DEPARTMENT OF HEALTH & HUMAN SERVICES **Office of Inspector General**

Washington, D.C. 20201

May 16, 2011

TO: Farzad Mostashari, M.D., Sc.M.
National Coordinator for Health Information Technology
Office of the National Coordinator for
Health Information Technology

FROM: /Daniel R. Levinson/
Inspector General

SUBJECT: Audit of Information Technology Security Included in Health Information Technology Standards (A-18-09-30160)

The attached final report provides the results of our review of information technology security included in health information technology standards.

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that the Office of Inspector General (OIG) post its publicly available reports on the OIG Web site. Accordingly, this report will be posted at http://oig.hhs.gov.

If you have any questions or comments about this report, please do not hesitate to call me, or your staff may contact Lori S. Pilcher, Assistant Inspector General for Grants, Internal Activities, and Information Technology Audits, at (202) 619-1175 or through email at Lori.Pilcher@oig.hhs.gov. We look forward to receiving your final management decision within 6 months. Please refer to report number A-18-09-30160 in all correspondence.

Attachment

Department of Health & Human Services

OFFICE OF INSPECTOR GENERAL

AUDIT OF INFORMATION TECHNOLOGY SECURITY INCLUDED IN HEALTH INFORMATION TECHNOLOGY STANDARDS

Daniel R. Levinson
Inspector General

May 2011
A-18-09-30160

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health & Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at http://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

BACKGROUND

Office of the National Coordinator for Health Information Technology

On April 27, 2004, Executive Order 13335 created within the Department of Health & Human Services (HHS) the Office of the National Coordinator for Health Information Technology (ONC) to lead the development and nationwide implementation of an interoperable health information technology (HIT) infrastructure. The National Coordinator for Health Information Technology was charged with developing, maintaining, and directing the implementation of a strategic plan to guide the nationwide implementation of interoperable HIT that will reduce medical errors, improve quality, produce greater value for health care expenditures, ensure that patients' individually identifiable health information is secure and protected, and facilitate the widespread adoption of electronic health records (EHR).

In 2005, ONC established the Health Information Technology Standards Panel (HITSP) as a cooperative partnership between the public and private sectors to harmonize and integrate standards for sharing information among organizations and systems. HITSP has developed interoperability specifications, which define the transactions between systems, including the message, the content, and the terminology for the information exchange. Interoperability specifications also give directions to health care providers about implementing EHRs and sharing information among health organizations and systems. In developing the interoperability specifications, HITSP considered overarching principles and concepts derived from an analysis of Federal and State laws and regulations.

Health Information Technology for Economic and Clinical Health Act

Through the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (P.L. No. 111-5), Congress reestablished ONC by statute and directed ONC to develop a nationwide HIT infrastructure that allows for the electronic use and exchange of information, specifically EHRs. Important responsibilities for ONC included recommending to the HHS Secretary the adoption of standards, implementation specifications, and certification criteria by December 31, 2009. In addition, the HITECH Act requires ONC to update its strategic plan to include specific objectives, milestones, and metrics with respect to, among other matters, the use of an EHR by every individual in the United States by 2014; ensuring appropriate authorization and electronic authentication of health information; and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable to unauthorized users.

Privacy and Security Protections

The responsibility to maintain the privacy and security of health information is dispersed among several Federal agencies, including three within HHS: ONC, the Centers for Medicare & Medicaid Services (CMS), and the Office for Civil Rights (OCR).

General Information Technology Security Controls Versus Application Controls

General information technology (IT) security controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure the proper operation of information systems, and create a secure environment for application systems and controls. General IT security controls work together to ensure a secure environment for health data. Application controls, in contrast, function inside systems or applications to ensure that they work correctly. Application controls may be easily bypassed if general IT security controls are missing or ineffective.

OBJECTIVE

Our objective was to assess the IT security controls in HIT standards.

SUMMARY OF FINDING

We found that ONC had application controls in the interoperability specifications, but there were no HIT standards that included general IT security controls. At the time of our audit, the interoperability specifications were the ONC HIT standards and included security features necessary for securely passing data between EHR systems (e.g., encrypting transmissions between EHR systems). These controls in the EHR systems were application security controls, not general IT security controls.

