As President and CEO of Bass and Associates and Executive Director of NeHII, the Nebraska Health Information Initiative, I have worked closely with the NeHII team and project members to ensure we engaged key stakeholders across our state. We knocked on doors, developed educational materials, and launched community-based consumer education campaigns. We spoke in cities and across rural Nebraska—rotary clubs, state associations and chamber of commerce meetings. In short, no stone was left unturned in our efforts to engage citizens across the state. The Office of the National Coordinator has done an excellent job of reaching out to the stakeholders including our own opportunity to host Dr. Blumenthal on his recent visit to Nebraska. Dr. Blumenthal took time from his busy schedule to tour the NeHII-enabled facilities and witness the successful health information exchange up close. I am certain his travels are extensive and require a great deal of effort but the benefits of these stakeholder visits across the country are immeasurable.

As the ONC develops its next set of standards, I strongly urge them to continue to avail themselves of stakeholder conferences, meetings and other opportunities to demonstrate their continued support of these standards, and I express appreciation for the efforts states make to understand, implement and adhere to these guidelines. The stakeholder engagement is especially important as standards are being examined and released, and particularly those supporting the ONC's efforts to develop technical standards to ad-

dress interoperability demands. At its March 24, 2010, HIT Standards Committee hearing, ONC identified the need to support a broader set of stakeholders and providers in information exchange. This I believe was another critical step in the right direction to encourage stakeholders. We have included our circle for pharmacists, dentists, chiropractors and school nurses.

NeHII was implemented using the most current available standards and we remain committed to conforming to standards as they are developed. We will make every effort to pursue the conversations and affirmations from NeHII participants in setting those standards to guarantee the ability of HIEs to operate with the least amount of impact to daily operations.

Recently, I met with a state that, while it possessed all the components to successfully build an HIE, is struggling with the critical issue of physician adoption of their HIE. Our conversations around solutions to reverse this trend revealed how difficult it is to move forward on interoperability of electronic records without fully engaged physicians. At NeHII, we are fortunate to have Dr. Harris Frankel, a respected Omaha practicing board-certified physician, who serves as the NeHII visionary. In this capacity, he is able to reach deep within the physician community as a respected leader and as one of their own. I cannot tell you the number of times Dr. Frankel's reach within the physician community allowed us access to respected physicians who became champions of NeHII and therefore supported interoperability across the health care spectrum. Dr. Blumenthal is a practicing physician and enjoys this esteem as well. His continued contact with the physician community toward adhering to standards and interoperability of electronic records will be the cornerstone to engaging this critical constituency and ultimately one of the key success factors of health care reform.

Finally, I believe the Office of the National Coordinator should continue to be a dedicated resource for current information in offering a collection of lessons learned and best practices for states to rely upon. A national repository of best practices from all states would be a helpful guide in that direction. We at NeHII have offered, and to date 16 states have accepted, our privacy and security policies for states to utilize and as an example for drafting their own policies. Sharing this information has engendered goodwill, trust, and a shared commitment. I urge the ONC to facilitate the sharing of knowledge among states throughout the reform effort. The ONC's Support Grant Opportunity administered through RTI [Research Triangle Institute] is an excellent example of encouraging states to cooperatively identify barriers and share knowledge in overcoming them.

Chairman Wu, Ranking Member Smith, and Members of the Committee, thank you for the opportunity to testify today. Your commitment to reach out to those who shoulder the largest part of health care reform effort is much appreciated and will go a long ways toward its continued success. I look forward to answering your questions. Thank you.

[The prepared statement of Ms. Bass follows:]

PREPARED STATEMENT OF DEBORAH BASS

Chairman Wu, Ranking Member Smith, Committee Members, Staff and Guests:

Thank you for the opportunity to present on this important topic. I am honored to be among such esteemed members of the health care community, my fellow testifiers, all who are contributing so much to the advancement of health care reform.

In preparing for this testimony, I spent considerable time reflecting on our experiences in Nebraska. There is a great deal of expert dialogue on this topic in the industry. Certainly, hearings like this provide additional subject matter expertise that will surely benefit the ongoing development of standards for interoperability and Information security, and health care reform in general. It is clear this committee has significant data and information at its disposal to continue its pursuit to develop solid and workable standards.

I would like to focus my testimony on principles Nebraska has implemented in this arena and respectfully share with you lessons learned I believe directly apply to the success of the efforts for those at the Office of the National Coordinator who are developing these critical standards.

There are three areas that have contributed tremendously to Nebraska's success in implementing the federal health care initiatives of achieving meaningful use:

- Extensive and persistent stakeholder engagement
- Physician Engagement and,
- Sharing knowledge among States

As President and CEO of Bass & Associates, and Executive Director of NeHII, the Nebraska Health Information Initiative, I worked closely with our NeHII team and project members to ensure we engaged key stakeholders across the State. We knocked on doors, developed educational materials and launched community-based consumer education campaigns. We spoke in the cities and across rural Nebraska at Rotary Clubs, State Associations and Chamber of Commerce meetings. In short, no stone was left unturned in our efforts to engage citizens across our State. The Office of the National Coordinator has done an excellent job of reaching out to stakeholders, including our own opportunity to host Dr. Blumenthal on his recent visit to Nebraska. Dr. Blumenthal took time out of his busy schedule to tour NeHII-enabled facilities and witness our successful health information exchange up close. I am certain his travels are extensive and require a great deal of effort, but the benefits of these stakeholder visits across the country are immeasurable.

As the ONC develops its next set of standards, I strongly urge them to continue to avail themselves of stakeholder conferences, meetings, and other opportunities to demonstrate their continued support of these standards, and express appreciation for the effort States make to understand, implement and adhere to their guidelines across the country. This stakeholder engagement is especially important as standards are being examined and released, in particular those supporting the ONC's efforts to develop technical standards to address interoperability demands. At its March 24, 2010 HIT Standards Committee hearing, ONC identified the need to support a broader set of stakeholders and providers in information exchange. This, I believe, was another critical step in the right direction to encourage stakeholders to embrace the new standards.

NeHII was implemented using the most current available standards, and we remain committed to conforming to new standards as they are developed. We will make every effort to pursue the conversations and affirmations from NeHII participants in setting those standards to guarantee the ability of HIEs to operate with the least amount of impact to daily operations.

Recently, I met with a State that, while it possessed all of the components to successfully build an HIE, is struggling with the critical issue of physician adoption of that same HIE. Our conversations around solutions to reverse this trend revealed how difficult it is to move forward on interoperability of electronic records without fully engaged physicians. At NeHII, we are fortunate to have Dr. Harris Frankel, a respected Omaha practicing, board-certified physician, who serves as the NeHII visionary. In this capacity, he is able to reach deep within the physician community as a respected leader and as one of their own. I cannot tell you the number of times Dr. Frankel's reach within the physician community, and not a little of his Midwestern charm, allowed us access to respected physicians who became champions of NeHII and therefore supported interoperability across the healthcare spectrum. Dr. Blumenthal, as a practicing physician, enjoys this esteem as well. His continued contact with the physician community toward adhering to standards in interoperability of electronic records will be the cornerstone to engaging this critical constituency and, ultimately, one of the key success factors of health care reform.

Finally, I believe the Office of the National Coordinator should continue to be a dedicated resource for current information in offering a collection of lessons learned and best practices for States to rely upon. A national repository of best practices

from all States would be a helpful guide in that direction. We at NeHII have offered, and to date 16 States have accepted, our Privacy and Security policies for States to utilize as an example for drafting their own policies. Sharing this information has engendered good will, trust and a shared commitment. I urge the ONC to facilitate the sharing of knowledge among States throughout the reform effort. The ONC's Support Grant Opportunity, administered through RTI, is an excellent example of encouraging States to cooperatively identify barriers and share knowledge in overcoming them.

Chairman Wu, Ranking Member Smith and members of the Committee, thank you for the opportunity to testify today. Your commitment to reach out to those who shoulder the largest part of the health care reform effort is much appreciated and will go a long way toward its continued success. Thank you.

BIOGRAPHY FOR DEBORAH BASS

Ms. Deborah Bass is the Executive Director and active board member for the Nebraska Health Information Initiative (NeHII). NeHII is the statewide health information exchange in the State of Nebraska. Ms. Bass directed the creation of this 501 (c) (3) non-profit corporation and currently oversees and manages the continued efforts in the development of Nebraska's statewide Health Information Exchange (HIE). Her duties have included creating and developing stakeholder relationships, building consensus and support for the organization, communications and implementing Board of Directors recommendations, managing vendor relationships, recruiting and building the management team, developing and implementing the consumer educational campaigns, leading the committee effort to develop the privacy, security and operational policies, writing the business plan, planning and leading the organization's public events and a multitude of other activities associated with implementing HIE. She is a regular public speaker for national conferences on a number of topics surrounding the development and future of HIE.

