Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY'S OVERSIGHT OF THE TESTING AND CERTIFICATION OF ELECTRONIC HEALTH RECORDS

Daniel R. Levinson
Inspector General

August 2014
A-06-11-00063

Office of Inspector General

https://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 and 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.

EXECUTIVE SUMMARY

The Office of the National Coordinator for Health Information Technology's oversight of the authorized testing and certification bodies did not fully ensure that electronic patient information in the currently available electronic health record applications was secure and protected.

WHY WE DID THIS REVIEW

To improve the quality and value of American health care, the Federal Government promotes the use of certified electronic health record (EHR) applications by health care professionals and hospitals (providers). As an incentive, the Federal Government is paying providers who attest to the "meaningful use" of EHRs. As of December 2013, the Centers for Medicare & Medicaid Services had paid more than $19 billion in incentive payments to more than 340,000 providers who have attested to using EHRs. To receive incentive payments, providers must use EHRs that have been certified by an authorized testing and certification body (ATCB) in accordance with Federal security standards. The U.S. Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC), oversees the testing and certification process for EHRs. Together with ONC and with ONC's approval, the National Institute of Standards and Technology (NIST) developed test procedures for the ATCBs to use when determining whether EHRs met the Federal security standards.

Certification assures health care providers that the EHR has the capabilities needed, including appropriate record security and protection, for providers to participate in the Medicare and Medicaid EHR Incentive Programs. If insecure systems have been certified by an ATCB, providers and patients may have a false sense of security and assurance. We have identified risks related to ATCBs' certifying EHRs with inadequate security and privacy controls and for which health care providers have received incentive payments. As of August 30, 2013, 3,590 certified EHRs were available to health care providers, 95 percent of which were certified by ATCBs under the Temporary Certification Program for Health Information Technology (Temporary Program).

The objectives of this review were to assess whether (1) ONC's oversight of ATCBs ensured that electronic patient information was secure and protected, (2) the ATCBs' standards and procedures for testing and certifying EHRs met NIST test procedure requirements, and (3) NIST test procedures were sufficient to secure and protect electronic patient information.

BACKGROUND

On June 24, 2010, HHS established the Temporary Program for health information technology to test and certify EHRs using the temporary program's criteria. Once tested and certified, EHRs meet the definition of Certified EHR Technology and may be used by providers to help them qualify for incentive payments under the Medicare and Medicaid EHR Incentive Programs.

Federal regulations outline security standards to which the ATCBs must adhere when testing and certifying EHRs. At a minimum, all certified EHRs must meet security requirements related to

seven information technology areas: access control, emergency access, automatic log-off, audit log, integrity, authentication, and general encryption.

WHAT WE FOUND

ONC's oversight of the ATCBs did not fully ensure that test procedures and standards could adequately secure and protect electronic patient information contained in EHRs. Specifically, ONC did not ensure that the ATCBs:

- developed procedures to periodically evaluate whether certified EHRs continued to meet Federal standards and

- developed a training program to ensure that their personnel were competent to test and certify EHRs and to secure proprietary or sensitive EHR information.

The ATCBs' standards and procedures for testing and certifying EHRs met all NIST test procedure requirements that ONC approved. However, those NIST test procedures were not sufficient to ensure that EHRs would adequately secure and protect patient health information; in particular, the procedures allowed ATCBs to certify EHRs that demonstrated the use of a single-character password during testing. In addition, the NIST test procedures did not address common security issues, such as, but not limited to, password complexity and/or logging emergency access or user privilege changes.

WHAT WE RECOMMEND

To ensure that each patient's health information in EHRs is secure and protected, we recommend that ONC require the ATCBs to:

- develop procedures to periodically evaluate whether certified EHRs continue to meet Federal standards and

- develop a training program to ensure that their personnel are competent to test and certify EHRs and to secure proprietary or sensitive EHR information.

We also recommend that ONC work with NIST to strengthen EHR test procedure requirements so that ATCBs can ensure during testing that EHR vendors incorporate a baseline set of security and privacy features into the development of EHRs to address common security issues.

ONC COMMENTS AND OUR RESPONSE

In written comments on our draft report, ONC stated that ATCBs are no longer active in the ONC Certification Program and that testing and certification functions are now performed by separate entities in the ONC Health Information Technology Certification Program. ONC also stated that it currently is using new certification criteria, the 2014 Edition EHR Certification Criteria, that have "strengthened test procedures for common security and privacy features for inclusion in EHRs."

We do not agree that the 2014 Edition EHR Certification Criteria sufficiently address our security concerns regarding the Temporary Program.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

To improve the quality and value of American health care, the Federal Government promotes the use of certified electronic health record (EHR) applications by health care professionals and hospitals (providers). The Medicare and Medicaid EHR Incentive Programs provide financial incentives for the meaningful use of certified EHR technology. To demonstrate meaningful use, providers must meet certain measurement thresholds that range from recording patient information as structured data to exchanging summary care information. EHR incentive programs include three stages with increasing requirements for participation.[1] As of December 2013, the Centers for Medicare & Medicaid Services had paid more than $19 billion in incentive payments to more than 340,000 providers who have attested to using EHRs. To receive incentive payments, providers must use EHRs that have been certified by an authorized testing and certification body (ATCB) in accordance with Federal security standards.