We reviewed the Interim Final Rule for Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, issued in January 2010, and the Final Rule published in the *Federal Register* in July 2010. Both documents discuss security in terms of application controls; they do not contain general IT security controls. A few examples of general IT security controls emphasized by the Office of Management and Budget and the National Institute of Standards and Technology but not addressed by ONC are:

- encrypting data stored on mobile devices, such as compact disks and thumb drives;
- requiring two-factor authentication when remotely accessing an HIT system; and
- patching the operating systems of computer systems that process and store EHR.

We found the lack of these and other general IT security controls during prior Office of Inspector General audits at Medicare contractors, State Medicaid agencies, and hospitals. The vulnerabilities that we noted, combined with our findings in this audit, raise concern about the effectiveness of IT security for HIT if general IT security controls are not addressed.

RECOMMENDATIONS

We recommend that ONC:

- broaden its focus from interoperability specifications to include well-developed general IT security controls for supporting systems, networks, and infrastructures;

- use its leadership role to provide guidance to the health industry on established general IT security standards and IT industry security best practices;

- emphasize to the medical community the importance of general IT security; and

- coordinate its work with CMS and OCR to add general IT security controls where applicable.

OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY COMMENTS

ONC concurred with our recommendations and described the actions that it was taking to address them. ONC's comments are included in their entirety as the Appendix.

TABLE OF CONTENTS

ACRONYMS

CD	compact disk
CMS	Centers for Medicare & Medicaid Services
EHR	electronic health record
FISCAM	*Federal Information System Controls Audit Manual*
HHS	Department of Health & Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIT	health information technology
HITECH	Health Information Technology for Economic and Clinical Health Act
HITSP	Health Information Technology Standards Panel
IT	information technology
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONC	Office of the National Coordinator for Health Information Technology
OS	operating system
PHSA	Public Health Service Act

INTRODUCTION

BACKGROUND

Office of the National Coordinator for Health Information Technology

On April 27, 2004, Executive Order 13335 created within the Department of Health & Human Services (HHS) the Office of the National Coordinator for Health Information Technology (ONC) to lead the development and nationwide implementation of an interoperable health information technology (HIT) infrastructure to improve the quality and efficiency of health care. The National Coordinator for Health Information Technology (National Coordinator) was charged with developing, maintaining, and directing the implementation of a strategic plan to guide the nationwide implementation of interoperable HIT in both the public and private health care sectors that will, by 2014, reduce medical errors, improve quality, produce greater value for health care expenditures, ensure that patients' individually identifiable health information is secure and protected, and facilitate the widespread adoption of electronic health records (EHR).

Health Information Technology Standards Panel

In 2005, ONC established the Health Information Technology Standards Panel (HITSP) as a cooperative partnership between the public and private sectors to harmonize and integrate standards for sharing information among organizations and systems. HITSP is a multistakeholder organization that has developed interoperability specifications through a voluntary, consensus-based process. Interoperability specifications define the transactions between systems, including the content and the terminology for the information exchange. Interoperability specifications also give directions to health care providers about implementing EHRs and sharing information among health organizations and systems.

Since 2007, HITSP has developed and refined its interoperability specifications to integrate already existing and emerging standards and to align overlapping standards. In developing the interoperability specifications, HITSP considered overarching principles and concepts derived from an analysis of Federal and State laws and regulations.

Health Information Technology for Economic and Clinical Health Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5 (Recovery Act), amended the Public Health Service Act (PHSA) to improve health care quality, safety, and efficiency through the promotion of HIT and the electronic exchange of health information.

Through HITECH, Congress reestablished ONC by statute and directed ONC to develop a nationwide HIT infrastructure that allows for the electronic use and exchange of information, specifically EHRs. Important responsibilities for ONC included recommending to the HHS Secretary the adoption of standards, implementation specifications, and certification criteria by December 31, 2009. In addition, HITECH requires ONC to update its strategic plan to include specific objectives, milestones, and metrics with respect to, among other matters, the use of an

EHR by every individual in the United States by 2014; ensuring appropriate authorization and electronic authentication of health information; and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable to unauthorized users. HITECH permits ONC to recommend and the HHS Secretary to apply the standards developed by HITSP before the law's enactment.