Chairman WU. Thank you, Ms. Bass.

And now it is in order for questions, and the Chair recognizes himself for five minutes.

Dr. Blumenthal, in Dr. Gibson's testimony, he notes that there aren't enough IT implementation professionals to help with the implementation of health IT systems. Can you tell us what the Office of the National Coordinator has done to provide assistance to educational institutions to expand the health IT workforce? And Dr. Gibson, can you tell us what other assistance may be helpful to educational institutions to help with workforce needs. Dr. Blumenthal?

Dr. BLUMENTHAL. Thank you, Mr. Chair. We agree with Dr. Gibson, and in fact, the HITECH legislation very wisely encouraged us to support the training of health IT professionals. We have pro-

vided funding to 84 community colleges around the country to train a group of IT professionals who will be certified as competent to assist with the installation and maintenance of information technology but also to help professionals and hospitals with redesigning their work flow to take advantage of those new technologies.

We also have a series of curriculum development grants, one of which has gone to the Oregon Health Science University, to develop the curricula for these community college programs and we have developed a certification exam through a contract, a grant, actually, with another university to be able to certify these professionals. We expect to train in excess of 40,000 new health information technology professionals. The first class has enrolled in community colleges as of this fall so they will be graduating in the winter and in the spring of this year. So that will be in time for Meaningful Use Stage 1. It would be nice if they had been trained before the HITECH Act was passed but we are trying to live within the realities that we face.

Chairman WU. Thank you very much.

Dr. Gibson.

Dr. GIBSON. I think that the training that has been prescribed is excellent and I think it will help a great deal and I believe in that. Oregon is a proud leader in training many of those people at the community college level. I think practices will find it helpful, and it should address some of the need. I am concerned just with the many hundreds of thousands of eligible providers that the timeline might be a bit longer than we expect but I think we are all going in the right direction right now on that.

Chairman WU. Terrific. Thank you very much.

Last week the Office of the National Coordinator released a framework that will coordinate future work on interoperability and standards. How will the framework identify priorities and allow for stakeholder input and interface with the Health IT Standards Committee?

Dr. BLUMENTHAL. The framework is a means to an end, Mr. Chairman. Actually our priorities for developing standards are identified by the Meaningful Use framework, by the requirements for Meaningful Use that health professionals and providers across the country have to meet. We go backward, we work backward from the Meaningful Use requirements to identifying the standards, the capabilities that electronic health systems have to have, and that actually gives us guidance which the Health IT Standards Committee then works on to recommend standards. So it is really an ends-driven process. We focus on outcomes, the health of patients and what the record has to do in order to improve the health of patients, and that gives us guidance as to standards.

The framework that you referred to is a method of producing those standards, so once we know which standards we need, we then go to the framework and say what is the process for standards development. That process needs to be inclusive. It needs to be inclusive of other federal agencies like NIST. It needs to be inclusive of stakeholders. It needs to be inclusive of standards development organizations, the profession and all the many voices that are interested in our standards work. But ultimately it is not a standards-driven process, it is a health care-driven process, and we are

trying to put in place the requirements for records to make them tools to improve the health and safety of the population.

Chairman WU. Thank you.

And Ms. Roberts, you mention in your testimony that NIST is working with Health and Human Services' Office of Civil Rights to develop baseline security configuration checklists as well as conducting outreach and awareness about security challenges for health IT. Can you focus down on the specific challenges for smaller practices in implementing these security regulations?

Ms. ROBERTS. Yes. One of the things, the very first thing that a small practice needs to do is a risk assessment to determine what the risk is in the environment that they are in and then based on their risk assessment they can choose which security controls they would need to put in place in order to meet the security requirements spelled out in the security rule. So it is sort of graduated. If the risk is fairly low, then they don't have as many controls they need to put in place but larger practices have more risk and they will have to put more in place.

Chairman WU. Thank you very much.

Mr. Smith, five minutes.

Mr. SMITH. Thank you, Mr. Chairman.

I am wondering if any of our witnesses could comment on how perhaps consumers could be empowered through health IT. And I understand we want to maintain privacy but I think that consumers, if they become patients, would be empowered and I think more effective in managing their own health care, perhaps assuming better health habits and so forth through health IT, and if anyone would wish to talk about that.

Dr. GIBSON. Yes, I would like to address that. I think that electronic health records really will allow patients to be much more involved in their health care than they are now because I believe ultimately they will have access to the full professional record, not a diminished record that has only part of it. Ultimately they will have access to all their laboratory results, diagnostic imaging reports, problem lists, medication lists, allergy lists. They will be looking at the same data that their providers look at, and with the use of the Internet so that they can bone up on what the professional diagnoses are, I think they will come to the table saying, you know, I have read about this, I have concerns about how this treatment might affect my lifestyle and that sort of thing. So we are quite looking forward to having patients more on an equal footing with their providers because of the spreading of electronic data into the home.

Ms. MCGRAW. The law has always required providers to provide patients with a copy of their health information if they ask for it but Congress took some significant steps forward in that regard to make sure that happens by being very clear when a provider has an electronic health record, that copy has to be electronic, and then with respect to the Meaningful Use criteria, there are a number of provisions that are required for Meaningful Use that involve sharing data with patients, and not just when they ask, but giving them a discharge summary, for example, and instructions and a summary of their care, and I suspect that in stage 2 this will be enhanced even more. And the other thing that Congress did was

to say not only can you get your electronic copy of your record, but if you want your provider to send it to your personal health record if you have opened up one of those either because the provider gave it to you or your health plan sponsors one or you signed up for one from an Internet company like Microsoft or Google. So I completely agree with you and it is absolutely privacy enhancing to give people copies of their data. It helps to reduce errors because patients catch them.

Ms. BASS. I would like to comment on real-life examples that we have seen in Omaha. We have had an operational HIE now for over 18 months and throughout the State of Nebraska, not just Omaha. Our opt-out rate—we are an opt-out platform. The opt-out rate has been anywhere between one and a little over three percent of the general population. I think Nebraska has been viewed as somewhat of a conservative state, so I think that speaks well to how well the consumer is anxious to have this opportunity. Many times when we educate them about their decision that they make at this point, at the point of care, their comment is, so if I sign up for this, I am not going to be handed the pencil and clipboard every time I see my physician. I can say it is interesting how many times that comment is made.

I also have had situations, and I think sometimes we think it is a generational thing that the older generations are more concerned versus the younger generation are very interested in having this information. I have had elderly individuals that come to the office, and my receptionist will call me and she will say there is one of those individuals out there. They had opted out of the system and then they educated themselves and they were adamant to be back into the system and they asked me how long will this take for you to do the processing, and we have made it difficult. Once they have opted out, we make it difficult for them to get back in. But they want to know how long is it going to take for me to get back into the system now that I understand what this is all about.

Mr. SMITH. Okay. What about then connecting the care and consumer, their own detection of perhaps what might be necessary or even with the advice of their provider tying that to the financing? I think that there is not—anecdotally, I think that there is not enough access to the dollars associated with the care over the phone. I mean, when you have providers say well, we don't provide that over the phone. Is there any way we can tie that in? I mean, I would think there would be less concern about—but still we need to be sensitive to the privacy issues but to involve consumers more in the financing of their care, whether it is third-party payer or not.

Ms. BASS. I can go on to comment about some of these real-life examples. One of the individuals that came to the office that insisted to be opted back in as soon as possible had just had to experience a second round of testing because he left one health system and went to another health system, and he received a bill for that, and he said so I understand if I sign up for this, this is not going to happen any longer, and we said yes. He got it. And I think there are many out there that as we are having to pay for more and more of our health care costs are becoming much more aware of what it costs and duplicative tests and how to avoid them.

Mr. SMITH. Okay.

Ms. SENSMEIER. I would just like to speak to the standards aspect of that. There are standards available from the HITSP work products for consumer empowerment which would enable their personal health record data to be exchanged with the electronic health record, so work is there to support your concerns.

Mr. SMITH. Okay. Thank you.

Chairman WU. Thank you very much, Mr. Smith.

Dr. Gibson, you noted in your testimony that implementing EHRs is somewhat stressful for physicians, particularly in small practices, and that further, it is essential that we are able to transfer patient information as easily as fax machines accomplish that transfer today. What are the biggest challenges in making this data transfer that easy for physicians, particularly in small practices?