The U.S. Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC), oversees the testing and certification process for EHRs. Certifying EHRs that have inadequate security may increase the risk for unauthorized individuals to gain access to patient health information or to submit improper claims. We have identified risks that are related to ATCB certification of EHRs with inadequate security and privacy controls and for which health care providers have received incentive payments. As of August 30, 2013, 3,590 certified EHRs were available to health care providers, 95 percent of which were certified by ATCBs under the Temporary Certification Program for Health Information Technology (Temporary Program).

OBJECTIVES

Our objectives were to assess whether (1) ONC's oversight of ATCBs ensured that electronic patient information was secure and protected, (2) the ATCBs' standards and procedures for testing and certifying EHRs met National Institute of Standards and Technology (NIST) test procedure requirements, and (3) NIST test procedures were sufficient to secure and protect electronic patient information.

BACKGROUND

Health Information Technology for Economic and Clinical Health Act

On February 17, 2009, the President signed the American Recovery and Reinvestment Act of 2009 (Recovery Act), P.L. No. 111-5. Title XIII of Division A and Title IV of Division B of the Recovery Act are cited together as the Health Information Technology for Economic and Clinical Health Act (HITECH Act). The HITECH Act established ONC, an entity within the

[1] To meaningfully use certified EHRs, providers must use numerous EHR functions defined in Federal regulations, including functions meant to improve health care quality and efficiency, such as computerized provider order entry, electronic prescribing, and the exchange of key clinical information.

Office of the Secretary for HHS, as the principal Federal entity responsible for coordinating the effort to implement a nationwide health information technology (health IT) infrastructure that allows for the use and exchange of health information in an electronic format that protects patient information from unauthorized access. The HITECH Act includes provisions to promote the meaningful use of health IT and authorizes incentive payments to providers.

Temporary Certification Program for Health Information Technology

Section 3001(c)(5) of the Public Health Service Act (PHSA) (as amended by the HITECH Act) requires the National Coordinator to establish a program to certify that EHR technology complies with the certification criteria adopted by the Secretary of HHS in the Standards and Certification Criteria Final Rule (Final Rule). The Temporary Certification Program was in effect from June 24, 2010, to October 4, 2012. The Permanent Certification Program (Permanent Program) came into effect after the sunsetting of the Temporary Program.[2] These programs govern the authorization and operations of bodies that certify EHRs in accordance with ONC certification criteria.[3]

In addition, ONC promulgated its 2011 and 2014 Edition EHR Certification Criteria, to which ATCBs are to certify EHRs.[4] The Temporary and Permanent Certification Programs require ATCBs to abide by the principles of proper conduct. ONC obtained a signed formal agreement, *Agreement to Adhere to the Principles of Proper Conduct for ONC-ATCBs* (Principles of Proper Conduct), from six ATCBs authorized under its certification programs: The Certification Commission for Health Information Technology, Drummond Group, SLIGlobal, ICSA Labs, InfoGard, and SureScripts.

The Principles of Proper Conduct required the ATCBs to, among other things, operate (1) a certification program in accordance with the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Guide 65:1996, *General requirements for bodies operating product certification systems,* and (2) a testing program in accordance with ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*.[5] The Principles of Proper Conduct also require ATCBs to use test procedures approved by ONC.

In addition, ATCBs test EHRs and certify that they meet the certification criteria at 45 CFR part 170, subpart C, which include several security standards (45 CFR §§ 170.302(o)–(u)). To be certified, an EHR must, at a minimum, meet security standards related to the following:

[2] 75 Fed. Reg. 36158 (June 24, 2010) and 76 Fed. Reg. 1262 (January 7, 2011).

[3] Five of the six ATCBs in the Temporary Program have been approved to test and certify EHRs under the Permanent Program, and EHRs certified during the Temporary Program are valid in the Permanent Program. However, starting in 2014, providers and hospitals must use EHRs that are certified under the 2014 Edition EHR Certification Criteria to achieve meaningful use. See 45 CFR § 170.102 Nt. (2012).

[4] 75 Fed. Reg. 44590 (July 28, 2010) and 77 Fed. Reg. 54163 (Sept. 4, 2012).

[5] ISO and IEC develop international standards through technical committees established by the organizations.

access control, emergency access, automatic log-off, audit log, integrity, authentication, and general encryption. Together with ONC and with ONC's approval, NIST developed test procedures for the ATCBs to use when determining whether EHRs met the Federal security standards.

After an EHR is tested and certified, the ATCB informs ONC, which lists the EHR on its Certified Health IT Product List (Product List). Eligible providers may then qualify for incentive payments under the Medicare and Medicaid EHR Incentive Programs by using an EHR on the Product List. Certification assures health care providers that the EHR has the capabilities needed, including appropriate record security and protection, for providers to participate in the Medicare and Medicaid EHR Incentive Programs.