To facilitate the development and adoption of an HIT infrastructure and standards, HITECH created two committees: the HIT Policy committee and the HIT Standards committee. The National Coordinator is a leading member of both committees. The Policy committee makes policy recommendations to the National Coordinator relating to the implementation of a nationwide HIT infrastructure. The Standards committee recommends to the National Coordinator standards, implementation specifications, and certification criteria for the electronic exchange and use of health information.

Privacy and Security Protections

The responsibility to maintain the privacy and security of health information is dispersed among several Federal agencies, including three entities within HHS.

Office of the National Coordinator

Section 13101 of HITECH (PHSA §§ 3001(b)(1), 3001(c)(3)(A), and 3002(b)(2)(B), as amended) states that ONC and its committees must develop standards and a framework for the protection and security of health information being exchanged through a nationwide health information network. ONC published an Interim Final Rule (75 Fed. Reg. 2013 (2010)) containing the initial set of standards. ONC finalized the rule, which contains provisions that address privacy and security protection (75 Fed. Reg. 44590 (2010)).

Centers for Medicare & Medicaid Services

Pursuant to Title IV of the Recovery Act, which authorizes Medicare and Medicaid incentive payments to eligible professionals and hospitals for the meaningful use of EHR technology, the Centers for Medicare & Medicaid Services (CMS) promulgated its Final Rule defining "meaningful use" (75 Fed. Reg. 44313 (2010)). This definition includes the protection of health data and requires that eligible professionals and hospitals conduct a risk analysis of their EHR systems and implement updates to address identified vulnerabilities.

Office for Civil Rights

The Office for Civil Rights (OCR) oversees compliance with the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). On September 23, 2009, OCR's Interim Final Rule (74 Fed. Reg. 42740 (2009)) for breach notifications of unsecured sensitive information became effective. Pursuant to HITECH, the Interim Final Rule established regulations requiring covered entities to notify affected individuals, the media, and the HHS Secretary following a breach of their protected health information.

General Information Technology Security Controls Versus Application Controls

General information technology (IT) security controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure the proper operation of information systems, and create a secure environment for application systems and controls. Some primary objectives of general IT security controls are to protect networks, computer systems, and data. General IT security controls work together to ensure a secure environment for health data.

Application controls, in contrast, function inside systems or applications to ensure that they work correctly. Application controls may be easily bypassed if general IT security controls are missing or ineffective.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

Our objective was to assess the IT security controls in HIT standards.

Scope

We assessed ONC's process for creating and adopting interoperability specifications as of April 2009. We also reviewed the Interim Final Rule for Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, issued in January 2010, and the Final Rule published in the *Federal Register* in July 2010. We did not review ONC's overall internal control structure.

We performed our fieldwork at ONC headquarters in Washington, DC, from June through August 2009 and from February through August 2010. After the end of our initial fieldwork in 2009, ONC management provided additional information to demonstrate the steps that ONC had taken to address the security of sensitive information.

Methodology

To accomplish our objective, we:

- reviewed applicable Federal laws, regulations, and guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST);

- interviewed ONC staff; and

- reviewed supporting documentation.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective.

FINDING AND RECOMMENDATIONS

We found that ONC had application controls in the interoperability specifications, but there were no HIT standards that included general IT security controls. At the time of our audit, the interoperability specifications were the ONC HIT standards and included security features necessary for securely passing data between EHR systems (e.g., encrypting transmissions between EHR systems). These controls in the EHR systems were application security controls, not general IT security controls.

We reviewed the Interim Final Rule issued in January 2010 and the Final Rule published in the *Federal Register* in July 2010. Both documents discuss security in terms of application controls; they do not contain general IT security controls. A few examples of general IT security controls emphasized by OMB and NIST but not addressed by ONC are:

- encrypting data stored on mobile devices, such as compact disks (CD) and thumb drives;
- requiring two-factor authentication when remotely accessing an HIT system; and
- patching the operating systems (OS) of computer systems that process and store EHR.