Dr. GIBSON. The technology needs to be such that the provider himself or herself or their staff can do it directly, that they can do it without perhaps having a health information exchange in their local or regional area, and that is the key point. If an electronic health record for a small practice is going to exchange with a health information exchange, that electronic health record will still need to export those data, and the point of my testimony is just let us make a requirement that electronic health records can export and import those data directly because most care occurs among providers who are known to each other so if you are in John Day, Oregon, your family doctor and perhaps a surgeon are likely to be in the same town. They are going to be known to each other and to the patient and so the need is for the office of the family doctor to be able to send the records to the surgeon without requiring that the State of Oregon provide a health information exchange. We will, ultimately. So my comments address the shorter-term need of saying let us require in the next round of standards that the EHRs have to do it so you just put in the address of the receiving provider and then it is done without requiring a third party to intervene.

Chairman WU. Thank you very much.

Ms. McGraw, there is a lot of personal data openly available today and we deidentify some of that data. You addressed the reidentification phenomenon and potentially the need to impose some sanctions for reidentification. Can you unpack that set of ideas a little bit for us? This is a hot issue for us.

Ms. MCGRAW. Yeah. I rushed through it a bit. So we have a standard in the HIPAA privacy rule for data deidentification and there are two prongs to it. One is what is called a safe harbor because it is fairly easy for people to implement. There are 19 different common identifiers that you must strip out of the data in order for it to qualify as deidentified, and it doesn't mean that it goes down to zero risk of reidentification but the risk is supposed to be very small. And then the other mechanism, if you want to be able to leave some identifiers in like dates of service, for example, which are often needed in research but other identifiers are not. So you can use a statistician and they can do their math magic to make it so that it meets the same standard of having a very low risk of reidentification. So that is already in the law.

The problem I think is, number one, the safe harbor was created more than five years ago and now, as you mentioned, Chairman Wu, there is a lot of other personal information widely available on the Internet and with respect to reidentification, the risks are about what the recipient might have access to in order to connect the dots and put that data set together in a way that makes it possible to reidentify individuals. And so we tend in the law to treat deidentified data as though it has reached some sort of holy grail moment of posing no risk at all regardless of who gets it or what data they have access to. So we need to rethink the standard. I think that is what HHS is focusing on now at the direction of Congress. But even if we tighten the standard as much as we possibly could, to still make that data more widely available as it has lots of important purposes both in health care as well as in business analytics. If in fact that data goes to an entity who then reidentifies it, puts two and two together, we don't right now have a mechanism in the law to reach them to say you weren't supposed to do this. Right now, you would hope that entities when they release the data actually contractually require the entities not to reidentify it, but even that if it happens, because it is not required to happen, that is the extent of accountability is only through that contract and usually only the contracting parties, not law enforcement or governmental authorities or even an individual under a private right of action.

Chairman WU. Does anyone else want to comment on this reidentification problem?

Dr. BLUMENTHAL. Mr. Chairman, it is very much on our minds as we go forward at the Office of National Coordinator. We do have a study that is ongoing. I think we are going to have to look at the science of deidentification and identification, if you will, and come to a consensus on what level of risk we can tolerate for reidentification and then what level of removal, what kinds of removals of information are required to get to that level of risk, and that is going to require that we continually look at the Internet and the information that is available, and it is not going to be a one-time judgment. It is a judgment that we are going to have to continue to make based on how the technology advances. But it is something that we recognize is critical to assuring public trust and enabling some of the most valuable uses of information to go forward.

Chairman WU. Thank you. Earlier we had a sidebar discussion about proper compensation for Meaningful Use. There will be compensation for Meaningful Use from Medicare and Medicaid. To what extent would compensation from private insurers be helpful in the uptake of health care information technology?

Dr. BLUMENTHAL. We think, at the Office of National Coordinator, it would be extremely valuable. The Federal Government does pay for probably 40 percent, roughly, of the health care bill but there is another 60 percent that benefits from the availability of health information technology. In August we actually worked with some of the major insurance companies to help to get them to agree to begin to incorporate meaningful use in their pay-for-performance programs. So United Health Care, Aetna, and Wellpoint all agreed that they would start to look for Meaningful Use as an indicator of either high performance or quality improvement and

United Health Group said that they were going to launch a pilot project to make loan funds available in two states for physicians who want to adopt electronic health records.

Chairman WU. And how much of a bump are the private insurers considering for Meaningful Use?

Dr. BLUMENTHAL. You mean how much are they willing to put on the table? I think that remains to be seen. We are going to keep working with them. We are actually going out to meet with the Blue Cross Association in a month or so to talk about the same issue. What I can assure you is that we will continue to work with them to try to make sure or try to assure that their contribution is a meaningful contribution.

Chairman WU. Ms. Bass.

Ms. BASS. Thank you, Chairman Wu. I would like to comment on this as well. Blue Cross Blue Shield of Nebraska has been a significant player in the implementation of HIE and they currently pay a license fee of $25,000 a year plus a dollar per member per year and we are talking about increasing that levy to $1.50. So they have been an active participant but I will tell you that we have also met with the other providers or the other payers in the State of Nebraska and they are somewhat hesitant to play a role in this, and their answer, understandably so, is that we deliver health insurance on a national perspective so we are looking for a national strategy versus having to accommodate state by state. So again, to be able to help us find a way around that obstacle, it is critical that we have them participate.

And then to go back to your previous point about the deidentified/reidentified data, that was a huge issue for us as we developed our privacy and security policies, and hence—we were talking about this prior to the HITECH Act. So originally we were designed for treatment and payment purposes only, but even to this point in time we only provide eligibility verification for Blue Cross Blue Shield and it is because of this fear of reidentification, and we have excluded all research for that fear.

Chairman WU. Thank you.

Dr. Gibson, my understanding is that there is a private insurer in Portland, Oregon, which provides some compensation for use of health information technology to private providers. Can you tell us something about that?

Dr. GIBSON. I am sorry. I am unaware of that. I am sorry I am not able to contribute. Can you give more——

Chairman WU. I think it is the Providence Group. I am not completely confident of that.

Dr. GIBSON. Okay. That they would provide funding for sharing of health information? Yes.

Chairman WU. That is, if the record—if reimbursement is submitted to Providence, that Providence would provide a small bump in the reimbursed amount.

Dr. GIBSON. Oh, the Providence health plan does provide—I apologize, Chairman Wu. You are absolutely right. Providence health plan does provide—give extra one percent payment to physicians if they have an electronic health record. Absolutely. Thank you for reminding me.

Chairman WU. It is one percent?

Dr. GIBSON. One percent.

Chairman WU. Thank you very much, Dr. Gibson.

Dr. GIBSON. Thank you.

Chairman WU. Mr. Smith, do you have any further questions?

Mr. SMITH. Just one briefly.

Dr. Blumenthal, it is my understanding that some large organizations, health care organizations, kind of are early adopters and they have been innovative. How do we dovetail what they have already done and how do we take that into account, you know, without rendering the progress that they have made useless or certainly the expenditures that they made worthwhile?

Dr. BLUMENTHAL. Well, fortunately, though the United States lags behind most of the western world in its adoption and use of information technology in health care, there are some large organizations that are leaders in the United States and I think are as far along or further along than any place else in the world, and these are organizations whose names we would all recognize, places like the Mayo Clinic and the Cleveland Clinic and Intermountain Health Care in Salt Lake City, and so that is good news. They will, because of their farsighted investments, be eligible for Meaningful Use compensation just as any other organization would be. We are trying to take advantage of the lessons they have to learn—they have to teach, and we certainly engage them. We engage them in our Policy Committee. We have representatives from Intermountain on our Policy Committee, for example, as well as from the Rankin Street—on the Standards Committee, someone from the Rankin Street program which is in Indianapolis, which is another leader in health IT. So we take advantage of their input on an almost daily basis in terms of our policy development.

Our learning—our effort to enhance the adoption of health information technology works to a large degree through a program called the Regional Extension Center Program. This is a program that is actually modeled on the USDA Agriculture Extension Program, and its goal, if I can sort of over-generalize and over-simplify, is to bring the latest information technology of the family doctor the way the U.S. Agriculture Extension Service brings technology to the family farm. That group, that program is oriented towards small practices and underserved areas including rural areas and to critical access hospitals. Now, they will be trying to channel the lessons that have been learned elsewhere in our health system to make them available to the least well-resourced, least IT-sophisticated members of the health care community, and that is why we have focused them on small primary care practices in underserved areas and critical access hospitals, but they will create learning communities that we hope will take advantage of the latest progress that has been made.

