Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

NOT ALL RECOMMENDED FRAUD SAFEGUARDS HAVE BEEN IMPLEMENTED IN HOSPITAL EHR TECHNOLOGY

Daniel R. Levinson
Inspector General

December 2013
OEI-01-11-00570

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 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: Not All Recommended Safeguards Have Been Implemented in Hospital EHR Technology
OEI-01-11-00570

WHY WE DID THIS STUDY

Electronic health records (EHRs) replace traditional paper medical records with computerized recordkeeping to document and store patient health information. Experts in health information technology caution that EHR technology can make it easier to commit fraud. The Office of the National Coordinator for Health Information Technology (ONC), which coordinates the adoption, implementation, and exchange of EHRs, contracted with RTI International (RTI) to develop recommendations to enhance data protection; increase data validity, accuracy, and integrity; and strengthen fraud protection in EHR technology. This study determined how hospitals that received EHR Medicare incentive payments, administered by the Centers for Medicare & Medicaid Services (CMS), had implemented recommended fraud safeguards for EHR technology.

HOW WE DID THIS STUDY

We administered an online questionnaire to the 864 hospitals that received Medicare incentive payments as of March 2012. The questionnaire focused on the presence of features and capabilities in Certified EHR Technology based on the RTI-recommended safeguards regarding audit functions, EHR user authorization and access, and EHR data transfer. We also conducted onsite structured interviews with hospital staff and observed a demonstration of the hospitals' Certified EHR Technology in eight hospitals. Finally, we conducted structured surveys with four EHR vendors and asked them the extent to which they had incorporated recommended fraud safeguards into their products.

WHAT WE FOUND

Nearly all hospitals with EHR technology had RTI-recommended audit functions in place, but they may not be using them to their full extent. In addition, all hospitals employed a variety of RTI-recommended user authorization and access controls. Nearly all hospitals were using RTI-recommended data transfer safeguards. Almost half of hospitals had begun implementing RTI-recommended tools to include patient involvement in anti-fraud efforts. Finally, only about one quarter of hospitals had policies regarding the use of the copy-paste feature in EHR technology, which, if used improperly, could pose a fraud vulnerability.

WHAT WE RECOMMEND

We recommend that audit logs be operational whenever EHR technology is available for updates or viewing. We also recommend that ONC and CMS strengthen their collaborative efforts to develop a comprehensive plan to address fraud vulnerabilities in EHRs. Finally, we recommend that CMS develop guidance on the use of the copy-paste feature in EHR technology. CMS and ONC concurred with all of our recommendations.

TABLE OF CONTENTS

Objectives 1

Background 1

Methodology 7

Findings 9

Nearly all hospitals with EHR technology had RTI-recommended audit functions in place, but they may not be using them to their full extent 9

All hospitals employed a variety of RTI-recommended user authorization and access controls 12

Nearly all hospitals were using RTI-recommended data transfer safeguards 13

Almost half of hospitals had begun implementing RTI-recommended tools to include patient involvement in anti-fraud efforts 13

Only about one quarter of hospitals had policies regarding the use of the copy-paste feature in EHR technology 14

Conclusion and Recommendations 15

Agency comments and Office of Inspector General response 17

Appendixes 18

A: RTI Recommendations and General Consistency With ONC Certification Criteria or CMS Meaningful Use 18

B: Nonrespondent Analysis 20

C: Agency Comments 21

Acknowledgments 26

OBJECTIVES

1. To assess the extent to which hospitals that had received electronic health record (EHR) Medicare incentive payments implemented recommended fraud safeguards for EHR technology in the following categories:
    - audit functions,
    - user authorization and access controls,
    - data transfer standards, and
    - patient involvement in anti-fraud activity.
2. To assess the extent to which hospitals had implemented policies to address inappropriate copy-paste in EHRs.

BACKGROUND

Electronic Health Records

EHRs replace traditional paper medical records with computerized recordkeeping to document and store patient health information. EHRs may include patient demographics, progress notes, medications, medical history, and clinical test results from any health care encounter.[1] Vendors create EHR technology that includes a variety of applications and tools for collecting, managing, and sharing patient information electronically and for clinical decisionmaking.

Health Information Technology for Economic and Clinical Health Act

The Health Information Technology for Economic and Clinical Health Act (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) to support the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information.[2] Its goal is to achieve widespread adoption of EHRs by 2014. The Office of the National Coordinator for Health Information Technology (ONC) coordinates the adoption, implementation, and exchange of EHRs.

To encourage adoption and meaningful use of EHRs, ARRA also established the Medicare and Medicaid EHR incentive programs.[3] Since

[1] CMS, *Electronic Health Records Overview*. Accessed at http://www.cms.gov on Jan. 11, 2011.
[2] P.L. 111-5, Title XIII.
[3] ARRA, Title IV, P.L. 111-5.

2011, the Centers for Medicare & Medicaid Services (CMS) has paid $13.5 billion in incentive payments to eligible professionals and hospitals that demonstrate meaningful use of Certified EHR Technology.[4] Medicare professionals and hospitals will face payment adjustments under Medicare starting in 2015 for failing to successfully demonstrate meaningful use of Certified EHR Technology.[5]

EHR Certification Criteria. Hospitals must use Certified EHR Technology to receive EHR incentive payments. Certified EHR Technology must be able to perform specified functions, such as enabling a user to electronically record, modify, and retrieve patient information.[6] ONC oversees the EHR certification process.

Meaningful Use Criteria. Federal regulations established meaningful use measures for hospitals.[7] These measures address EHR capabilities meant to improve health care quality and efficiency, such as computerized provider order entry, e-prescribing, and exchange of key clinical information. CMS is promulgating regulations specifying criteria to meet meaningful use in three stages.[8] Stage 1 criteria set the baseline for electronic data capture and information sharing. CMS released Stage 2 final rules in September 2012, which focus on advanced functionality of EHRs, including interoperability, patient engagement, clinical decision support, and quality measurement.[9] CMS expects to propose Stage 3 criteria at a later date.