We found the lack of these and other general IT security controls during prior Office of Inspector General (OIG) IT audits at Medicare contractors, State Medicaid agencies, and hospitals. The vulnerabilities that we noted, combined with our findings in this audit, raise concern about the effectiveness of IT security for HIT if general IT security controls are not addressed.

ADOPTING GENERAL INFORMATION TECHNOLOGY SECURITY CONTROLS

Federal Requirements

We identified the following Federal security standards for the protection of Federal data as reasonable benchmarks to assess the adequacy of the general IT security controls established for EHRs.

Recovery Act

The Recovery Act added section 3001 of the PHSA, which states that the National Coordinator "shall perform [his or her] duties … in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information that – (1) ensures that each patient's health information is secure and protected, in accordance with applicable law." The Recovery Act states that the National Coordinator should, in consultation with appropriate Federal agencies, update the *Federal Health IT Strategic Plan* to include specific objectives, milestones, and metrics. The update should:

- include the "incorporation of privacy and security protections for the electronic exchange of individually identifiable health information" and

- use "security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable" to unauthorized users (section 3001(c)(3)(A)).

Office of Management and Budget

In OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," OMB recommends:

- encrypting "all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing" and

- allowing "remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access."

National Institute of Standards and Technology Special Publication 800-40

NIST Special Publication 800-40, revision 2, *Creating a Patch and Vulnerability Management Program*, states that:

> Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization…. Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of IT systems…. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed before the outbreaks [Executive Summary, November 2005].

Federal Information System Controls Audit Manual

The *Federal Information System Controls Audit Manual* (FISCAM) states that general IT security controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure the proper operation of information systems, and create the environment for application systems and controls. General controls protect networks, safeguard data, and prevent unauthorized access to software. The effectiveness of general controls is a significant factor in determining the effectiveness of application controls. Without effective general controls, application controls "can generally be rendered ineffective by circumvention or modification."[1]

[1] Government Accountability Office, FISCAM, section 1.2, February 2009.

General Information Technology Security Controls Needed

Health Information Technology Standards

ONC did not have HIT standards that included general IT security controls. A few examples of general IT security controls are encrypting data stored on mobile devices, using two-factor authentication, and updating (patching) the OSs that process and store sensitive health-related information. For example:

- Encryption is required by ONC interoperability specifications for data transmission between systems. However, encrypting data stored on portable media is not included in a standard, creating a potential vulnerability if unprotected HIT data were copied to portable media, such as a CD or flash drive, and transported to another location. Encrypting data stored on portable media is not included in any HIT standard.

- Two-factor authentication is not required by the HIT standards. Two-factor authentication is a security process in which the user provides two means of identification. Typically, this requires a physical token, such as a card, and something memorized, such as a security code (i.e., "something you have and something you know").

- Patching computer systems, which includes timely security updates and enhancements to protect IT systems from viruses, malware, and other attacks, is not required by the HIT standards.

Lack of any of these or other IT security controls can expose HIT systems to a host of problems. Each year, Cisco Systems issues a security report that encompasses threat information, trends, and a snapshot of the state of IT security. The *Cisco 2009 Annual Security Report* stressed the importance of patching computer systems, our third example, by stating:

> Conficker, the big botnet[2] of 2009, gained traction because computer users failed to download a patch that was readily available from Microsoft. Although most of today's attacks are launched via social media networks, criminals still look for ways to exploit these old-style vulnerabilities.

We found these three vulnerabilities, as well as many others, during OIG IT audits at Medicare contractors, State Medicaid agencies, and hospitals.

[2] A botnet is a large group of computers taken over by a hacker and frequently used without the computer owners' knowledge.