Mr. SMITH. And then very briefly, we have heard a little bit about the ARRA funds, they are going to go away, and Dr. Blumenthal, can you speak to how that might be addressed long term? I mean, can we achieve a lot with a one-time expenditure as opposed to maintaining the need for a budget line item in perpetuity?

Dr. BLUMENTHAL. Well, one way to think about the ARRA funding is as a pump primer, so ultimately the use of health informa-

tion technology in my view is a part of the business of health care and it should be a private sector responsibility. I think the investment that the Congress and the Administration have made was meant to correct a market failure which stemmed from the fact that we don't sufficiently reward providers for care for high performance, lower cost, higher quality. We pay them by piecework whether it is a high-quality or high-cost product or a low-quality product. So there wasn't an incentive to pay the money that is required in order to get health information technology so I think we needed to prime the pump.

We will very soon, I think, see that it becomes an essential part of providing care to the American people, one that physicians, nurses, health care institutions don't feel they can afford not to have, and at that point I think the Federal Government and my office can pass the baton to the professional community, to the hospitals, the nurses of the country, and the market will take off and do its own work for the American people.

Mr. SMITH. Okay.

Dr. GIBSON. I thoroughly agree with Dr. Blumenthal. If you survey providers a year after they have gone on an EHR, 90 percent of them say they would never go back to paper, so they realize the benefits. It is that intervening year that I think that the priming of the pump that Dr. Blumenthal's office and CMS have provided for is adequate to the degree that it will stimulate doctors to switch over. Once they get over, there will be a network effect. They won't be able to communicate as easily with their colleagues without an electronic health record. I think that consumer pressure will be such that, "gee, doctor, don't I have access to your records; if not, why not?" So I believe that that will take over and I don't see a longstanding line item in the budget for this.

Mr. SMITH. Ms. Sensmeier?

Ms. SENSMEIER. Yes. Another thing to note is, since 1994 HIMSS has sponsored the Davies Award, which awards organizations and public health systems, community health organizations and private practices for implementing electronic health records, and it is notable that they all identify the return on investment for them. I mean, it is certainly a huge investment up front but at the end they have improved their processes and really all of them have achieved cost savings, so that is noteworthy as well. And two of them are from the State of Oregon, two of the winners, Chairman Wu.

Mr. SMITH. Ms. Bass.

Ms. BASS. Thank you. We take that call from the ONC to be sustainable within four years very seriously, and we are already beginning to see some of the opportunities just as the web services came from the World Wide Web, we are beginning to see HIE services, and I visited with a group this morning about some of the things that we are doing to be able to generate revenue, and I can go into detail on some of those but we are very confident that we will be seeing many opportunities to create revenue through the health information exchange.

Mr. SMITH. Okay. Thank you, Mr. Chairman.

Chairman WU. Thank you.

Many of you traveled long distances and also spent a lot of time and energy preparing your testimony, and I want to give you all an opportunity to add anything to your testimony that we have not asked about today.

Dr. BLUMENTHAL. I just want to express my gratitude to the Congress for putting in place the HITECH Act. I think it is a superb piece of legislation that as I have gotten to know it and trying to implement it, I have been impressed at how it addresses almost all the major issues that we need to address with respect to the implementation of an electronic health system in the United States. That is not to say it is going to be easy but I think you have given us a great start. So my appreciation to you and your colleagues.

Chairman WU. Thank you, Dr. Blumenthal.

Anyone else?

Ms. ROBERTS. I would like to echo his comments as well as to thank the Committee for recognizing NIST's role in health IT and ensuring that we are involved as a partner with ONC in making this go forward. Thank you.

Chairman WU. We appreciate NIST's work.

Ms. Sensmeier.

Ms. SENSMEIER. Thank you, Chairman Wu. I just would like to briefly go back to your comments on the workforce and I want to emphasize how important that is, and also recognize the role of nurses in this process. It is often a silent voice, and there are 3.1 million of us out there and there are approximately 9,000 informatics nurses working in the United States helping to implement and lead these projects. So it is critical work and I appreciate the support that you have put to the workforce efforts in making sure we all have the competencies for informatics we need to do this work.

Chairman WU. Thank you very much.

Dr. GIBSON. I also would like to commend Congress for the HITECH Act, the Meaningful Use final rule, and the remarkable cooperation between the Office of the National Coordinator and the Centers for Medicare and Medicaid Services who have brought order out of chaos within electronic health records. We now see where we need to go. I think it will be very challenging to get there. I also want to state that I believe that this information technology is crucial in terms of bringing down health care costs in the long run. We are not the answer. We are an enabling technology that ultimately will allow all the care to be subject to review and comparison to national scientific standards, and I think it will be a useful technology in the long run as we work on the challenging problem of health care and health care cost and quality. Thank you for allowing me to testify.

Chairman WU. Thank you very much.

Ms. McGraw.

Ms. MCGRAW. I feel like I got some good opportunities to speak so I don't have anything to add but I am happy to follow up with additional information such as ideas about the deidentification/reidentification issue, the security issues I raised and anything else in my testimony.

Chairman WU. Thank you.

Ms. Bass.

Ms. BASS. I too would like to echo, thank you for the work that you have done. It has been outstanding.

One point I do want to make when we are talking about enabling EHR to talk to other EHRs to be aware of the interface fees that can be obstacles, and I just wanted you to be aware of that piece of information. Also, I would like to close with the fact that I too was a registered nurse for 20 years before I went into technology, and I am very thankful that because of the work you are doing, people are no longer asking me what technology has to do with nursing. Thank you.

Chairman WU. Thank you very much, and thank you all for appearing before the Subcommittee this afternoon. The record will remain open for two weeks for additional statements from Members and for questions to any follow-up questions the Committee may ask of the witnesses. The witnesses are excused and the hearing is adjourned. Thank all very, very much.

[Whereupon, at 11:31 a.m., the Subcommittee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. David Blumenthal, National Coordinator for Health Information Technology, Office of the National Coordinator, U.S. Department of Health and Human Services

Questions submitted by Chairman David Wu

Q1. As your testimony describes, there are many health IT implementation activities currently occuring around the country. Could you please describe how the standards needed for all of these initiatives, such as state and national health information exchanges and meaningful use, are being coordinated by the Office of the National Coordinator?

A1. The Health Information Technology for Economic and Clinical Health (HITECH) Act includes several sections that authorize the Office of the National Coordinator for Health Information Technology (ONC) to coordinate standards activities and, in so doing, assure that meaningful public input is obtained.

The HITECH Act established two Federal Advisory Committees (the HIT Policy Committee and HIT Standards Committee) from which we regularly seek recommendations. Each committee plays a specific role with respect to standards coordination. The HIT Policy Committee is charged with recommending the areas in which standards, implementation specifications, and certification criteria are needed for the electronic exchange and use of health information as well as a priority order for the development, harmonization, and recognition of standards, implementation specifications and certification criteria. The HIT Standards Committee is charged with recommending to the National Coordinator the standards implementation specifications, and certification criteria developed for the electronic exchange and use of health information. It is also responsible for recognizing harmonized or updated standards from an entity or entities for the purpose of facilitating the achievement of uniform and consistent implementation of such standards and implementation specifications. Finally, once HIT Standards Committee recommendations are issued to the National Coordinator, the HITECH Act requires that the National Coordinator must determine whether to endorse each standard, implementation specification, and certification criterion recommended for the purposes of adoption by the Secretary under section 3004 of the Public Health Service Act.

Among these activities and within this statutory context, ONC has also recently developed and established the Standards and Interoperability Framework (the Framework) to proactively identify areas requiring standards harmonization, development, and coordination across the many activities in which we are engaged.

The Framework seeks to implement a coordinating process that is inclusive of SDOs, the provider community, and the public with the purpose of developing and harmonizing standards and specifications. The Framework supports the coordination of standards from the identification of a particular challenge requiring new or harmonized standards, to the testing and certification criteria that are necessary to ensure compliance with those standards.

Each step in the Framework is meant to engage affected and relevant stakeholders to assure full participation and involvement from qualified, knowledgeable resources. This is especially important in working with healthcare standards, which in most cases have been developed by collaborative processes external to the Framework and which have a cumulative body of knowledge to draw from.

Q2. What efforts is the Federal Government involved in to help coordinate and align U.S. health IT standards with those used internationally?