As of August 30, 2013, 3,590 certified EHRs were listed on the Product List. Under the Temporary Program, 3,403 EHRs (95 percent) were certified; the remaining 187 were certified under the Permanent Program. EHRs certified under the Temporary Program are still available to health care providers.

Appendix A contains more details about Federal and international requirements related to the Temporary Program.

HOW WE CONDUCTED THIS REVIEW

We focused our audit on ONC's procedures for oversight of the ATCBs. We also assessed the ATCBs' procedures for testing EHRs and certifying that EHRs meet certain Federal requirements and NIST Special Publications (SP). We judgmentally selected 30 EHRs and reviewed their ATCBs' testing documentation. We also reviewed certain ISO/IEC security requirements related to the security of records and to training at five of the six ATCBs.[6]

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 findings and conclusions based on our audit objectives.

Appendix B contains the details of our audit scope and methodology.

FINDINGS

ONC's oversight of the ATCBs did not fully ensure that electronic patient information in EHRs was secure and protected. Specifically, ONC did not ensure that the ATCBs:

- developed procedures to periodically evaluate whether certified EHRs continued to meet Federal standards and

[6] One of the six ATCBs (SureScripts) did not certify any EHRs; therefore, we excluded it from our review.

- developed a training program to ensure that their personnel were competent to test and certify EHRs and to secure proprietary or sensitive EHR information.

Regulations for the Temporary and Permanent Certification Programs require that ATCBs use testing procedures approved by ONC to evaluate conformance of EHRs to each of ONC's requirements.[7] ONC worked with NIST to develop these test procedures.[8] The ATCBs' standards and procedures for testing and certifying EHRs met all NIST test procedure requirements; however, those NIST test procedures were not sufficient to ensure that EHRs would adequately secure and protect patient health information; in particular, the procedures allowed ATCBs to approve EHRs that demonstrated the use of a single-character password during testing. In addition, the NIST test procedures did not address common security issues, such as, but not limited to, password complexity and logging emergency access or user privilege changes.

ONC'S OVERSIGHT OF AUTHORIZED TESTING AND CERTIFICATION BODIES NEEDS IMPROVEMENT

The HITECH Act requires ONC to develop a nationwide health IT infrastructure that allows for the electronic use and exchange of information and that ensures that each patient's health information is secure and protected, in accordance with applicable law.

Insufficient Procedures for Periodic Evaluation of Electronic Health Record Applications

The ATCB must periodically evaluate the EHRs to confirm that they continue to conform to Federal standards (ISO/IEC Guide 65:1996 § 13.4).

Although the ATCBs were required to comply with the Principles of Proper Conduct, which required compliance with ISO/IEC Guide 65, three of the five ATCBs did not have procedures in place to periodically evaluate EHRs to determine whether they continued to conform to Federal standards. ONC officials informed us that although ISO/IEC Guide 65 required periodic evaluations, ONC did not enforce that requirement during the Temporary Program. ONC officials stated that ONC was developing procedures for periodically evaluating EHRs.[9] Without periodic evaluations, ONC could not assure providers that a certified EHR continued to conform to Federal standards. For example, after its initial certification, an EHR could be modified to conduct fraudulent activities, such as classifying a medical procedure as more expensive than it actually was ("upcoding").

[7] 45 CFR §§ 170.423(e) and 170.523(h).

[8] These procedures were approved by ONC in 75 Fed. Reg. 47817 (August 9, 2010). ONC approved procedures are independent of Federal Information Security Management Act of 2002 (FISMA) standard Federal Information Processing Standards No. 200 (FIPS-200) and the associated FISMA guidance Special Publication 800-53.

[9] ONC officials stated that the requirement for following the procedures would be included in the Permanent Program.

Insufficient Training Program Specifically Related to Electronic Health Record Test Procedures and Security of Records

The Principles of Proper Conduct require ATCBs to maintain a training program that is consistent with ISO/IEC standards; those standards include documented procedures and training requirements to ensure that ATCB personnel are competent to test and certify Complete EHRs or EHR Modules or both (ISO/IEC 17025:2005 § 5.2.1).

ONC did not require the ATCBs to maintain a training program consistent with ISO/IEC standards. That training program would have ensured that ATCB personnel were competent to test and certify EHRs in IT security topics specifically related to the NIST test procedures the ATCBs used. While one of the five ATCBs we reviewed trained its EHR testers appropriately, the remaining four did not train their EHR testers in IT security specifically related to NIST's EHR test procedures. Without this training, the ATCBs could not ensure that testers were knowledgeable about the security-related requirements they were testing. ONC officials explained that they require ATCBs to pass the American National Standards Institute audit and National Voluntary Laboratory Accreditation Program audit, which require some form of IT security training for testers and which all five ATCBs passed. However, ONC could not provide documentation to support that those audits required EHR testers to be trained in IT security topics specifically related to the NIST test procedures the ATCBs used. Without training specifically related to NIST test procedures, ONC could not ensure that testers were knowledgeable about the security-related requirements they were testing.