EHR Fraud Vulnerabilities

The full extent of health care fraud is unknown, but it is substantial. The annual cost of health care fraud is between $75 billion and $250 billion. These figures are based on CMS estimates of total health care expenditures in 2009.[10] Experts in health information technology caution

---

[4] CMS, *Medicare and Medicaid Incentive Provider Payments by State. Program Type: January 2011-March 2013.* Accessed at http://www.cms.gov on April 25, 2013.

[5] See §§ 1848(a)(7), 1853(l)(4), and 1886 (b)(3)(B), as enacted in ARRA. See also CMS, *CMS Finalizes Requirements for the Medicare EHR Incentive Program*. Accessed at http://www.cms.gov on Jan. 3, 2012.

[6] 45 CFR §§ 170.302, 170.306, and 170.314. At the time of our review, hospitals were required to be certified as meeting the 2011 EHR Certification Criteria to receive EHR incentive payments. Beginning on October 1, 2013, hospitals must be certified as meeting the 2014 EHR Ceritfication Criteria to receive EHR incentive payments.

[7] 42 CFR Part 495.

[8] CMS, *EHR Meaningful Use Overview*. Accessed at http://www.cms.gov on March 7, 2012. See 42 CFR Part 495.

[9] 77 Fed. Reg. 53968 (Sept. 4, 2012).

[10] CMS, *National Health Expenditure Data*. Accessed at http://www.cms.gov on Jan. 3, 2012.

that EHR technology can make it easier to commit fraud.[11] Certain EHR documentation features, if poorly designed or used inappropriately, can result in poor data quality or fraud. Below we describe two examples of EHR documentation practices that could be used to commit fraud.

Copy-Pasting. Copy-pasting, also known as cloning, allows users to select information from one source and replicate it in another location.[12] When doctors, nurses, or other clinicians copy-paste information but fail to update it or ensure accuracy, inaccurate information may enter the patient's medical record and inappropriate charges may be billed to partients and third-party health care payers. Furthermore, inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims.

Overdocumentation. Overdocumentation is the practice of inserting false or irrelevant documentation to create the appearance of support for billing higher level services. Some EHR technologies auto-populate fields when using templates built into the system. Other systems generate extensive documentation on the basis of a single click of a checkbox, which if not appropriately edited by the provider, may be inaccurate. Such features can produce information suggesting the practitioner preformed more comprehensive services than were actually rendered.[13]

Recommended EHR Fraud Management Safeguards

In 2006, ONC contracted with RTI International (RTI) to develop recommendations to enhance data protection; increase data validity, accuracy, and integrity; and strengthen fraud protection in EHR technology. RTI convened industry experts, including providers, payers, and EHR technology vendors, to develop 14 functional recommendations that offer the highest benefit in reducing waste due to fraud and data inaccuracies.[14] These recommendations addressed several types of vulnerabilities, including copy-paste and overdocumentation. RTI

---

[11] Dougherty, Michelle. *HIT Policy Committee Hearing on Clinical Documentation*, February 13, 2013. Accessed at http://www.healthit.gov on March 19, 2013.

[12] Association of American Medical Colleges, Compliance Officers' Forum. *Appropriate Documentation in an EHR: Use of Information That Is Not Generated During the Encounter for Which the Claim Is Submitted: Copying/Importing/Scripts/Templates*. July 11, 2001.

[13] Dougherty, Michelle. *HIT Policy Committee Hearing on Clinical Documentation*, February 13, 2013. Accessed at http://www.healthit.gov on March 19, 2013.

[14] ONC, *Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems*. June 2007. Accessed at http://www.rti.org/pubs/enhancing_data_quality_in_ehrs.pdf on May 20, 2013.

reported that incorporating these 14 recommendations could increase data quality and reduce exposure to "new and ever-evolving forms of electronically enabled health care fraud." (See Table 1. Numbers in parentheses are the RTI recommendation numbers.)

Usage policies and technology features could help prevent EHR fraud if used consistently. However, providers that use EHR technology can disable or bypass these features, potentially making them ineffective. For this analysis, we have grouped the 14 recommendations into categories of fraud safeguards, including: audit functions, user authentication and access controls, data transfer standards, and patient involvement in anti-fraud.

Table 1: RTI Recommendations Grouped Into Fraud Safeguard Categories

RTI Recommendations
Audit Functions
1) Requires the use of an audit log function and specifies audit log operation and content for tracking EHR updates. (4.2.1)
2) Requires that the methods (i.e., copy/paste, direct entry, import) for any update to an EHR be documented and tracked. (4.2.4)
3) Requires that the user ID of the original author be tracked when an EHR update is entered "on behalf" of another author (i.e., distinguish between entries made by an assistant and a provider). (4.2.6)
4) Requires that EHR technology be able to record and indicate the method used to confirm patient identity (i.e., photo identification, prior relationship). (4.2.11)
5) Requires that original EHR documents be retained after they are signed off and modifications be tracked as amendments. (4.2.7)
User Authorization and Access Controls
6) Requires the use of user IDs and passwords to restrict unauthorized access to EHRs. (4.2.3)
7) Requires the use of a provider's National Provider Identifier to restrict EHR access and track updates to EHRs by author. (4.2.2)
8) Requires that EHR technology support an "auditor" class of user to have read-only access to patient records. (4.2.8)
Data Transfer Standards
9) Requires that a document ID tracking number be generated and attached to an EHR any time an EHR is exported (i.e., printed or electronically communicated). (4.2.9)
10) Requires that EHRs be exchanged using certain data standards (encryption) to ensure that data have not been altered during the transmission. (4.2.13)
11) Requires that EHR technology have the capacity to directly capture clinical information in structured and coded data and not impact EHR user productivity. (4.2.12)
Patient Involvement in Anti-Fraud
12) Requires that patients be able to access and comment within their EHRs. (4.2.10)
Other
13) Requires that information transmitted for payment of claims be accurately linked and tracked to the appropriate EHR. (4.2.14)
14) Requires that EHR technology not prompt an EHR user to add documentation but be able to alert a user to inconsistencies between documentation and coding. (4.2.5)

Source: OIG analysis of RTI's recommended requirements for enhancing data quality in EHR systems, 2013.