Interoperability Specifications

Interoperability specifications do not address general IT security controls recommended by NIST and best practices. For example, interoperability specifications do not address controls on the networks that the EHR applications use. Dr. John Halamka, chairman of HITSP and vice-chairman of the Standards Committee, stated that security is broader than just EHR interoperability standards and EHR applications:

> **Security is not just about using the right standards or purchasing products that implement those standards.** It's also about the infrastructure on which those products run and the policies that define how they'll be used. A great software system that supports role-based security is not so useful if everyone is assigned the same role and its accompanying access permissions. Similarly, running great software on an open wireless network could compromise privacy.… **Security is a process, not a product.** Hackers are innovative, and security practices need to be constantly enhanced to protect confidentiality. Security is also a balance between ease of use and absolute protection. The most secure library in the world—and the most useless—would be one that never loaned out any books.… **Security is an end-to-end process.** The health care ecosystem is as vulnerable as its weakest link. Thus, each application, workstation, network and server within an enterprise must be secured to a reasonable extent. The exchange of health care information between enterprises cannot be secured if the enterprises themselves are not secure.[3] [Emphasis in the original.]

Health Information Technology Standards Panel's Focus

HITSP itself has said that it did not intend to resolve privacy or security policy issues in its standards-making process:

> The HITSP SPI-TC[4] designed the constructs described in this Technical Note to support a wide variety of security and privacy policies and technical frameworks…. HITSP has not attempted to resolve privacy or security policy issues, risk management, healthcare application functionality, operating systems functionality, physical control specifications, or other low-level specifications…. [Emphasis in the original.][5]

At the time of our review, the meeting transcripts and reports from the Standards committee and its Security subcommittee showed recommendations for encrypting data on portable devices but no recommendations relating to two-factor authentication, system patching, or any other general IT security issues. At the end of our audit period, the Standards committee had not acted on encrypting data on portable devices.

---

[3] John Halamka, "Opinion: E-health security requires a delicate balance," *ComputerWorld,* p. 34, October 5, 2009.

[4] Security, Privacy, and Infrastructure Domain Technical Committee.

[5] HITSP, *Security and Privacy Technical Note*, TN 900, section 1.1.1, October 2007, revised July 2009.

Additional Office of the National Coordinator Documentation

After the end of our fieldwork, ONC gave us documents to show its position on general IT security:

- Four documents, published after our initial fieldwork, related to EHR system certification.

- One document, from OCR and published after our initial fieldwork, was on breach notification and the way in which the use of encryption would negate the need for notification. ONC told us that this would encourage the use of encryption.

- ONC provided documentation on three grants that it had funded. We found that two of the grants (posted after our fieldwork) might have enhanced general IT controls because they discussed general IT security, but they did not address the specific conditions found in this report even though the tasks in the two grants included those conditions:

    - One grant will establish the Strategic Health IT Advanced Research Projects program, which will fund research that focuses on identifying technology solutions to problems impeding broad adoption of HIT, including HIT security.

    - Another grant will establish at least 70 Regional Extension Centers and a national HIT Research Center to offer technical assistance, guidance, and information on best practices, including those on IT security issues, to support and accelerate health care providers' efforts to become meaningful users of EHRs.

- Three documents related to HIPAA security: one was from NIST and two were from CMS. ONC management told us that it relies on the HIPAA Security Rule to ensure that appropriate IT security controls are in place.

Prior Office of Inspector General Work and the
Health Insurance Portability and Accountability Act of 1996

Our concern with the effectiveness of the HIPAA Security Rule is based on work that we did on CMS's oversight of covered entity compliance with HIPAA and the significant weaknesses we found in IT security at eight hospitals. Examples of the weaknesses identified at the eight hospitals included:

- unprotected wireless networks,

- lack of vendor support for OSs,

- inadequate system patching,

- outdated or missing antivirus software,

- lack of encryption of data on portable devices and media,
- lack of system event logging or review,
- shared user accounts, and
- excessive user access and administrative rights.

Our experience with HIPAA implementation in hospitals does not support ONC's position that HIPAA provides adequate general IT security. We also have similar findings in Medicare and Medicaid audits.

CONCLUSION

We found that the interoperability specifications, the Interim Final Rule, and the Final Rule did include some security features necessary for securely passing data between systems. However, ONC did not have standards that included general IT security controls, which need to be addressed to ensure a secure environment for health data.