The Principles of Proper Conduct required ATCBs to operate a testing and certification program consistent with ISO/IEC standards. ISO/IEC standards state that all records[10] must be secure (17025:2005 § 4.13.1.3).

ONC did not require the ATCBs to train personnel in IT security to ensure that all records were secure in accordance with ISO/IEC standards. The records used during testing could have contained proprietary or sensitive information related to EHR testing and certification. Specifically, one of the five ATCBs used the wired equivalent privacy (WEP) protocol to encrypt its wireless network during meetings in rented office space. The WEP suffers from weaknesses that enable attackers to easily decipher data moving over the wireless network and is not an acceptable encryption method.[11] The ATCB was unaware that the wireless network used WEP for encryption because it rented the office space only when it needed to hold meetings and exchange test data stored at remote sites using the wireless network. We are concerned that an ATCB that uses WEP to secure its wireless network may not have sufficient IT security knowledge to certify EHRs and to protect sensitive or proprietary data.

[10] Records may be in any medium, such as hard copy or an electronic format (ISO/IEC 17025:2005 § 4.13.1.2).

[11] NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.*

AUTHORIZED TESTING AND CERTIFICATION BODY STANDARDS MET REQUIREMENTS BUT NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY TEST PROCEDURES NEEDED STRENGTHENING

Standards and Procedures of Authorized Testing and Certification Bodies Met Requirements

The ATCBs' standards and procedures for testing and certifying EHRs met all the requirements of the NIST test procedures adopted by ONC.

Test Procedures Need Strengthening

The PHSA § 3004 (added by the HITECH Act) requires ONC to define the standards, implementation guides, and certification criteria for evaluating how EHRs conform to criteria for protecting electronic health information through implementing appropriate technical capabilities. ONC's standards, found at 45 CFR § 170.302, include several relating to security.[12] Regulations for the Temporary and Permanent Certification Programs require that ATCBs use testing procedures approved by ONC to evaluate conformance of EHRs to each of ONC's requirements.[13] ONC worked with NIST to develop these test procedures.[14]

ONC's approved NIST test procedures did not ensure that certified EHRs would secure patient information. For example, the test procedures allowed ATCBs to approve EHRs that demonstrated the use of a single-character password during testing. In addition, the NIST test procedures did not address common security issues, such as, but not limited to, password complexity and logging emergency access or user privileges changes. Without test procedures to address such common issues, ATCBs could continue to certify EHRs with vulnerabilities that could pose a significant risk to protection of EHR-related information.

CONCLUSION

The process of certifying EHRs is designed, in part, to give providers the confidence to know that patient health information is secure and protected. Our audit revealed vulnerabilities with the Temporary EHR certification program. These vulnerabilities could allow hackers to penetrate EHR systems, thereby compromising the integrity, confidentiality, and availability of patient information stored in and transmitted by a certified EHR.[15]

[12] 45 CFR §§ 170.302(o)–(u)).

[13] 45 CFR §§ 170.423(e) and 170.523(h).

[14] These procedures were approved by ONC in 75 Fed. Reg. 47817 (August 9, 2010).

[15] The use of a certified EHR for meaningful use attestation applies to all stages of meaningful use; therefore, all vulnerabilities related to certified EHRs also apply to all stages of meaningful use.

RECOMMENDATIONS

To ensure that each patient's health information in EHRs is secure and protected, we recommend that ONC require the ATCBs to:

- develop procedures to periodically evaluate whether certified EHRs continue to meet Federal standards and

- develop a training program to ensure that their personnel are competent to test and certify EHRs and to secure proprietary or sensitive EHR information.

We also recommend that ONC work with NIST to strengthen EHR test procedure requirements so that the ATCBs can ensure that EHR vendors incorporate common security and privacy features into the development of EHRs.

ONC COMMENTS

In written comments on our draft report, ONC stated that ATCBs are no longer active in the ONC Certification Program and that testing and certification functions are now performed by separate entities in the ONC Health IT Certification Program: Authorized Certification Bodies (ACBs) and Accredited Testing Laboratories. ONC also stated that although ONC ATCBs were not required to conduct surveillance activities during the Temporary Certification Program, ACBs are required to conduct surveillance, and ONC issued guidance on the subject in July 2013. In addition, ACBs must be accredited by the ONC-Approved Accreditor, which is the American National Standards Institute, as a condition of applying to become an ACB. ONC also stated that the 2014 Edition EHR Certification Criteria "strengthened test procedures for common security and privacy features for inclusion in EHRs."

Regarding our recommendation that ONC work with NIST to strengthen EHR test procedure requirements to ensure that EHR vendors incorporate into EHRs common security and privacy features, ONC stated that "the adopted criteria strive to set certain common baselines yet, at the same time, aim to allow EHR technology developers the flexibility to include and demonstrate innovative techniques to protect health information." ONC added that "it is the ONC's intention to work with health care providers to encourage and educate them on the use of multi-factor authentication in instances where its use can provide added protections to patient data." ONC's comments are included in their entirety as Appendix C.