Audit Functions. Audit functions, such as audit logs, track access and changes within a record chronologically by capturing data elements, such as date, time, and user stamps, for each update to an EHR. An audit log can be used to analyze historical patterns that can identify data inconsistencies. To provide the most benefit in fraud protection, audit logs should always be operational while the EHR is being used and be stored as long as clinical records. Users should not be able to alter or delete the contents of the audit log.

User Authorization and Access Controls. Access controls are policies and EHR technology features that require unique identifiers, passwords, and user authentication to help prevent inappropriate access to EHRs. Such access controls discourage fraud schemes that involve stealing provider and patient information to submit false claims. These controls can also validate claims by verifying that services align with provider profiles associated with unique identifiers.

Data Transfer Standards. These standards are technology features that restrict the printing, transferring, or exporting of EHR data by requiring a distinct authorization and additional documentation and tracking elements. Unrestricted export of EHRs could make patient information readily available to create fraudulent claims.

Patient Involvement in Anti-Fraud. EHR technology can allow patients to view their medical records and make comments in their EHRs. Patients may be able to help detect potentially fraudulent activity by identifying errors and validating the services that they receive from their providers.

In addition, these 14 recommendations can be broken down into 60 individual criteria, one-third of which focus on audit log functions and features, highlighting audit logs as an important fraud safeguard.

Although ONC posted RTI's recommendations on its Web site, its certification criteria and CMS's meaningful use measures do not specifically address all of RTI recommendations. For example, RTI lists detailed requirements for the functions that the audit log should be able to perform. Although ONC certification criteria require that certified EHRs have an audit log, they do not require it to be operational at all times as recommended by RTI. (See Appendix A for a summary of RTI's 14 requirements and general consistency with ONC certification criteria or CMS meaningful use objectives).

Related Office of Inspector General Work

The Office of Inspector General (OIG) will release a companion report to this one that describes the program integrity practices CMS and its contractors have implemented in light of EHR adoption.[15] OIG considers the effective use of data and technology, including EHRs, to be a top management challenge facing the Department and its operating divisions.[16]

In 2012, OIG released a report on physicians' reported use of EHR technology that found that 57 percent of Medicare physicians used an EHR at their primary practice locations in 2011. Additionally, three of every four Medicare physicians with an EHR system used a certified system to document evaluation and management services. [17] OIG is currently determining the extent to which documentation errors were facilitated by using EHR technology.[18]

In 2012, OIG released a study that found that CMS faces obstacles to overseeing the Medicare EHR incentive program that leave the program vulnerable to paying incentives to professionals and hospitals that do not fully meet the meaningful use requirements.[19]

In 2011, OIG released an audit of information technology (IT) controls in health IT standards. OIG found that ONC EHR certification criteria focused on IT security application controls for communication between EHR systems, but did not include basic, general IT security controls.[20]

---

[15] OIG, *CMS and Its Contractors Have Adopted Few Program Integrity Practices To Address Vulnerabilities in EHRs,* OEI-01-11-00571, in progress.

[16] OIG, *2012 Top Management and Performance Challenges*, 2012.

[17] OIG, *Use of Electronic Health Record Systems in 2011Among Medicare Physicians Providing Evaluation and Management Services*, OEI-04-10-00184, June 2012.

[18] OIG, OEI-04-10-00182, in progress.

[19] OIG, *Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program*, OEI-05-11-00250, November 2012.

[20] OIG, *Audit of Information Technology Security Included in Health Information Technology Standards*, A-18-09-30160, May 2011.

METHODOLOGY

SCOPE

This study determined the extent to which hospitals that received EHR Medicare incentive payments between January 2011 and March 2012 implemented safeguards to protect against health care fraud. This study also assessed the extent that hospitals have implemented copy-paste policies.

Data Sources

Hospital Questionnaires: We administered an online questionnaire to 864 hospitals between October 2012 and January 2013 to learn about the Certified EHR Technology hospitals are using. We obtained a list from CMS of all hospitals (877) that received Medicare incentive payments for demonstrating meaningful use of Certified EHR Technology as of March 2012. The questionnaire focused on the presence of features and capabilities in Certified EHR Technology based on the RTI-recommended safeguards regarding audit logs, EHR access, and EHR data transfer. The questionnaire also asked about barriers to adopting selected RTI recommended fraud and abuse safeguards. Prior to our data collection, we reviewed the RTI recommendations with ONC, CMS, and external stakeholders and confirmed that these recommendations were relevant and appropriate. We had a 95-percent response rate. See Appendix B for a nonrespondent analysis.

Hospital Site Visits: We chose eight hospitals for site visits on the basis of geographic diversity, number of beds, and ownership type. While onsite, we conducted structured interviews with hospital staff and observed a demonstration of the hospitals' Certified EHR Technology. We conducted site visits in August and September 2012.

EHR Vendor Interviews: We conducted structured interviews with four EHR vendors that develop Certified EHR Technology products for hospitals. We selected five EHR vendors that together represented at least 50 percent of the market share of Certified EHR Technology products used in hospitals that received Medicare incentive payments. We removed one EHR vendor/health care company from our sample because its products were not commercially available and were designed for its own health care facilities. We asked EHR vendors about the extent to which they had incorporated recommended fraud and abuse safeguards into their products. We had a 100-percent response rate to our request for interviews.