A2. ONC has been regularly involved in international health IT standards coordination meetings with leadership from a number of countries including Canada, the UK, and Australia. Earlier this month, ONC staff participated in a meeting convened in Cambridge, MA by Health Level 7 International (HL7) to discuss standards development and coordination.

Across our international partners, there is an interest in finding commonality in health IT standards, and significant progress has been made, including the widespread adoption of international standards such as the Systematized Nomenclature of Medicine – Clinical Terms (SNOMED). SNOMED originated as a U.S.–England collaboration, but is now maintained by The International Health Terminology Standards Development Organisation (IHTSDO). This summer, the IHTSDO announced an agreement with the multi-lateral World Health Organization (WHO) to integrate SNOMED into the WHO's international classification of disease (ICD) terminology.

Additionally, ONC is supporting, along with the Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA), a US-led Secretariat to the technical advisory group (TAG) for ISO TC 215, the international standards organization for health care standards.

Q3. You mentioned that ONCHIT is working on a study regarding the de-identification of private data. When will this study be published?

A3. The draft report associated with the study was recently submitted and is currently under review by ONC and the HHS Office for Civil Rights, because of its relevance to the HIPAA Privacy Rule. Given that the report may require further revisions in response to questions and comments from our respective offices, we cannot, at the present time, predict a specific publication date for the report. We do, however, intend to make it publicly available as soon as possible. We would be happy to furnish your staff and the committee staff with a copy of the final version of the report as soon as one becomes available.

Questions submitted by Representative Paul D. Tonko

Q1. CMS has announced that it will promulgate regulations for the HITECH Act in three stages. Stage 1 measures focus on capturing and sharing data. Stage 2 will target advanced care processes with clinical decisions support services. Stage 3 will concentrate on improving health care outcomes. It appears that results from Stage 1 will heavily influence the regulatory process in later stages.

A1. CMS received numerous comments from providers, advocates, and Congress on the proposed rule for the Medicare and Medicaid EHR Incentive programs which included Stage 1 of meaningful use. We carefully evaluated these comments and tried to accommodate concerns in a way that provides flexibility for providers while moving forward on the adoption and meaningful use of certified EHR technology. During future rulemaking for the other Stages, we plan to take a similar approach to engage stakeholder input as well as take into account our experience and results from Stage 1.

For Stage 1 measures, we worked to meet the statutory objectives of improving the quality of health care, reducing medical errors, reducing health disparities, increasing prevention, and improving the continuity of care among health care settings. Further, we identified core objectives that are both patient-centered and crucial to laying the foundation for obtaining value from meaningful use. For example, providing electronic copies of health information to patients will not be useful if the copies do not contain basic information such as a problem list, medication list, or allergy list.

We provided some possible specificity about Stage 2, but will not finalize details about other stages until later rulemaking. There are two reasons for this.

1. We want to get results from Stage 1 to help us determine if the requirements that we have set are appropriate.
2. Many of the requirements for later stages will be dependent on infrastructure improvements that are anticipated over the next several years due to HITECH funding.

Q2. How does CMS/HHS plan to measure physician progress and challenges associated with implementing Stage 1 before moving to alter stages? Will CMS/HHS gather data from a range of physician stakeholders before implementing later stages?

A2. ONC is taking a number of actions to gather input from physician stakeholders. First, ONC's Office of Provider Adoption Support—in collaboration with the ONC funded Regional Extension Centers—has launched the Meaningful Use Vanguard (MUV) program, identifying providers who are committed to leading the way in meaningful use of certified EHR technology. The program is designed to support feedback mechanisms for Stage 1 implementation, future stages, and monitoring the general progress and barriers of the program. ONC will provide quantitative and qualitative data collected from MUV to the HIT Policy Committee, as that federal advisory committee deliberates and makes recommendations to the National Coordinator for Stages 2 and 3. Second, ONC is undertaking a new survey effort in cooperation with the National Center for Health Statistics to obtain information from a nationally representative set of physicians at various stages of EHR adoption about the barriers to and benefits of achieving the Stage 1 meaningful use criteria. Finally, Dr. Blumenthal has personally undertaken a set of outreach efforts, meet-

ing with professional groups across the country to hear about their progress and challenges.

CMS is working to educate providers about the EHR incentive program and meaningful use, and tailoring outreach efforts based on the questions received from stakeholders. CMS has posted over 100 frequently asked questions and answers on its website, and will soon be posting meaningful use specifications for each meaningful use measure to further educate providers on all of the objectives. CMS will also be monitoring the participation in the Medicare and Medicaid EHR Incentive Programs, to determine if particular segments of the provider community such as certain physician specialties or geographic locations are having more difficulty registering or successfully demonstrating meaningful use. This data will enable CMS to target its outreach efforts strategically. Through the attestation data that CMS will begin collecting in April 2011, they will be able analyze if some of the measures are more challenging to achieve than others. Both CMS and ONC intend to fully leverage all available data collected as well as program experiences with implementing stage 1 for purposes of informing later stages of meaningful use criteria.

Questions submitted by Representative W. Todd Akin

Q1. A number of traditionally hospital-based physicians are eligible for incentives under the HITECH Act program. Some of these physicians are concerned that the rules and the "meaningful use" requirements released to date don't necessarily apply to the way they actually practice or use electronic health records. What are the plans to ensure that hospital-based physicians, such as anesthesiologists, pathologists and radiologists, who are deemed eligible for the incentives, are able to successfully participate in the program?

A1. The Medicare and Medicaid meaningful use incentive programs final rule conforms to the Continuing Extension Act of 2010 which addresses provider concerns about hospital-based providers in ambulatory settings being unable to qualify for incentive payments by defining a hospital-based eligible professional (EP) as performing substantially all of his or her services in an inpatient hospital setting or emergency room only. Hospital-based EPs are those who furnish 90 percent or more of their covered professional services in a hospital inpatient setting, or hospital emergency department and thus are not eligible for incentive payments.

CMS understands the scope of the Medicare and Medicaid EHR incentive programs is vast and that doctors and hospitals across the country have varying degrees of awareness of EHRs and of the program. As a result, CMS is conducting wide-scale outreach to educate those eligible for the program—hospitals and eligible professionals, as well as States, and provider stakeholders. Outreach has already started and will continue for the coming months and years to prepare and encourage participation by all who are eligible. Some accomplishments and plans to date include:

- CMS conducted awareness tracking among potential participants to gauge levels of knowledge and inform outreach efforts. This tracking will continue as the program launches.
- CMS established a specific website for the program on cms.gov and are actively promoting it through all related communications channels reaching these audiences. This website provides detailed information about eligibility, requirements, how to participate, and more in digestible portions to assist providers with learning and understanding the information. This website will continue to grow with content and tools for providers to learn about the program.
- CMS facilitated, in conjunction with ONC, a bi-weekly hospital and provider stakeholder call to share information and receive feedback from the field. The stakeholders are committed to helping in the educational effort of their constituents.
- CMS continues to conduct training for multiple audiences, including rural providers, through open door forums, CMS-hosted trainings, presentations at key conferences and webinars, partnering with ONC both at the national and local levels.
- HHS is actively engaging its 10 Regional Offices to promote and educate on the program through local activities and collaboration with the States and ONC Regional Extension Centers.

In the coming months surrounding the launch of the programs, we will be promoting the program through both traditional and non-traditional media as well as

introducing an Incentive Program Information Center to assist those participating in the program and to answer their questions.

Questions submitted by Representative Paul C. Broun

Q1. As a primary care physician with over three and a half decades of clinical experience, I understand the importance a patient's laboratory data has towards a proper patient diagnosis. This laboratory data is essential to many of the quality measures in the Final Meaningful Use rule (rule). How have you addressed the funding challenges between the necessary interfaces of laboratory information systems, where pathologists house patient laboratory data, and Electronic Health Records (EHR)? In particular, smaller laboratories need financial assistance in acquiring these interfaces, which at this time, only large national laboratories can afford.[1]

A1. The ability to electronically receive laboratory test results is an important tool for improving patient care and we recognize that certain financial and technical challenges need to be overcome to realize all of the benefits that this HIT can provide. We are engaged in several efforts that we hope will help tip the scales and lower the costs and barriers to obtaining and implementing laboratory interfaces. Our Regional Extension Centers are working with health care providers to help them become meaningful users and in doing so are providing training and support services related to EHR adoption; offering information and guidance to help with EHR implementation; and giving technical assistance as needed. A primary focus of this activity is working with providers and EHR vendors on implementing interfaces, with an immediate priority on lab interfaces. The state health information exchange grantees are working and partnering with both national and smaller independent labs on several fronts:

- Gaining participation of clinical laboratories in health information exchange networks so that providers can receive lab results from several labs with a single interface.
- Providing financial and technical support to independent and hospital labs to defray the costs of establishing laboratory information system interfaces.
- Advancing adoption of LOINC standards through translation and validation services and value sets, to make it easier for providers to incorporate and use labs results in EHRs.