OFFICE OF INSPECTOR GENERAL RESPONSE

We do not agree that the 2014 Edition EHR Certification Criteria sufficiently address our security concerns regarding the Temporary Certification Program. For example, the 2014 criteria do not address common security issues that we identified in our review of the Temporary Certification Program, such as password length and complexity or logging emergency access or user privilege changes.

We agree with ONC's statement that "the adopted criteria strive to set certain common baselines." However, ONC's baseline does not address certain specific security concerns and industry best practices. For example, multifactor authentication has been recommended by NIST since the publication of NIST SP 800-53 in February 2005. However, ONC still did not require multifactor authentication in the 2014 criteria. Therefore, we continue to recommend that ONC strengthen EHR Test Procedure requirements to address such issues to ensure providers have EHR systems that have adequate security and privacy features.

OTHER MATTERS

Neither the Temporary Certification Program nor the Permanent Certification Program directly addresses ONC's authority to remove a certified EHR from the Product List absent evidence of improper conduct by the ATCB.[16] Therefore, if an EHR is exploited and used to conduct malicious activities, ONC is not able to remove the EHR, even temporarily, from the Product List to prevent further purchases of it. In order to assure the public that certified EHRs on the Product List meet current security and privacy requirements, ONC would need to have the ability to decertify and remove obsolete, unsupported, or less secure EHRs on the basis of its own assessment of them or to otherwise have procedures to notify the public.

In addition, none of the five ATCBs we reviewed verified whether the EHRs that they certified were marketed for the specific operating systems for which they were tested. For example, even though an EHR was tested using Microsoft Windows, it could have been marketed as having been tested and certified under another operating system platform (e.g., iOS, Android, or Linux). Without standards requiring testing for specific operating systems, EHRs could have been used for operating systems that had an entirely different set of vulnerabilities, increasing the risks to the security and privacy of protected health information.

[16] See 45 CFR §§ 170.470 and 170.570.

APPENDIX A: FEDERAL AND INTERNATIONAL REQUIREMENTS ON THE TESTING AND CERTIFICATION OF ELECTRONIC HEALTH RECORDS

FEDERAL REQUIREMENTS FOR ONC

Section 3001(C) of the Recovery Act states that ONC must review Federal health IT investments to ensure that (1) Federal health IT programs are incorporating privacy and security protections for the electronic exchange of an individual's personally identifiable health information and that (2) security methods ensure appropriate authorization and electronic authentication of health information and include technologies or methodologies for rendering health information unusable, unreadable, or indecipherable.

Section 3001(b) of the Recovery Act states: "The National Coordinator shall perform the duties under subsection (c) in a manner consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information and that—(1) ensures that each patient's health information is secure and protected, in accordance with applicable law."

Section 3004(b)(1) of the PHSA requires "the Secretary of Health and Human Services to adopt an initial set of standards, implementation specifications, and certification criteria … to enhance the interoperability, functionality, utility, and security of health information technology."

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, states that the WEP suffers from cryptographic weaknesses that enable attackers with readily available software tools to decipher data.

INTERNATIONAL REQUIREMENTS FOR THE AUTHORIZED TESTING AND CALIBRATION LABORATORIES[17]

ISO/IEC 17025:2005 § 4.1.5, states that the testing laboratory must have policies and procedures to ensure the protection of its customers' confidential information and proprietary rights, including procedures for protecting the electronic storage and transmission of results.

ISO/IEC 17025:2005 § 4.13.1.3, states that all records[18] must be held secure and in confidence. Section 4.13.1.4 states that the laboratory must have procedures to protect and back up records stored electronically and to prevent unauthorized access to or amendment of these records.

ISO/IEC 17025:2005 § 5.2.1, states that personnel performing specific tasks must be qualified on the basis of appropriate education, training, experience, or demonstrated skills, as required. The personnel responsible for the opinions and interpretation included in test reports should have, in addition to having the appropriate qualifications, training, experience, and knowledge of the

[17] According to ONC's Principles of Proper Conduct, the ATCBs must comply with these international requirements.

[18] ISO/IEC 17025:2005 § 4.13.1.2 states that records may be in any medium, such as hard copy or electronic format.

testing carried out, knowledge of the general requirements and an understanding of the significance of deviations from the normal use of the items, materials, or products concerned.

ISO/IEC Guide 65:1996 § 13.4, states that the certification body must periodically evaluate EHRs to confirm that they continue to conform to the standards.

APPENDIX B: AUDIT SCOPE AND METHODOLOGY

SCOPE

We focused our audit on ONC's procedures for monitoring the ATCBs and assessed the ATCBs' effectiveness in testing and certifying EHRs. We limited our review to controls that were in effect at the time of our onsite visit to ONC and the ATCB offices. We did not review any of the 187 EHRs certified under the Permanent Program.