Limitations

Our analysis used self-reported data from hospitals and EHR vendors. We did not independently verify their responses. This study did not assess whether individual EHR technology products were capable of implementing RTI recommendations. We also did not verify that hospital's EHR technology met ONC certification criteria as all the hospitals we surveyed attested to using ONC certified technology. In addition, we did not address vulnerabilities associated with hardware or those covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

Our analysis did not assess each of the 60 individual criteria specified in the 14 recommendations that RTI developed. Changes in EHR technology made some criteria less relevant to our assessment than when they were developed 6 years ago.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

Nearly all hospitals with EHR technology had RTI-recommended audit functions in place, but they may not be using them to their full extent

Ninety-six percent of hospitals reported that their audit logs remain operational at all times despite reporting barriers, including limited human resources, a lack of vendor-provided audit log user guides, and inadequate training on audit log functionality. Audit logs monitor user activity and are an important tool against fraud in EHRs. They are so important that one-third of RTI's recommended safeguards concern audit log operation and content.

Hospitals' EHR audit logs captured most RTI-recommended data

Generally, hospitals' audit logs captured the RTI-recommended data for each entry or access to the EHR, modification to the EHR, and signature event.[21] Almost all hospitals' audit logs recorded the date and time of entry, the user identification, and the type of access to the EHR (e.g., creating, editing, viewing). See Table 2 for details on the data that hospitals' EHR audit logs capture.

Fewer hospitals' audit logs captured data when an EHR user released an encounter for billing, exported or imported an EHR document, or disabled the audit log. In addition, hospital audit logs are less likely to record the method of data entry (e.g., direct text entry, speech recognition, automated) or the original date, time, and user identification when data are copy-pasted.

[21] A signature event is the proactive or auto default completion of a patient encounter.

Table 2: Percentage of Hospitals That Report Their Audit Logs Capture RTI-Recommended Data

When Data Are Recorded	Percentage of Hospitals' Audit Logs
Each entry or access to an EHR	99%
Each time a user modifies an EHR	99%
Each signature event (proactive or automatic completion of an encounter)	92%
Each time a user releases an encounter for billing	85%
Each export of an EHR document	81%
Each import of an EHR document	79%
Each time a user disables the audit log	61%
What Data Are Recorded	**Percentage of Hospitals' Audit Logs**
Date, time, and user identification	100%
Access type (creating, editing, or viewing data)	96%
Synchronized network time protocol	80%
Data, time, user ID of original author when data are entered on behalf of another	67%
Internet protocol address (i.e., location of user accessing EHR)	61%
Date, time, user ID of original author when data are copied	49%
The method used when data are entered into the EHR (such as direct text entry, speech recognition, automated, copy-paste)	44%
National Provider Identifier	33%

Source: OIG analysis of hospitals' responses to Certified EHR Technology questionnaire, 2012.

Most hospitals stored audit log data according to RTI recommendations

Some EHR vendors we spoke with stated that costs associated with additional storage space for audit logs may be a challenge for some hospitals; nevertheless, 67 percent of hospitals reported storing audit log data indefinitely. Only 10 percent of hospitals reported storing audit log data for less than 5 years. See Table 3 for how long hospitals reported storing audit log data. One vendor explained that it was easy to add storage space and discontinue collecting redundant or less useful audit log data to increase storage capacity. Several hospitals reported archiving audit log data prior to deleting them from their servers, which saves space and improves system processing speeds. RTI recommends that hospitals store audit log data as long as clinical records. This is important so that audit log data are available for fraud detection.

Table 3: Length of Time Hospitals Reported Storing Audit Log Data

Length of Time Audit Log Data Are Stored	Percentage of Hospitals
≤ 12 months	5%
1-5 years	5%
6-10 years	9%
≥ 11 years	1%
Indefinitely	67%
Other	13%

Source: OIG analysis of hospitals' responses to Certified EHR Technology questionnaire, 2012.

Hospitals' control over audit logs may be at odds with their RTI-recommended use as fraud safeguards

RTI recommends that EHR users not be allowed to delete the contents of their audit log so that data are always available for fraud detection, yet nearly half of hospitals (44 percent) reported that they can delete their audit logs. Although these hospitals reported that they limit the ability to delete the audit log to certain EHR users, such as system administrators, one EHR vendor noted that any software programmer could delete the audit log.

RTI recommends that the ability to disable the audit log be limited to certain individuals, such as system administrators, and that EHR users, such as doctors and nurses, be prevented from editing the contents of the audit log because these actions can compromise the audit log's effectiveness. Hospitals reported they have the ability to disable (33 percent) and edit (11 percent) their audit logs, although they reported restricting those abilities to certain EHR users, such as system administrators or EHR vendors. All four EHR vendors we spoke with reported that the audit logs cannot be disabled in their products, but one vendor again noted that a programmer could disable the audit log.

Most hospitals reported analyzing audit log data; however, their efforts appeared limited to ensuring privacy of patient data rather than detecting and preventing fraud and abuse

None of the hospitals we visited analyzed their audit logs to prevent or detect fraud, such as by identifying duplicate or fraudulent claims and inflated billing. Rather, all eight hospitals we visited described their audit log analyses as focused on privacy, such as detecting unauthorized viewing of an EHR of a celebrity, family member, or hospital employee. EHR vendors confirmed that their hospitals use the audit log as a HIPAA

compliance tool rather than a tool to detect fraud. One vendor reported that hospitals were generally not aware of all the audit log features available to them. For example, all four EHR vendors explained that they provide standard product implementation and training and that hospitals do not commonly ask for additional audit log training.