Finally, the Nationwide Health Information Network Direct project we are leading is developing technical specifications and reference implementations that we also anticipate will lower the cost of establishing interfaces.

Q2. Given the rule's numerous measures that eligible health care providers must meet to receive EHR incentive funding and prevent financial penalties after 2015, how will you deal with eligible health care providers who regrettably fail to meet the rule's numerous required measures? For example, some pathologists who practice outside of a hospital may be eligible for funding, but they do not evaluate some of the measures included in the final rule due to not having direct patient contact that most of the rule's measures envision.

A2. In accordance with the statute, eligible health care providers must be able to demonstrate meaningful use of certified electronic health record (EHR) technology by 2015 in order to avoid negative Medicare payment adjustments in future years. While the Medicare and Medicaid EHR Incentive Programs have similar reporting requirements, the Medicaid Incentive Program does not include payment adjustments for eligible professionals and hospitals who are unable to successfully demonstrate meaningful use.

The use of EHRs among eligible health care providers varies greatly by specialty, and CMS understands that not all measures will apply to all providers. The requirements of meaningful use for Stage 1 have been adjusted to be more flexible based upon comments received during the rulemaking process. The measures have been divided into a core set and a menu set. Where it may be impossible for an eligible professional (EP) or eligible hospital to meet a specific measure, an exclusion is defined in the final rule. If an exclusion applies to an EP or eligible hospital, then such an EP or eligible hospital does not have to meet that measure in order to be

[1] See page 4, bullet point 6 in the attached March 15, 2010 Small Business Administration, Office of Advocacy letter to Charlene M. Frizzera, Acting Administrator of the Centers for Medicare and Medicaid Services.

determined a meaningful EHR user. For instance, if an EP such as a pathologist writes fewer than one hundred prescriptions during the EHR reporting period, then the EP would be excluded from meeting the measure associated with electronically prescribing medication. Added flexibility also allows eligible providers to defer reporting on up to five menu set measures.

The requirements for meaningful use for Stage 2 and 3 of this program will be set through open and transparent rulemaking. Consideration will be given to public comment from stakeholders during future rulemaking. HHS anticipates the need to make changes into account to the overall HIT infrastructure and lessons learned from Stage 1 implementation for implementing future stages of the program.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Kamie Roberts, Associate Director for Federal and Industrial Relations, Information Technology Laboratory, National Institute of Standards and Technology

Questions submitted by Chairman David Wu

Q1. You testify that NIST is heavily engaged in usability research. What are some of the challenges currently associated with usability? How does NIST establish the priorities for this research? How does NIST ensure that the research is utilized?

A1. Usability is fundamental to the adoption of health IT. It enables users—in the case of healthcare clinicians and consumers alike—to use products quickly and easily to accomplish their goals. Usability of health IT systems can offer efficiencies of scale in improving healthcare and reducing disparities, and enable more effective use of information technology to improve health and maintain wellness.

Challenges in achieving usability in health IT systems include: designing systems to support tasks, not complicate them, so that clinicians can focus on their patients; designing effective user interfaces that reduce complexity of operations and training time; establishing consensus based usability standards with quantifiable test methods to assess compliance with the standards; and, determining specific objective pass/fail criteria for usability certification.

NIST sets priorities for this research by collaborating with and receiving input from many individual stakeholders in the public and private sectors, including Federal agencies, standards development organizations, professional societies and nonprofit organizations, academia, healthcare delivery organizations, industry, and consumers. Extensive input from these parties was critical to the NIST-led development of a usability road map focusing on R&D priorities. Recently, NIST, the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ) held a workshop to further refine the road map by determining a prioritized list of short, medium, and long-term strategies to improve usability of electronic health record (EHR) systems.

To help ensure that the usability research is utilized, NIST is providing stakeholders with focused guidance on usability and accessibility, such as methods for building usability into product design and development from the beginning. NIST is also disseminating the research outcomes broadly to the stakeholder community through workshops, publications and presentations at key health IT meetings and conferences. In addition, NIST's collaborations with the ONC will enhance development of data on usability in the event that certification criteria in this area are considered in the future.

Questions submitted by Representative W. Todd Akin

Q1. A number of traditionally hospital-based physicians are eligible for incentives under the HITECH Act program. Some of these physicians are concerned that the rules and the "meaningful use" requirements released to date don't necessarily apply to the way they actually practice or use electronic health records. What are the plans to ensure that hospital-based physicians, such as anesthesiologists, pathologists and radiologists, who are deemed eligible for the incentives, are able to successfully participate in the program?

A1. NIST's efforts focus on enabling adoption of health IT by accelerating standards development and testing efforts within the health IT domain. Questions related to the meaningful use criteria and physician incentives are under the purview of the Department of Health and Human Services.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Joyce Sensmeier, Vice President, Informatics, Healthcare Information and Management Systems Society

Questions submitted by Chairman David Wu

Q1. In your testimony, you note that "data transport and basic security are focus areas where selected standards [for meaningful use] are missing," and that having these standards available would make it much easier for vendors to prepare for phase two of meaningful use.

Has the Office of the National Coordinator, or any other body, developed a standards roadmap, that would help software developers and device makers build products that meet future requirements? Would such a roadmap or guide be beneficial?

A1. We are not aware of a publicly available national standards roadmap or guide. We do agree that such a roadmap would help software developers and device makers build products that meet future requirements. A standards roadmap would also allow the industry to work in a coordinated effort to plan future software development cycles and implement standards in a manner that builds on a consistent foundation to more advanced capabilities.

However, we would like to clarify that when we stated "data transport and basic security are focus areas where selected standards [for meaningful use] are missing," we were not saying that there are standards gaps, or that additional standards need to be developed for these focus areas. Many data transport and basic security standards are already published and available; they simply need to be selected by CMS and ONC for future stages of meaningful use and certification criteria.

Q2. Included in the NIST FY2011 budget request is a $10 million initiative for Standards and Conformity Assessment for Interoperability in Emerging Technology. What level of funding do you believe is necessary to support NIST's health IT activities? If more funding were available, what priorities would you recommend to support standards for interoperability and related measures?

A2. Without knowing what requirements are included in the NIST FY2011 budget request, it is difficult to suggest a necessary level of funding. However, priorities for this funding should address the need for a broad and extensible test infrastructure which is critical to ensure standards-based interoperability between health IT applications. This infrastructure should include a modular, web-based testing environment that provides a variety of conformance and interoperability testing services to support instance validation testing, isolated system testing, and peer to peer system testing.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Dr. Richard Gibson, President, Oregon Health Network

Questions submitted by Chairman David Wu

Q1. The meaningful use criteria require that providers do a risk assessment to gauge the appropriate level of security they will need for their health IT systems. What type of experience do physicians have in performing security risk assessments? What resources exist to help them?

A1. Most small physician practices have no experience in performing security risk assessments. Larger physician offices could possibly already have someone on their staff familiar with IT security risk assessments especially if they are currently supporting their own in-house electronic health record. Even in the larger physician offices, they are likely to be rusty on risk assessment skills. With a checklist provided by a Regional Extension Center or by their specialty society, an experienced staff member might be able to carry out their own security risk assessment for that larger physician office. Smaller physician offices are unlikely to be able to perform this assessment without significant help. Perhaps a small physician office could perform their own security risk assessment if they were provided a plainly written, nontechnical, detailed checklist with full explanations of each risk topic. The staff member or physician could read the explanation of each question and be guided through how to indicate their level of risk on each topic. Generally, I am not aware that there are many resources currently available to help physicians with IT security risk assessments. It is certainly not a routinely advertised or discussed service among physicians. There is an opportunity for private firms to compete in offering a fixed price IT security risk assessment based on the size of the physician practice. I can envision many smaller and some larger practices taking advantage of this route as they might be uncomfortable making their own risk assessment.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Deven McGraw, Director of the Health Privacy Project, Center for Democracy and Technology

Questions submitted by Chairman David Wu

Q1. The meaningful use criteria require that providers do a risk assessment to gauge the appropriate level of security they will need for their health IT systems. What type of experience do physicians have in performing security risk assessments? What resources exist to help them?