We conducted our fieldwork from January 24 through June 28, 2012, at ONC in Washington, DC, and at five ATCB offices: The Certification Commission for Health Information Technology (Chicago, Illinois), Drummond Group (Nashville, Tennessee), SLIGlobal (Denver, Colorado), ICSA Labs (Mechanicsburg, Pennsylvania), and InfoGard (San Luis Obispo, California).

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal requirements, NIST SPs, the Principles of Proper Conduct, ISO/IEC Guides 17025:2005 and 65:1996, and industry best practices;
- reviewed ATCBs' procedures related to violations/complaints, training, and the security of records in accordance with ISO/IEC Guides 17025:2005 and 65:1996;
- interviewed ONC officials responsible for monitoring ATCBs to help determine whether the ATCBs complied with the Principles of Proper Conduct;
- reviewed ONC documentation for monitoring ATCBs to determine whether the ATCBs complied with the Principles of Proper Conduct;
- interviewed ATCB testers and other individuals about their procedures for testing and certifying EHRs;
- judgmentally selected 30 EHRs and reviewed supporting documentation for each; and
- discussed our findings with ONC.

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 findings and conclusions based on our audit objectives.

APPENDIX C: ONC COMMENTS

The Office of the National Coordinator for Health Information Technology

Improving health and health care for all Americans through the use of information and technology

TO: Daniel R. Levinson
Inspector General

FROM: Dr. Karen B. DeSalvo
National Coordinator, Office of the National Coordinator for Health Information Technology

SUBJECT: The ONC's Response to Office of Inspector General (OIG) Draft Report -- The Office of the National Coordinator for Health Information Technology's Oversight of the Testing and Certification of Electronic Health Records (A-06-11-00063)

Thank you for the opportunity to respond to the subject report. It is important to remember that the program which the OIG reviewed is no longer in existence. Specifically, the Authorized Testing and Certification Bodies (ATCBs) are no longer active in the ONC Certification Program. ATCBs participated in the Temporary Certification Program which ended in 2012 and now testing and certification functions are performed by separate entities in the ONC Health IT Certification Program. Testing is performed by Accredited Testing Laboratories (ATLs), and certification is performed by Authorized Certification Bodies (ACBs). ACBs are required to perform surveillance activities on certified electronic health records (EHRs) and have trained, competent personnel. In addition, the OIG, when conducting their study, looked at the 2011 Edition EHR certification criteria, rather than the more recent 2014 Edition EHR certification criteria. The 2014 Edition HER certification criteria strengthened test procedures for common security and privacy features for inclusion in EHRs.

The ONC's response to the recommendations identified in the subject report is provided below:

OIG Recommendation 1
ONC require the ATCBs to develop procedures to periodically evaluate whether certified EHRs continue to meet Federal standards.

ONC Response
ONC-Authorized Testing and Certification Bodies (ONC-ATCBs) are no longer operational as part of the ONC HIT Certification Program. ONC-ATCBs were only granted authorization to operate during the Temporary Certification Program, which was the first step of the two-step process ONC used to develop its HIT Certification Program for the purposes of testing and certifying health information technology. The Temporary Certification Program ended October 2012, at which point the permanent ONC HIT Certification Program, the second part of the two-part process, was launched.

ONC-ATCBs were encouraged, but not required, to conduct surveillance activities during the Temporary Certification Program. However, under the ONC HIT Certification Program, ONC-Authorized Certification Bodies (ONC-ACBs) are required to conduct surveillance and ONC

issued its first annual guidance in July 2013 (Program Policy Guidance 13-01) to inform ONC-ACBs priorities.[1] Moreover, testing and certification must be performed by separately accredited lines of business. Testing laboratories must be accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) (to ISO 17025 – International Standard Organization standard for test laboratories) and certification bodies must be accredited by the ONC-Approved Accreditor, which is American National Institute of Standards (ANSI) (to ISO Guide 65 – International Standard Organization guide for Certification Bodies).

ONC-ACBs are required to perform surveillance activities to evaluate whether the products they certify continue to perform according to the standards to which they were certified. Their surveillance efforts include both proactive and reactive surveillance. For example, ONC-ACBs perform random audits of certified products, according to their individual surveillance plans. Also, reactive surveillance activities are implemented if complaints are received for a particular product.

OIG Recommendation 2

ONC require the ATCBs to develop a training program to ensure that their personnel are competent to test and certify EHRs and to secure proprietary or sensitive EHR information.

ONC Response

Certification bodies under the ONC HIT Certification Program must be accredited by the ONC-Approved Accreditor, ANSI, as a condition of applying to become an ONC-ACB. The accreditation process, and standard to which ANSI evaluates certification bodies, requires that those certification bodies have trained personnel, and maintain competencies, to secure sensitive EHR information. Further, the ONC- Approved Accreditor is responsible for overseeing the certification bodies' adherence to the standard and for re-evaluating the accreditation it issues on an annual basis.

OIG Recommendation 3

ONC will work with NIST to strengthen EHR test procedure requirements so that the ATCBs can ensure that EHR vendors incorporate common security and privacy features into the development of EHRs.