In addition, ONC deferred at this time to the HIPAA Security Rule for addressing IT security for HIT. Our HIPAA reviews identified vulnerabilities in the HHS oversight function and the general IT security controls. Those vulnerabilities in hospitals, Medicare contractors, and State agencies, combined with our findings in this audit, raise concern about the effectiveness of IT security for HIT if general IT security controls are not addressed by ONC.

RECOMMENDATIONS

We recommend that ONC:

- broaden its focus from interoperability specifications to include well-developed general IT security controls for supporting systems, networks, and infrastructures;
- use its leadership role to provide guidance to the health industry on established general IT security standards and IT industry security best practices;
- emphasize to the medical community the importance of general IT security; and
- coordinate its work with CMS and OCR to add general IT security controls where applicable.

OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY COMMENTS

ONC concurred with our recommendations. ONC's comments are included in their entirety as the Appendix.

APPENDIX

APPENDIX: OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the National Coordinator
for Health Information Technology
Washington, D.C. 20201

DATE: March 23, 2011

TO: Daniel R. Levinson
Inspector General

FROM: David Blumenthal
National Coordinator for Health Information Technology

Farzad Mostashari on behalf of David Blumenthal

SUBJECT: Office of Inspector General Draft Report: "Audit of Information Technology Security Included in Health Information Technology Standards (A-18-09-30160)

Thank you for the opportunity to review and comment on the above referenced Office of Inspector General (OIG) draft report. The Office of the National Coordinator for Health Information Technology (ONC) appreciates the effort and resources OIG has invested to research and report on ONC's activities related to Health Information Technology (health IT) standards.

ONC recognizes the crucial role of health IT security in maintaining the public's trust in health IT and health information exchange. In its early stages, ONC contracted with the Health Information Technology Standards Panel (HITSP) as an ANSI-accredited body to select and harmonize healthcare data standards that are foundational to the interoperability use cases identified by the American Health Information Community (AHIC), a Federal Advisory Committee Act Committee (FACA). Under contract with ONC from 2005 through 2010, HITSP established a Security and Privacy Technical Committee, which identified and recommended security standards that cut across all AHIC's use cases. These standards were referenced in published interoperability specifications. Beginning in January 2008, the HHS Secretary officially recognized a number of HITSP-produced interoperability specifications as HHS policy.[1] The first set of HITSP interoperability specifications incorporated security features such as transmission encryption, audit logging, entity authentication, digital signatures, access controls, and rights management. These standards were also incorporated into the certification process formerly managed by the Certification Commission for Health IT (CCHIT). An open source health information exchange product, CONNECT, developed by a 29-agency cooperative agreement (the Federal Health Architecture) incorporates these recognized standards.

The focus of standards activity shifted with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which created a framework for providing Medicare and Medicaid incentive payments for the meaningful use of certified electronic health record (EHR) technology. HITECH also established the Health IT Policy Committee (HITPC) and the Health IT Standards Committee (HITSC), AHIC's successors. Under HITECH and with a new FACA panel in place, the methodology and scope of ONC's security standards activities evolved from a transaction-level approach to a product-oriented approach consistent with the statutory mandate that ONC certify health IT, including EHR technology. The HHS Centers for Medicare and Medicaid (CMS) EHR Incentive Programs provide incentive payments to eligible health care providers participating in these programs only when they adopt certified EHR technology and use it to achieve meaningful use.