A1. The security risk assessment required by the meaningful use criteria is essentially the same risk assessment required by the security regulations under the Health Information Portability and Accountability Act of 1996 (HIPAA). However, the Security Rule applies only to electronic protected health information. Consequently, providers who are adopting electronic health records for the first time have *no experience* in conducting these risk assessments. Further, providers who are upgrading existing systems may have little-to-no familiarity with the new, more advanced security features and functions present in certified EHR technology. Providers in small practices may not have the resources to hire in-house IT security professionals.

For these risk assessments to be effective, it is essential that providers perform them effectively. To help providers comply with the HIPAA security rule, there are written materials on the websites of both the Centers for Medicare and Medicaid Services (CMS) (which, until recently, enforced the HIPAA security rule) and the HHS Office of Civil Rights. These resources are a good start, but they are not sufficient to ensure that providers participating in the meaningful use program are actively implementing adequate security. Vendors of certified EHR technology should educate their provider customers on how to deploy the EHR security functionalities—but vendors are not a good, consistent source of support on how to comply with security laws, or to implement good security practices.

CDT has recommended that the Regional Extension Centers (RECs) established in the HITECH legislation provide hands-on assistance to providers to implement the security risk assessment. However, it is not clear that the Regional Extension Centers have the expertise to adequately take on this role. Also, given that providers need only attest that they have performed a security risk assessment, is unclear that the security meaningful use provisions will be much of a priority for the RECs. It will be important to monitor compliance with the security meaningful use provisions during Stage 1 of the program to ensure that consistent implementation of good security practices is a top priority.

Appendix 2:

Additional Material for the Record

LETTER TO CHARLENE M. FRIZZERA, ACTING ADMINISTRATOR, CENTERS FOR MEDICARE AND MEDICAID SERVICES, DEPARTMENT OF HEALTH AND HUMAN SERVICES, FROM SUSAN M. WALTHALL, ACTING CHIEF COUNSEL ADVOCACY, AND LINWOOD L. RAYFORD III, ASSISTANT CHIEF COUNSEL FOR FOOD, DRUG, AND HEALTH AFFAIRS, SMALL BUSINESS ADMINISTRATION, DATED MARCH 15, 2010, SUBMITTED BY REPRESENTATIVE PAUL C. BROUN

SBA Office of Advocacy
www.sba.gov/advo

Advocacy: the voice of small business in government

March 15, 2010

Charlene M. Frizzera
Acting Administrator
Centers for Medicare and Medicaid Services
Department of Health and Human Services
Room 309-G
Hubert Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

Centers for Medicare and Medicaid Services
Department of Health and Human Services
Attention: CMS-0030-P
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Medicare and Medicaid Programs; Electronic Health Record Incentive Program (75 Fed. Reg. 1844, January 13, 2010)

Dear Acting Administrator Frizzera:

On January 13, 2010, the Centers for Medicare and Medicaid Services (CMS) published the above-captioned proposed rule in the *Federal Register* implementing certain provisions of the American Recovery and Reinvestment Act of 2009 (Act) to increase the use of health information technology (HIT).(1)

Section 612 of the Regulatory Flexibility Act (RFA) requires Advocacy to monitor agency compliance with the RFA, as amended by the Small Business Regulatory Enforcement Fairness Act.(2) Congress established the Office of Advocacy (Advocacy) under Pub. L. 94-305 to represent the views of small business before federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such the views expressed by Advocacy do not necessarily reflect the views of the SBA or of the Administration.

As Acting Chief Counsel for Advocacy, I am submitting comments on this matter because this regulation is expected to have an impact on a signficant number of the health care providers and hospitals in this country, and because my office has been contacted by numerous health care providers and their representatives that are required to comply with various provisions of the Act. I believe there is merit to bringing the following comments to the attention of CMS as the vast majority of these entities are considered small pursuant to SBA size standard definitions.

I. Background

According to the proposed rule's preamble, the regulation would provide incentive payments to eligible professionals (EPs) and eligible hospitals (EHs) participating in Medicare and Medicaid programs that adopt and meaningfully use certified electronic health record (EHR) technology. The proposed rule provides the initial criteria an EP and EH would have to use in order to qualify for incentive payments designed to encourage EHR technology.

CMS states that the proposed rule will be economically significant and will have an impact on virtually every EP and EH and other affected health entities.(3) CMS believes that most EPs using EHR systems will require significant changes to achieve certification and/or the EPs will have to make process changes to achieve Meaningful Use (MU).(4) Per CMS there are approximately 624,000 healthcare organizations (EPs and eligible hospitals) that will be affected by the incentive program.(5) Also, CMS estimates that the incentive program will cost EPs approximately $54,000 to purchase a certified EHR and $10,000 annually for ongoing maintenance.(6) The agency estimates that it will cost eligible hospitals $5 million to purchase a certified EHR and $1 million annually for maintenance.(7) CMS rightfully states that for RFA purposes it is assuming that all affected providers are small based on SBA size standards.(8)

Advocacy commends CMS for appreciating the extent to which this rulemaking will impact the health care industry in the United States, and for complying with §603 of the RFA that requires agencies that conclude that a rule will have a significant impact on a substantial number of small entities to complete an Initial Regulatory Flexibility Analysis (IRFA). While CMS correctly included a discussion of alternatives in its IRFA (as required by §603(c) of the RFA), CMS asserts that it has no discretion with respect to the Act's provisions regarding incentive payments or payment reductions.(9) However, CMS believes it does have some discretion on how best to meet the requirements of the HITECH Act.(10)

My office has received several verbal and written communications from physicians, clinical laboratory health providers, and their representatives, who enthusiastically support the public policy underlying this proposed rule. However, they are concerned that some of the rule's provisions may result in unintended consequences that will have a significant negative economic impact on their professions. Advocacy encourages CMS to utilize its discretion and consider the alternatives/comments suggested by the stakeholders that contacted Advocacy concerning this rule. This will improve the transparency of the rule and result in encouraging health care providers to use EHR, which is consistent with the public policy underlying this regulation and the Act. Advocacy presents CMS with the following comments based on our review of the proposed rule and the concerns brought to our attention by affected stakeholders.

I. Physicians, through the American Medical Association (AMA), suggest that CMS is moving too aggressively in Stage 1 of the rule and that certain changes are needed that will minimize its potential economic impact on their profession.(11)

The AMA is particularly concerned that the aggressive implementation requirements of Stage 1 will have an especially negative impact on smaller physicians' practices, increasing the chance that they will not be able to meet Stage 1 incentive program measures. AMA's position is consistent with CMS' concern that some providers may have difficulty meeting the proposed rule's objectives.(12) As such, the AMA recommends that CMS should:

1. Remove the "all or nothing" approach that requires physicians to meet all 25 objectives and measures contained in the proposed rule, as well as the reporting requirements that involve the use of numerators and denominators particularly when it would involve manual data collection by the provider. In its place the AMA recommends that physicians should only have to meet 5 of the rule's 25 objectives and measures.(13)

2. Eliminate objectives and measures that were not germane to EHR adoption (i.e. practice management functions) and others that the AMA feels are not ready for Stage 1 due to the lack of electronic exchange readiness (e.g. reporting immunization data).

3. Revise the proposed definition for hospital-based physicians to broaden eligibility; and only require EPs to attest that they have selected three clinically relevant quality measures, if appropriate, and have downloaded and reviewed the Level 1 (human readable) measure specifications for these measures.

4. Only require EPs to attest that they have selected three clinically relevant quality measures, if appropriate, and have downloaded and reviewed the Level 1 (human readable) measure specifications for these measures.

II. The College of American Pathologists (CAP) believe that the proposed rule will not adequately address the need for pathologist and laboratory support of MU efforts, and therefore EPs will not be able to comply with many MU requirements that rely on laboratory data.

The CAP recommends that:

1. Based on the Act, laboratories are not considered EPs and do not qualify for MU incentives. In defining "hospital-based" EP, CMS should take into consideration whether a pathologist has or will be required to contribute funding towards an EHR. Those EPs who are required to contribute funding should not be considered hospital-based, as they are not provided full access to the "facilities and equipment of the hospital including the hospital's qualified EHR." This will reduce the possibility that EPs that do contribute funding will suffer a negative economic impact while complying with the spirit of the EHR regulation.