Most hospitals (95 percent) reported that they analyze audit log data. Forty-six percent of hospitals reported analyzing audit logs monthly, and 26 percent of hospitals conducted analysis on an as-needed basis. Hospitals cited barriers to analyzing audit logs, including limited human resources, a lack of vendor-provided user guides for audit log functionality, inadequate training on audit logs, and the inability to interpret audit log data.

All hospitals employed a variety of RTI-recommended user authorization and access controls

All hospitals reported that they authenticate EHR users via a unique user identification and password. Some hospitals had implemented stronger user authentication tools, such as tokens (21 percent of hospitals), public key infrastructure (14 percent), and biometrics (7 percent).[22] Hospitals also reported implementing additional safeguards to ensure appropriate access to the EHRs. Over 98 percent of hospitals had implemented automatic user logoffs after a set period of time, minimum user password configurations, and user agreements to access EHR technology. Eighty-six percent of hospitals required users to regularly change passwords. RTI recommends that EHR technology support strong user access authentication safeguards that evolve as technology advances to limit inappropriate access to EHRs.

Eighty-six percent of hospitals allowed outside entities to access their EHR data. Hospitals may define outside entities differently to include a variety of individuals and organizations, such as insurance companies, auditors, hospital-contracted provider groups, and physicians. Hospitals allowed both remote and onsite access depending on the relationships and reasons for access. All but one of the hospitals we visited allowed hospital physicians remote access to the EHR system, although the access privileges varied. Some of these hospitals limited access to certain patients or to view-only screens.

[22] Tokens may include a series of randomly generated numbers, biometrics include fingerprint or retinal scans, and public key infrastructure is a high-level encryption standard.

Nearly all hospitals that allowed outside entities to access their EHR data tracked access via a unique identifier (99 percent), and nearly as many limited outside entity access (95 percent). In addition, 96 percent did not allow outside entities access to the audit logs. Five of the hospitals we visited allowed outside entities access although they limited access to specific patients, claims, or information and allowed view-only access. RTI recommends that certain outside entities have limited access to EHR data to allow for a greater ability to detect fraud.

Nearly all hospitals were using RTI-recommended data transfer safeguards

Eighty-eight percent of hospitals reported having limits on which EHR users can export, transfer, or print EHR data. However, only 27 percent of hospitals reported that they require users to provide a reason before exporting, transferring, or printing EHR data. RTI recommends safeguards to restrict the export, transfer, or printing of EHR data so that patient information is not readily available to create fraudulent claims.

Almost half of hospitals had begun implementing RTI-recommended tools to include patient involvement in anti-fraud efforts

Forty-three percent of hospitals reported that they allow patients to view either components of their EHRs or their entire EHRs electronically. Hospitals and EHR vendors we spoke with revealed that hospitals were beginning to implement patient access features to achieve Meaningful Use Stage 2. Few hospitals had implemented additional features to allow patients a stronger role in detecting fraud. For example, 9 percent of hospitals allowed patients to comment in their EHRs, to view the entities to which the hospitals released their EHRs, or to view entities that accessed their EHRs. RTI recommends that patients have access to their EHRs and the ability to comment in their EHRs. This could enable patients to detect fraud by identifying errors and validating the services that they received.

Hospitals reported several barriers to allowing patients' access to their EHRs, including the inability of EHR technology to support the capability, the inability to integrate with existing systems, funding restrictions, resistance from physicians, and concerns with patient privacy. EHR vendors echoed some of these barriers. According to one EHR vendor we spoke with, physicians are especially hesitant to allow patients to communicate to providers and comment in the EHRs. Another EHR vendor told us that its small rural hospitals lack the patient demand for such a feature. Finally, one EHR vendor explained that providing patient

access tends to be one of the last features a hospital implements after focusing on initiating other EHR functions.

Only about one quarter of hospitals had policies regarding the use of the copy-paste feature in EHR technology

Although the copy-paste feature in EHRs can enhance efficiency of data entry, it may also facilitate attempts to inflate, duplicate, or create fraudulent health care claims. RTI acknowledges the potential for misuse of the copy-paste feature in EHRs and suggests that specific warnings directed to EHR users be considered. Further, RTI recommends that the use of such tools be captured in the audit log. However, only 24 percent of hospitals had policies in place regarding use of copy-paste, and only 44 percent of hospital audit logs recorded the method of data entry (e.g., copy-paste, direct text entry, speech recognition) when data are entered into the EHR.

Even the hospitals that had policies seemed to have limited control over the use of the copy-paste feature. Most of these hospital policies (61 percent) shifted the responsibility to the EHR user to confirm that any copied-pasted data were accurate. Twenty-two percent of hospitals' policies advised EHR users to avoid "indiscriminately copy-pasting," and 21 percent of policies required EHR users to cite the original source of the copied-pasted data. In addition, 51 percent of hospitals reported that they are unable to customize the copy-paste feature in their EHR technology, for example, by restricting its use or disabling it. Furthermore, the EHR vendors we spoke with explained that the copy-paste feature cannot be disabled or altered. One EHR vendor offered that it discourages hospitals from copy-pasting progress notes or copy-pasting identical text in records of multiple patients.

Copy-paste is most useful with facilitating data entry of physicians' progress notes; however, few hospitals had fully implemented that function. Only 4 percent of hospitals reported they had fully implemented electronic progress notes. Most hospitals (73 percent) reported having a combination of electronic and handwritten or dictated physician progress notes. Although this feature may enhance efficiency, it is vulnerable to fraudulent use.