The HITSC Privacy and Security Working Group formulated its standards recommendations using the HITSP standards as its basis. Considering the security standards recommendations from the HITSC, and

[1] Under Executive Order 13410, recognition is the process by which standards are required to be incorporated in all new or significantly upgraded Federal information systems.

after analyzing extensive public comment on ONC's Interim Final Rule, ONC published the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Final Rule on July 28, 2010, simultaneously with CMS's final rule on the Medicare and Medicaid EHR Incentive Program. The certification criteria in ONC's Final Rule included requirements and standards that EHR technology support important general IT security control capabilities: encryption of electronic Protected Health Information (ePHI) at rest and in motion; access controls to prevent unauthorized viewing or use of ePHI; and message integrity checking. These requirements are intended to allow health IT adopters to achieve meaningful use objective 14: "Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities." The measurement criterion for this objective requires adopters to "Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process"), adopting a well-recognized risk based approach to managing security. Consequently, the meaningful use Stage 1 rule specifically requires health IT adopters to identify and correct any security deficiencies. There are a number of general health IT standards, including the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA), as well as federal security frameworks which have served as best practices for the general public, including those developed by the National Institute for Standards and Technology (NIST), that are available for use in assessing and correcting such security deficiencies.

ONC's primary mission is to promote the adoption of health IT in support of improved healthcare: better outcomes, fewer errors, less cost. Consequently, in the early stages of adoption efforts under HITECH, ONC has worked to strike the right balance between ensuring the security of health information among new adopters while not creating such an onerous burden of technical requirements that the primary adoption goal would fail to be achieved. By the end of the HITECH-related wave of health IT implementations in 2015, ONC expects to have a well developed set of certification criteria that, coupled with practices initiated under the CMS meaningful use rule, will form a strong security framework for the use and exchange of electronic health information.

Adoption is not the whole story, however. There are many health IT users who are not eligible for Meaningful Use incentives. But unless the entire health IT ecosystem participates in good security practices, the well secure could face risk from the less secure. Therefore, ONC addresses security and cybersecurity at the enterprise level, with a strategic plan that considers all components of the greater world of health IT. HITECH required ONC to revise and update its Federal Health IT Strategic Plan. A key element of that plan is health IT security. ONC's Office of the Chief Privacy Officer is in the final stages of drafting a comprehensive security strategic plan that details its plans in this regard. ONC agrees with the sentiment expressed by HITSC vice-chairman John Halamka: "security is an end-to-end process." We support the vision of enterprise-class health IT security and have taken clear steps to bring this vision to fruition. It is a task neither fast nor easy, but it is one to which ONC remains fully committed.

Technical Comments

Page 2 (HITECH, final paragraph)

"ONC published an Interim Final Rule (75 Fed. Reg. 2013 (2010)) containing the initial set of standards, which superseded the interoperability specifications adopted before HITECH's enactment."

This statement is inaccurate. The standards adopted in ONC's IFR did not supersede the interoperability specifications adopted prior to the HITECH Act. We recommend a period be added to this sentence after "standards" and the rest of the language deleted.

Page 2, last sentence inaccurately describes the breach notification rule. We recommend that it be rewritten to read as follows:

Pursuant to HITECH, the Interim Final Rule established regulations requiring covered entities to notify affected individuals, the media, and the HHS Secretary following a breach of their protected health information.

OIG Recommendation I

[ONC should] broaden its focus from interoperability specifications to also include well-developed general IT security controls for supporting systems, networks, and infrastructure.

ONC Response I

ONC concurs with OIG that "general IT security controls" serve an important purpose and are necessary to ensure the overall protection of the confidentiality, integrity, and availability of health information. As OIG notes on page 2 of the draft report, the Office for Civil Rights (OCR) is responsible for regulating covered entities and their compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. However, in accordance with its mission, ONC has been (and will continue to be) proactive in helping providers safeguard the privacy and security of personal health information.

ONC has used its authority to regulate the certification criteria and standards for certified health information technology to ensure the availability of application security controls. ONC will work with the FACAs established under the HITECH Act to actively explore the feasibility of adding general IT security controls, such as encryption of portable media and two-factor authentication, to the certification criteria.

In addition, ONC has developed training and tools, such as the Privacy and Security Framework Toolkit that ONC launched in 2008, and more recently tools and materials streamed out through ONC's 62 Regional Extension Centers who are engaged in active outreach to healthcare providers. These materials include security awareness literature (and soon, a security awareness video), a detailed checklist covering all 10 security domains, and an automated risk analysis tool. Funded products now in development for the RECs include a security capability assessment, incident response planning and training, and continuity of operations training. For health information exchanges (HIEs), ONC is developing an enterprise-class resiliency plan based on a deep analysis of the health information exchange landscape and its risks and vulnerabilities. The above activities are the core elements of ONC's short-term security strategy, effective September 2010, with goals to address the pressing security issues related to rapid health IT and HIE adoption.