2. Under the Act, a hospital-based EP is an EP who furnishes ninety-percent or more of his or her covered professional services in the calendar year proceeding the payment year in a hospital setting. A setting is considered a hospital setting if it is identified by the codes used in the HIPAA standard transactions that identifies the site of service as an inpatient hospital, outpatient hospital, or emergency room. Because of the ninety-percent threshold, small changes in a pathologist's service mix could result in his or her meeting the definition of hospital-based in one year and not the next. The proposed rule is silent as to how such providers should be treated. CAP recommends that in the final rule CMS explicitly address the treatment of providers whose status may change from year to year.

3. Under the proposed rule, pathologists, who performed *less* than 90 percent of their professional services in any inpatient or outpatient setting in the prior year would be considered an EP pursuant to §495.100 of the Act, and would be subject to the requirements of the regulation. As such, all EPs would be required to report specified Health IT Functionality Measures that include several functions that pathologists do not usually perform, such as transmitting at least 75 percent of all permissible prescriptions electronically using certified EHR technology, or maintaining active medication and medication lists and allergy lists. Further, all EPs have to report on all Core Measures (i.e., preventive care and screening regarding tobacco use, blood pressure measurement, and drugs to be avoided by the elderly) and a subset of clinical measures that are most appropriate to the physician's specialty. Given the nature of pathology's scope of practice, none of these Core Measures could be met by pathologists in their day-to-day practice. Additionally, the proposed rule's specified specialty group measures –cardiology, pulmonology, endocrinology, oncology, proceduralist/surgery, primary care, pediatrics, obstetrics and gynecology, neurology, psychiatry, ophthalmology, podiatry, radiology, gastroenterology, and nephrology -- are also not applicable to pathology.

4. To ensure that pathologists, who are currently defined as EPs, are not penalized for the failure to meet measures they have no way of meeting in their normal scope of practice, the CAP recommends that CMS consider pathologists as "non-qualifying" eligible providers, exempt from future MU penalties. The CAP appreciates CMS' acknowledgment that certain physicians will not be able to report any specialty MU measures. However, the CAP believes that the exemptions process should be further defined. Specifically, the College recommends clarifying:

1) key terms necessary to support such an exemption process,

2) the exemption process itself, and

3) how and if exempt physicians would be protected from the financial penalties.

5. Several necessary definitions appear to be omitted from the regulation text. CAP is concerned with the omission of the term "specialist." This definition is not only necessary to identify what and who a specialist is, but who would qualify for the exemption. In addition, while referenced on several occasions in the preamble of the regulation, the key term "qualified EP" was not clearly

defined; nor did CMS formally provide a definition for a "Non-Qualifying EP."**(14)** Taken as a whole, the preamble and regulation text seem to define any EP who cannot report any specialty group **and** core measures as essentially a "Non-Qualifying Eligible Provider." For example, pathologists cannot report any measures, specialty or core. CMS should more clearly define or adopt the above-suggested language for "Non-Qualifying EPs" thereby exempting the non-qualifying physicians from potential financial penalties, starting in 2015, for non-compliance with the MU regulation.

Further, based on the suggested definition, the CAP recommends that CMS create a structured regulatory-defined process for the "Non-Qualifying Eligible Provider," to "attest" as to the "inapplicability of selecting and/or reporting any specialty group or core measures," and that pathologists be presumed to be "Non-Qualifying EPs." Lastly, as long as a specialist's specialty could be identified as pathology (through an analysis of the preponderance of their submitted billing codes), they would not need to attest on an individual basis, but could be presumed to be exempt by virtue of being a pathologist.

CAP supports the MU objectives and measures for EPs, eligible hospitals and critical access hospitals contained in §495.6 of the Act, and the incorporation of clinical lab-test results in EHRs. However, CAP observes that this is a rigorous goal that may be difficult for many EPs to meet. As such, the measure may require modification. Therefore, the CAP recommends that the MU requirement that "*at least 50 percent of all clinical lab tests results ordered by the EP ..... are incorporated in certified EHR technology as structured data*," be modified to clarify its specifications and that CMS consider the effects of the requirement on laboratory competition, particularly given the importance of small laboratories to many rural and underserved communities.

6. CAP recognizes that the proposed MU rule is focused on ordering physicians, particularly primary care doctors and the specialties listed in the rule. However, laboratory data is essential to the achievement of MU by EPs since many measures rely on laboratory data. Specifically, as noted above, labs will need to harmonize their HIT systems (i.e. LIS) with qualified EP EHR systems. Such support and data exchange is supported by the CAP and advances the goal of care coordination, achievable through the bidirectional EHR communication between the "Qualifying" and "Non-Qualifying Eligible Provider." However, as the Exchange Subcommittee of the ONC HIT Policy Committee recognized in a December 15, 2009, presentation, these interfaces often cost from $5,000 to $25,000 each (these numbers are for results systems only; the cost would be considerably higher for Computerized Physician Order Entry interfaces where they are even possible in the ambulatory environment) and the cost (except for low-volume customers) is usually borne by the lab. Therefore, the CAP suggests that CMS, in concert with ONC, identify a funding stream to help underwrite the cost of these interfaces. If no such funding stream is available under the Department's current legal authority, we recommend that HHS request such authority given the centrality of lab data to the achievement of MU. While the refinement of standards will bring the cost of these interfaces down over time, the market for laboratory services may experience heightened concentration before this cost reduction can occur.

7. The CAP looks forward to working with CMS as it implements the additional stages provided for in this proposed rule. In Stage 2, CMS anticipates requiring that pathology reports be reported as structured data. Pathologists will be essential to the achievement of this MU goal. Pathologists can play an important role in coordinating care with primary care and other clinicians, both inside and outside the hospital setting. However, to do so they need access to complete EHRs that includes the necessary software integration with electronic LIS infrastructures. Pathologists, regardless of practice setting, utilize LIS and anatomic pathology information systems (APIS) that enable them to order and track tests as well as monitor a patient's disease state. However, by itself the LIS/APIS does not provide enough information for a pathologist to track a patient's disease state. This information is stored and managed in the EHR. LIS/APIS systems only have the ability to work with a limited subset of patient data. Pathologists need to have direct access to the patient's electronic health record, not indirectly through their LIS/APIS system. Without access to robust EHRs, pathologists cannot access the clinical information necessary to determine appropriate testing, test interpretation and follow-up care.

Conclusion

In summary, Advocacy requests that CMS use its discretion and give consideration to the issues raised by the affected stakeholders herein. Advocacy believes there is value bringing these industry positions to CMS' attention in an attempt to balance industry concerns with the agency's regulatory policy. Advocacy encourages CMS to better analyze the possible effects of this regulation on the affected industries. Advocacy appreciates being given a chance to provide CMS with these comments. If you have any questions or concerns, please do not hesitate to contact me, or Assistant Chief Counsel Linwood Rayford, at (202) 205-6533.

Sincerely yours,

/s/

Susan M. Walthall
Acting Chief Counsel Advocacy

/s/

Linwood L. Rayford, III
Assistant Chief Counsel for Food, Drug
and Health Affairs

cc: Cass R. Sunstein, Administrator, Office of Information and Regulatory Affairs

ENDNOTES

1. Pub. L. No. 111-5.

2. Pub. L. No. 96-354, 94 Stat. 1164 (1981) (codified at 5 U.S.C. §§ 601-612) amended by Subtitle II of the Contract with America Advancement Act, Pub. L. No. 104-121, 110 Stat.857 (1996). 5 U.S.C. § 612(a).

3. 75 Fed. Reg. 1973 (January 13, 2010).

4. Id., "Meaningful use" is a term defined by CMS that describes the use of HIT that furthers the goals of information exchange among health car professionals.

5. 75 Fed. Reg. 1974 (January 13, 2010).

6. Id.

7. Id.

8. Id.

9. 75 Fed Reg. 1974.

10. Id., Title XIII of Division A of Act, may be cited as the Health Information Technology for Economic and Clinical Health Act'' or the '' HITECH Act. '' The incentive payments for adoption and meaningful use of HIT and qualified EHRs are part of a broader effort under the HITECH Act to accelerate the adoption of HIT and utilization of qualified EHRs.

11. Because of the short time frame for implementation provided by the HITECH Act for providers to begin using EHR technology, CMS proposes to adopt a phased approach to the requirements outlined in the rule. Stage 1, as provided for in this rule outlines the initial Meaningful Use criteria.

12. 75 Fed Reg. 1854.

13. Please refer to the AMA's comment letter to CMS for an outline of the 5 suggested objectives and measures.

14. CMS seems to imply a definition for Non-Qualifying EP on page 1891 of the rule by requiring EPs to select a specialty group on which to report all applicable cases for each of the measures in the specialty group, or to certify to CMS or the State that they should be exempt from selecting and reporting on a specialty measures group.

○