CONCLUSION AND RECOMMENDATIONS

In the Department of Health and Human Services' efforts to promote EHR adoption, it focused largely on developing criteria, defining meaningful use, and administering incentive payments. It gave less attention to the risks EHRs may pose to program integrity of Federal health care programs. Although ONC contracted with RTI to develop a list of recommended safeguards for EHR technology, the Department did not directly address all of these safeguards through certification criteria or meaningful use requirements. This review found that, on their own initiative, hospitals were employing EHR fraud and abuse safeguards to varying degrees. However, the Department must do more to ensure that all hospitals' EHRs contain safeguards and that hospitals use them to protect against electronically enabled health care fraud.

We recommend that:

Audit logs be operational whenever EHR technology is available for updates or viewing

Stage 2 EHR Technology Certification Criteria state that the audit log must be set by default at the point of installation to record the data specified in the standard. However, providers may disable the audit log at any point. The Department should ensure that providers cannot or do not disable audit logs whenever EHR technology is available for updates or viewing. Requiring that audit logs be operational in this manner reinforces their importance and conveys the Department's expectation that they will be used to detect fraud and abuse. To that end, we offer two options:

- ONC could propose a change to its EHR certification criteria, through rulemaking, to require that EHR technology keep the audit log operational whenever the EHR technology is available for updates or viewing.
- Alternatively, CMS could update its meaningful use criteria to require providers to keep the audit log operational whenever EHR technology is available for updates or viewing.

ONC and CMS strengthen their collaborative efforts to develop a comprehensive plan to address fraud vulnerabilities in EHRs

The Department has a responsibility to address the risks that EHRs pose to program integrity for Federal health programs. Toward that end, in May 2013, ONC and CMS jointly convened stakeholders to discuss appropriate coding in an electronic environment. This is a promising start, and they should build on it to develop a formal strategy aimed at detecting and reducing fraud in EHRs.

In July 2013, ONC released the *Health IT Safety Action and Surveillance Plan*, which integrated the efforts of ONC, CMS, and the Agency for Healthcare Research and Quality to make patient care safer through the use of health IT.[23] ONC and CMS could use this approach to develop a strategy to detect and reduce fraud in EHRs. It may also offer the Department the opportunity to establish clear responsibility for program integrity among the agencies that run its health IT programs.

CMS develop guidance on the use of the copy-paste feature in EHR technology

Because many hospitals cannot customize the copy-paste feature in EHR technology, the need for policies to govern its use is elevated. The copy-paste feature can be used appropriately and enhance efficiency; however, this feature also poses risks. CMS should work with ONC and hospitals to develop guidelines for using the copy-paste feature in EHR technology. Specifically, CMS should consider whether the risks of some copy-paste practices outweigh their benefits. For example, CMS could provide guidance to hospitals on copy-pasting identical text in records of multiple patients.

[23] ONC, *Health Information Technology Patient Safety Action & Surveillance Plan for Public Comment*, December 21, 2012. Accessed at www.healthit.gov on May 2, 2013.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS and ONC concurred with all three of our recommendations.

To address our recommendation that the audit log be operational at all times, ONC will propose the appropriate revision to the auditable events certification criteria in the next available and relevant rulemaking cycle. CMS responded that it supports ONC's development of certification criteria toward this goal.

To address our recommendation about developing a comprehensive plan to address fraud vulnerabilities in EHRs, ONC stated that it was committed to providing technical assistance to other Federal agencies with health care fraud enforcement authority. CMS commented that it audits hospitals to ensure the integrity of the EHR incentive payments. However, our recommendation concerned plans to address fraud vulnerabilities directly related to Medicare health claims. We ask CMS to address these vulnerabilities in its final management decision

To address our final recommendation that CMS develop guidance on the use of the copy-paste feature, CMS stated that it will develop guidelines to ensure that this feature is used to appropriately.

For a full text of CMS and ONC's comments, see Appendix C.

APPENDIX A

RTI Recommendations and General Consistency With ONC Certification Criteria or CMS Meaningful Use

RTI Recommendation	Description	General Consistency With ONC Certification Criteria or CMS Meaningful Use Objectives
Audit Functions		
1) Audit Functions and Features	Requires the use of an audit log function and specifies audit log operation and content for tracking EHR updates.	Certified EHR Technology is required to have an audit log that can be disabled only by authorized users, cannot be altered or deleted, and must be enabled by default but is not required to be operational at all times. 45 CFR § 170.314(d)(2)
2) Documentation Process Issues	Requires that the methods (i.e., copy/paste, direct entry, import) for any update to an EHR be documented and tracked.	ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement.**
3) Proxy Authorship	Requires that the user ID of the original author be tracked when an EHR update is entered "on behalf" of another author. (i.e., distinguish between entries made by an assistant and a provider.)	ONC notes that Certified EHR Technology is required to be capable of assigning the type of access and the actions the user can perform based on unique identifier(s). 45 CFR § 170.314 (d)(1) However, ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement.**
4) Record Modification After Signature	Requires that original EHR documents be retained after they are signed off and modifications be tracked as amendments.	Certified EHR Technology is required to have an audit log that tracks when a user makes any changes to a record (with pointer to original state). In addition, for patient-supplied information, EHR Technology must allow users to select the record and append the amendment. 45 CFR § 170.210(h); 45 CFR § 170.314(d)(4)
5) Patient Identity-Proofing	Requires that EHR technology be able to record and indicate the method used to confirm patient identity (i.e., photo identification, prior relationship).	ONC notes that Certified EHR Technology is required, through an electronic exchange, to properly match a transition of care/referral summary to the correct patient when a patient is transferred or referred to another care setting. 45 CFR 170.314(b)(1)(iii)(A) However, ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement.**
User Authorization and Access Controls		
6) Provider Identification	Requires the use of a provider's NPI to restrict EHR access and track updates to EHRs by author.	Certified EHR Technology is required to verify against unique identifier(s) that a person seeking access is the one claimed. The type of access and the actions the user can perform must be based on unique identifier(s). EHR technology must also record actions of user. 45 CFR § 170.314 (d)(1); 45 CFR § 170.314 (d)(2)
7) User Access Authorization	Requires the use of user IDs and passwords to restrict unauthorized access to EHRs.	Certified EHR Technology is required to verify against unique identifier(s) that a person seeking access is the one claimed. The type of access and the actions the user can perform must be based on unique identifier(s). 45 CFR § 170.314 (d)(1)