ONC has worked closely with OCR, which has the authority to establish general IT security standards through the HIPAA Security Rule, on a number of general IT security issues, including the development of security guidance on how to render protected health information (PHI) unusable, unreadable, and indecipherable for the purposes of the new breach notification provisions included in the HITECH Act. To this day, ONC continues to work with OCR and NIST on this effort.

ONC will continue to focus on broad health IT security issues and is currently working to identify remaining gaps where, within its mission and scope of responsibility, it can address security across the health IT enterprise with tools, techniques, research, recommendations and, where appropriate and within its authority, regulation.

OIG Recommendation II

[ONC should] use its leadership role to provide guidance to the health industry on established general IT security standards and IT industry security best practices

ONC Response II

ONC concurs with OIG on the importance of disseminating security principles and practices as they apply to health IT. As part of ONC's efforts to work with FACAs and relevant Federal partners to bolster security controls, will continue to issue recommendations and guidance to the health industry on health IT security best practices.

As described above, ONC has taken a leadership role in promoting health IT security controls through its education and outreach activities. In addition, ONC has provided (and will continue to provide) practical, hands-on security management assistance through the Regional Extension Centers. In addition, ONC participates widely in public outreach programs through speaking engagements, conferences, and workshops. ONC continues to sponsor health information exchange technology, such as the Direct project and NwHIN, both of which have developed strong security protections around health information exchange. In FY 2010, ONC leadership and staff participated in approximately 20 security and privacy related public engagements, including the Health Information and Management Systems Society, HIPAA Summit, HIPAA Summit West, RSA, Symantec Government Security, Smart Cards in Government, International Association of Privacy Professionals, Information Systems Security Association, Information Systems Audit and Control Association, and others.

OIG Recommendation III

[ONC should] emphasize to the medical community the importance of general IT security

ONC Response III

ONC concurs with OIG that it is vitally important to promote awareness of general IT security within the medical community. ONC has been active in reaching out to individual providers through the Regional Extension Centers, Beacon Communities, Health Information Exchanges, each of which operates a Privacy and Security Community of Practice, and through SHARP security research activities which reach the academic medical community. ONC has also ensured the inclusion of security and privacy education in health IT curricula developed under ONC grants. In fiscal year 2011, in collaboration with OCR, ONC will launch a Security/Cybersecurity communications campaign to raise awareness of and adherence to high-quality health IT security practices.

OIG Recommendation IV

[ONC should] coordinate its work with CMS and OCR to add general IT security controls where applicable.

ONC Response IV

ONC concurs with OIG's finding that coordination among ONC, CMS, and OCR is crucial to promoting the adoption of general IT security controls for health IT. ONC has collaborated extensively with CMS throughout Stage 1 of Meaningful Use. The next two stages of meaningful use and launching of the communications program mentioned above will provide additional opportunities for ONC to collaborate with its partners, including CMS and OCR, on how best to raise the overall level of health IT security with certification criteria and implementation incentives.

ONC is engaged in on-going collaboration with OCR, for example by providing technical research and recommendations on emerging security technologies and techniques, which OCR has used to inform its rulemaking and guidance. In turn, OCR has collaborated with ONC by providing input to ONC security and cybersecurity programs and products to insure that our efforts on security are synergistic and non-duplicative.

Conclusion

ONC has an extensive portfolio of initiatives (that are completed, in process, or in the planning and formulation stages) that seek to promote increased security and the public's trust in health IT technology and electronic health information exchange. In the interest of brevity, we have not detailed all of ONC's initiatives in our comments to this OIG report.

ONC thanks OIG for its efforts on this report and for addressing areas of future growth for ONC's security program. We look forward to continuing to work with OIG to assess and strengthen the underlying trust

fabric without which our mission to improve healthcare through widespread adoption and meaningful use of health IT could be at risk