ONC Response

Requirements for EHR testing and certification are adopted through regulation on a cyclical basis. The adopted standards and certification criteria are meant to serve as a floor and not a ceiling. That is, the adopted criteria strive to set certain common baselines yet, at the same time, aim to allow EHR technology developers the flexibility to include and demonstrate innovative techniques to protect health information. Over the long-term, it is the ONC's intention to work with health care providers to encourage and educate them on the use of multi-factor authentication in instances where its use can provide added protections to patient data. In that regard, test procedures are updated when certification criteria are updated to reflect new regulatory requirements. Test procedures cannot be modified in a manner that would impose requirements beyond those for which certification is required.

[1] http://www.healthit.gov/sites/default/files/onc-acb_2013annualsurveillanceguidance_final_0.pdf

During the course of its study, the OIG focused on the 2011 Edition EHR certification criteria. ONC subsequently issued the 2014 Edition EHR certification criteria in a final rule on September 4, 2012. The 2014 Edition EHR certification criteria, and the associated test procedures, have since been updated. ONC consulted with NIST information security subject matter experts as the test procedures were developed and also made the test procedures available for public comment, which allowed for private sector stakeholder/experts to submit feedback as well. The attached document provides a comparison between the 2011 Edition and 2014 Edition privacy and security certification criteria, which demonstrates the strengthened privacy and security requirements and inclusion of additional privacy and security capabilities as part of EHR technology certification.

Dr. Karen B. DeSalvo
National Coordinator, ONC

5/9/14
Date

Attachment:

- Comparison of Privacy and Security Certification Criteria

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
Authentication. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. Access control. Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.	(d)(1) Authentication, access control, and authorization. (i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i), and the actions the user is permitted to perform with the EHR technology.	We merged these capabilities to allow for more efficient testing and consistency with EHR technology development.
Audit log. (1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). (2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at §170.210(b). ***Standard*** (b) Record actions	(2) Auditable events and tamper-resistance. (i) Record actions. EHR technology must be able to: (A) Record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1); (B) Record the audit log status (enabled or disabled) in accordance with the standard specified in §170.210(e)(2) unless it cannot be disabled by any user; and (C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in §170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section). (ii) Default setting. EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (C), or both paragraphs (d)(2)(i)(B) and (C). (iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that EHR	Based on HITSC recommendations and stakeholder feedback, we split the 2011 Edition certification criterion into two separate certification criteria (+ added the "detection" capability from the "integrity" certification criterion). This will permit a wider variety of EHR technologies to be certified as EHR Modules. We expanded upon the scope of the HITSC's recommendation to address input from the HHS Office of Inspector General (May 2011 report/ http://oig.hhs.gov/oas/reports/other/180930160.pdf) and to reflect our general belief that a more stringent certification policy for audit logs will ultimately assist EPs, EHs, and CAHs to better detect and investigate breaches. We

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.	technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) Detection. EHR technology must be able to detect whether the audit log has been altered. (3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards at § 170.210(e). ***Standard(s)*** 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (1)(i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at §170.210(h) when EHR technology is in use. (ii) The date and time must be recorded in accordance with the standard specified at §170.210(g). (2)(i) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the audit log status is changed. (ii) The date and time each action occurs in accordance with the standard specified at §170.210(g). (3) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at §170.210(g). 170.210(g) Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following Request for Comments (RFC) 1305 Network Time Protocol (NTP) (Version 3) or RFC 5905 NTPv4.	adopted the consensus standard ASTM E2147-01 and the "synchronized clocks" standard.

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
	170.210(h) Audit log content. ASTM E2147-01(Reapproved 2009).	
Integrity. Create a message digest in accordance with the standard specified in § 170.210(c). Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered. [1]Detection. Detect the alteration of audit logs.	(d)(8) Integrity. (i) Create a message digest in accordance with the standard specified in § 170.210(c). (ii) Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered. § 170.210(c) *Verification that electronic health information has not been altered in transit. Standard.* A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-4 (March 2012)) must be used to verify that electronic health information has not been altered.	This certification criterion is consistent with the HITSC's recommendation. We moved the "detection" capability to the "auditable events and tamper resistance" certification criterion. We updated the NIST FIPS publication to 180-4 from 180-3.
Automatic log-off. Terminate an electronic session after a predetermined time of inactivity.	(d)(5) Automatic log-off. Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity. "After a period of inactivity the EHR technology must make a user's session inaccessible and subsequently require the user to re-authenticate using the same credentials used to begin or resume the session." "We clarify that this certification criterion is not meant to result in the termination of network connections, especially network connections that are not in use by the EHR technology, but by other applications."	This clarifies ambiguity and is also consistent with the language used for the "session lock" security control specified in NIST 800-53 rev3.
Emergency access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.	(d)(6) Emergency access. Permit an identified set of users to access electronic health information during an emergency.	We provided clarity. The certification criterion more clearly conveys the capabilities included and aligns with our consistent use of the phrase "identified set of users" in every certification criterion where we intend for the same