8) Auditor Access to Patient Record	Requires that EHR technology support an "auditor" class of user to have read-only access to patient records.	ONC notes that Certified EHR Technology is required to be capable of assigning the type of access and the actions the user can perform based on unique identifier(s). 45 CFR § 170.314 (d)(1) However, ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement**.
Data Transfer Standards		
9) EHR Traceability	Requires that a document ID tracking number be generated and attached to an EHR any time an EHR is exported (i.e., printed or electronically communicated).	ONC notes that Certified EHR Technology is required to have an audit log that tracks when health information is printed, copied, or queried. EHR technology is also required, through an electronic exchange, to properly match the transition of care/referral summary to the correct patient when a patient is transferred or referred to another care setting. 45 CFR 170.314(b)(1)(iii)(A). However, ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement**.
10) Structured and Coded Data	Requires that EHR technology have the capacity to directly capture clinical information in structured and coded data and not impact EHR user productivity.	ONC certification criteria generally require structured and coded data for certain information, including among other data, problem lists, demographics, smoking status, and laboratory test results, and CMS meaningful use objectives require that data be recorded in structured form in order to meet certain objectives.
11) Integrity of EHR Transmission	Requires that EHRs be exchanged using certain data standards (encryption) to ensure data have not been altered during the transmission.	Certified EHR Technology must create a message digest and verify upon receipt of electronically exchanged health information that such information has not been altered as specified in 45 CFR §170.210(c). 45 CFR §170.314(d)(8); 45 CFR §170.314(d)(7); 45 CFR §170.314(d)(2)(ii)(c)
Patient Involvement in Anti-Fraud		
12) Patient Involvement in Anti-Fraud	Requires that patients be able to access and comment within their EHRs.	Certified EHR Technology is required to provide patients with an online means to view, download, and transmit specified data to a third party. In an ambulatory setting, EHR technology must enable a user to electronically send and receive messages from a patient. In addition, for patient-supplied information, EHR technology must allow users to select the record and append the amendment. 45 CFR §170.314(e)(1); 45 CFR § 170.314(e)(3); 45 CFR § 170.314 (d)(4) Meaningful use requires that more than 50 percent of patients be allowed online access to their health information within 36 hours of discharge from the hospital. 42 CFR §§ 495.6(12)(ii)(B)
Other		
13) Accurate Linkage of Claims to Clinical Records	Requires that information transmitted for payment of claims be accurately linked and tracked to the appropriate EHR.	ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement**.
14) Evaluation and Management Coding	Requires that EHR technology not prompt an EHR user to add documentation but be able to alert a user to inconsistencies between documentation and coding.	ONC certification criteria and CMS meaningful use objectives **do not specifically address this requirement**.

APPENDIX B

Nonrespondent Analysis

A consideration in surveys or data collection efforts of this type is whether the results may be biased by significant differences between respondents and nonrespondents. To determine whether significant differences exist in this data collection effort, we compared respondents and nonrespondents by whether or not the hospital was a critical access hospital, the State the hospital is located in, and the ownership type of the hospital (i.e., profit, nonprofit, religious organization, physician owned).

We achieved a 95-percent response rate with respect to the hospitals sampled. As a result, we had 832 responses and 45 nonresponses to use for this analysis.

Our analysis suggests that our survey results were not biased with regard to those variables. A chi-square test showed no relationship between respondents and nonrespondents with respect to whether the hospital was a critical access hospital. In addition, there were no patterns in frequency counts between respondents and nonrespondents for the State the hospital was located in or the ownership type of the hospital.

APPENDIX C

Agency Comments

CMS Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Servic

NOV - 1 2013

Administrator
Washington, DC 20201

TO: Daniel R. Levinson
Inspector General

FROM: Marilyn Tavenner
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology," OEI-01-11-00570

Thank you for the opportunity to review and comment on the above referenced OIG draft report. The Centers for Medicare & Medicaid Services (CMS) appreciates the contributions by, and valuable input from, the OIG. The draft report assessed how hospitals that received Medicare electronic health record (EHR) incentive payments had implemented recommended fraud safeguards for EHR technology. The information in the report will help inform our administration and oversight of the EHR Incentive Programs.

CMS is committed to reducing fraud, waste, and abuse in the EHR Incentive Programs while ensuring that EHRs continue to improve the efficiency and effectiveness of patient care. CMS is conducting prepayment and postpayment audits to determine whether providers are properly receiving meaningful use incentive payments and complying with program rules. Audits of the EHR Incentive Program strengthen our program integrity oversight and help reduce improper payments. If an audit identifies potentially fraudulent activity, these are referred to our Center for Program Integrity for further investigation.

The draft report contained three recommendations for CMS and the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC). We address the CMS response to the recommendations below:

OIG Recommendation 1:

Audit logs be operational whenever EHR technology is available for updates or viewing. ONC could propose a change to its EHR certification criteria, through rulemaking, to require that EHR technology keeps the audit log operational whenever the EHR technology is available for updates or viewing.

Alternatively, CMS could update its meaningful use criteria to require providers to keep the audit log operational whenever EHR technology is available for updates or viewing.

CMS Response

CMS concurs with the finding that audit logs should be operational whenever EHR technology is available for updates or viewing. CMS will support ONC in its development of certification criteria towards this goal.