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
		capability to be available. We explained that the purpose of this certification criterion is to provide certain users (''identified set of users'') with the ability to override normal access controls in the case of an emergency.
General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in § 170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology.	(d)(7) End-user device encryption. Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion. (i) EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops. (A) Electronic health information that is stored must be encrypted in accordance with the standard specified in §170.210(a)(1). (B) Default setting. EHR technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users. (ii) EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.	This approach is more practical, effective, and easier to implement than the 2011 Edition general encryption requirement. It is consistent with the HITSC views that we should focus more attention on promoting EHR technology to be designed to secure electronic health information on end-user devices (which are often a contributing factor to a breach of protected health information). Further, the OIG provided similar rationale in its May 2011 report (previously cited under the discussion of the *''auditable events and tamper resistance'' and ''audit report(s)'' certification criteria*) in which it recommended that ONC address IT security controls for encrypting data on mobile devices.
Encryption when exchanging electronic health information. Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in § 170.210(a)(2).	N/A	We specify in our preamble discussion of the "view, download, and transmit to 3rd party" certification criterion that for EHR technology to be certified to either the "view, download, and transmit to 3rd party" certification criterion or the "transition of care - create and transmit summary care record" certification criterion it must be capable of performing transmissions in

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
		accordance with the proposed transport standards (which provide for encryption and integrity protection). Because of these proposed requirements, adopting a certification criterion similar to the 2011 Edition "encryption when exchanging" would have been redundant. In addition, we explicitly require that EHR technology have the capability to encrypt while exchanging to meet the proposed new secure messaging certification criterion.
Optional. Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d).	(d)(9) Optional. Accounting of disclosures. Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in § 170.210(d).	N/A
N/A	(d)(4) Amendments. Enable a user to electronically select the record affected by a patient's request for amendment and perform the capabilities specified in paragraphs (d)(4)(i) or (ii) of this section. (i) Accepted amendment. For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location. (ii) Denied amendment. For a denied amendment, at a minimum, append the request and denial of the request to the affected record or include a link that indicates this information's location.	We adopted this certification criterion based public comment and on HITPC and HITSC recommendations which included that a certification criterion should be adopted that provides some of the basic technical tools to support compliance with the HIPAA Privacy Rule. We noted in the rules that the certification criterion does not address all of the requirements specified at 45 CFR 164.526 and that EHR technology certification is not a substitute for, or guarantee of, HIPAA Privacy Rule compliance.
N/A	(e)(3) Ambulatory setting only—secure	This is new certification

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
	messaging. Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: (i) Both the patient (or authorized representative) and EHR technology user are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f). ***Standard*** § 170.210(f) Encryption and hashing of electronic health information. Any encryption and hashing algorithm identified by NIST as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2.	criterion that supports secure provider/patient communication. We adopted a baseline standard in terms of the encryption and hashing algorithms that would need to be used to implement secure messaging. This will permit a wide range of different secure messaging solutions, that will likely use different approaches and transport standards. This includes reference to an updated version of Annex A and updated NIST PIPS publications for the AES standard.
N/A	(e)(1) View, download, and transmit to 3rd party. (i) EHR technology must provide patients (and their authorized representatives) with an online means to view, download, and transmit to a 3rd party the data specified below. Access to these capabilities must be through a secure channel that ensures all content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at §170.210(f). (A) View. Electronically view in accordance with the standard adopted at §170.204(a), at a minimum, the following data: * * * (B) Download. (*1*) Electronically download an ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested) in human readable format or formatted according to the standard adopted at §170.205(a)(3) that includes, at a minimum, the following data (which, for the human readable version, should be in their English representation if they associate with a vocabulary/code set): * * * (C) Transmit to third party. (*1*) Electronically transmit the ambulatory summary or inpatient summary (as applicable to the EHR technology setting for which certification is requested)	This is a new certification criterion that supports patients' access to their health information. As required by the criterion, access to these capabilities must be through a secure channel that ensures all content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at §170.210(f). This is the same baseline standard as adopted for the "secure messaging" certification criterion. This ensures privacy and security requirements when health information is externally accessed or exchanged. The Activity history log must comply with the "synchronized clocks" standard (170.210(g)).

Comparison of Privacy and Security Certification Criteria		
2011 Edition	**2014 Edition**	**Change Analysis**
	created in paragraph (e)(1)(i)(B)(*1*) of this section in accordance with the standard specified in §170.202(a). * * * (ii) Activity history log. (A) When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A) through (C) of this section, the following information must be recorded and made accessible to the patient: (*1*) The action(s) (i.e., view, download, transmission) that occurred; (*2*) The date and time each action occurred in accordance with the standard specified at §170.210(g); and (*3*) The user who took the action. (B) EHR technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) of this section if it is also certified to the certification criterion adopted at §170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.	

Many of the revised privacy and security certification criteria for the 2014 Edition were grounded in recommendations of the HITSC and the FACA Privacy and Security Tiger Team. The revised certification criteria were also developed in consultation with NIST. Overall, they add, enhance, and clarify the privacy and security capabilities required of EHR technology.