OIG Recommendation 2:

ONC and CMS strengthen their collaborative efforts to develop a comprehensive plan to address fraud vulnerabilities in EHRs. ONC and CMS have a shared responsibility in addressing the risks that EHRs pose to program integrity for Federal health programs. Toward that end, in May 2013, ONC and CMS jointly convened stakeholders to discuss appropriate coding in an electronic environment. This is a promising start, and they should build on it to develop a formal strategy aimed at detecting and reducing fraud in EHRs.

In late 2012, ONC released the *Health IT Safety Action and Surveillance Plan*, which integrated the efforts of ONC, CMS, and the Agency for Healthcare Research and Quality to make patient care safer through the use of health IT. ONC and CMS could use this approach to develop a strategy to detect and reduce fraud in EHRs.

CMS Response

CMS concurs with this recommendation. CMS is planning to work with ONC to develop a comprehensive plan to detect and reduce fraud in EHRs.

CMS is conducting audits as a method to reduce fraud, waste, and abuse in the EHR Incentive Programs. In addition to the pre-payment edit checks that have been built into the EHR Incentive Programs' systems to detect inaccuracies in eligibility, and reporting, CMS began pre-payment audits in 2013, starting with attestations submitted during and after January 2013. Some of these pre-payment audits will be random and some will target suspicious or anomalous data. Providers selected for pre-payment audits will have to present supporting documentation to validate submitted attestation data before CMS will release payment.

CMS will also continue to conduct post-payment audits during the course of the EHR Incentive Programs. Providers selected for post-payment audits will also be required to submit supporting documentation to validate their submitted attestation data.

OIG Recommendation 3:

CMS develop guidance on the use of the copy-paste feature in EHR technology. Because many hospitals cannot customize the copy-paste feature in EHR technology, the need for policies to govern its use is elevated. The copy-paste feature can be used appropriately and enhance efficiency; however, this feature also poses risks. CMS should work with ONC and hospitals to develop guidelines for using the copy-paste feature in EHR technology. Specifically, CMS should consider whether the risks of some copy-paste practices outweigh their benefits. For example, CMS could provide guidance to hospitals on the use of copy-paste between EHRs for different patients.

CMS Response

CMS concurs that inappropriate use of the copy-paste feature in EHR technology could increase the risk of fraud, waste, and abuse. CMS will develop appropriate copy-paste guidelines to ensure that this feature is used appropriately for enhancing clinical efficiency.

The CMS appreciates the opportunity and comment on this OIG report.

ONC Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

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

TO: Daniel R. Levinson
Inspector General

FROM: Jacob Reider
Acting National Coordinator

SUBJECT: The Office of the National Coordinator for Health Information Technology's Comments to the Office of Inspector General's Draft Report Entitled, *Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology*, OEI-01-11-00570.

Thank you for the opportunity to review and comment on the findings and recommendations in the Office of Inspector General's (OIG) draft report, *Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology*, OEI-01-11-00570. The draft report addresses potential risks certified electronic health records technology may pose. ONC appreciates the OIG's efforts to improve program integrity and address fraud vulnerabilities.

The subject evaluation relies heavily on a report, commissioned by ONC and delivered by RTI in 2007, that identifies recommendations to address potential EHR vulnerabilities. While thoughtful input at the time, we note that some of this report's recommendations generated much debate in the stakeholder community and were not widely accepted or needed more evaluation as to their feasibility.

This response letter addresses the two recommendations from the OIG report that were directed to ONC.

OIG Recommendation 1:

Audit logs be operational whenever EHR technology is available for updates or viewing

ONC Response

ONC concurs with the recommendation. However, we wish to make clear that we do not have statutory authority to regulate how health care providers use EHR technology once certified – such as prohibiting providers from modifying their EHR technology to enable certain functionality post-certification. Further, while testing could verify that an EHR technology's audit log is functioning properly and available, we are presently unsure of the feasibility and difficultly associated with "testing the negative" – that the audit log is never not operational –

which is essentially how one would verify OIG's recommendation.

In order to modify any certification criteria adopted in the Code of Federal Regulations (CFR), ONC is required to go through a notice and comment rulemaking processes. Accordingly, ONC will propose the best appropriate revision to the auditable events certification criterion for public comment in the next available and relevant rulemaking cycle.

OIG Recommendation 2:

ONC and CMS strengthen their collaborative efforts to develop a comprehensive plan to address fraud vulnerabilities in EHRs

ONC Response

ONC concurs with the recommendation. However, we note that ONC has no enforcement ability related to healthcare fraud laws. That said, we recognize that EHR technology can assist in detecting potential fraud, and are very committed to providing technical assistance to those Federal agencies having healthcare fraud enforcement authority (such as the HHS Office of Inspector General, CMS, and the Department of Justice).

Technical Comments

In APPENDIX A, RTI Recommendations and General Consistency with ONC Certification Criteria or CMS Meaningful Use, please note the following corrections:
11 – Integrity of EHR Transmission
Reference provided is
45 CFR 170.314(d)(2)(i)(C)
Reference should be replaced with
45 CFR 170.314(d)(2)(ii)(C)

12 – Patient Involvement in Anti-Fraud
In order to align with text, reference order should switch from
45 CFR 170.314(d)(4); 45 CFR 170.314(e)(3)
To
45 CFR 170.314(e)(3); 45 CFR 170.314(d)(4)

CC: Marilyn Tavenner, CMS
Stuart Wright, OIG
David Tawes, OIG

ACKNOWLEDGMENTS

This report was prepared under the direction of Joyce Greenleaf, Regional Inspector General for Evaluation and Inspections in the Boston regional office; Kenneth Price, Deputy Regional Inspector General; and Russell Hereford, Deputy Regional Inspector General.

Danielle Fletcher served as the team leader for this study. Other Office of Evaluation and Inspections staff from the Boston regional office who conducted the study include Kimberly Yates. Central office staff who provided support include Kevin Manley, Clarence Arnold, and Christine Moritz.