Electronic Health Records

Program Integrity Issues in Electronic Health Records: An Overview

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Content Summary

As of June 2014, the Centers for Medicare & Medicaid Services' Electronic Health Record (EHR) Incentive Programs had paid incentives to 75 percent of eligible professionals and 92 percent of eligible hospitals.[1] As of September 2015, 548,000 eligible professionals, hospitals, and critical access hospitals had registered to participate in EHR Incentive Programs.[2] While the advancement of EHRs has many recognized benefits such as improved quality patient care, there is also increased concern about the potential for fraud, waste, and abuse, and the loss of documentation integrity that could compromise patient care. This booklet addresses common EHR system features and methods, which, if used inappropriately, could compromise the integrity of Federal health care programs by facilitating fraud, waste, abuse, and improper payments. The booklet also covers some program integrity tools and techniques that can help providers and others to recognize, report, and prevent such activities.

Introduction

The increasing use of electronic health records (EHRs) necessitates developing and changing how to identify and address Federal health care program integrity vulnerabilities. Program integrity depends on consistent incentives for better patient outcomes within a context that avoids over- or underutilization of services. It also requires effective, ongoing program management and monitoring. The success of such efforts directly affects the appropriate spending of taxpayer dollars.[3]

A base EHR must meet certification criteria according to Federal regulations (45 Code of Federal Regulations [CFR] Section 170.315) and contain patient demographic and clinical medical history and problems. An EHR must also be able to:

- Provide clinical decision support;
- Support physician order entry;
- Capture and query information relevant to health care quality; and
- Exchange electronic health information with other sources and integrate health information from other sources.[4]

Do not confuse EHRs with electronic medical records (EMRs). A single medical practice or health care organization creates and accesses EMRs, while EHRs are for use by multiple entities.[5]

Benefits of EHR Use

There are many benefits associated with the use of EHRs, including:

- **Improved Coordination of Care:** Timely access to complete patient health care records helps providers make decisions that are more informed.[6] EHR systems can track health changes over time, allow providers at multiple locations to view the record at the same time,[7] and reduce misplaced or lost charts and records;[8]
- **Reduced Costs:** EHRs can lower health care costs by applying clinical practice guidelines to avoid duplicate procedures and unnecessary tests.[9] EHRs allow providers to respond to auditors' requests for medical records through secure electronic means such as the Electronic Submission of Medical Documentation (esMD) systems;[10, 11]
- **Enhanced Security and Patient Privacy:** EHRs can offer major improvements over paper documentation, providing such features as secure networks, firewalls, encryption of data, and password protection that ensure only appropriate or authorized entities can access certain information.[12, 13] Physical security at data storage (server) sites, locked and access-restricted facilities, server redundancy, and backup processes control risk of data loss from natural disasters or system failure.[14] Additionally, edits, audits, and system logs can track all persons editing and accessing information, flag potentially inappropriate activity, and correct mistakes in real time;[15] and
- **Prevention and Detection of Fraud, Waste, and Abuse:** Internal monitoring and auditing can help identify data that is outside the normal range,[16] when and by whom records were accessed, and new or amended entries.[17] EHRs also allow information sharing between EHR e-prescribing systems and State Prescription Drug Monitoring Programs (PDMPs). PDMPs can review

prescriptions for controlled substances, which can help prevent doctor shopping and reduce the volume of drugs available to abusers.[18]

Need for Education

As with any new or emerging technology, providers and others need education. They may need information on the importance of creating and adapting internal policies and processes to accommodate use of EHRs. Training should cover appropriate EHR use, security issues, and preventing, detecting, and reporting of fraud, waste, and abuse. Management and staff can benefit from learning about internal monitoring and auditing to identify, investigate, and correct any issues found. Realization of the program integrity benefits of EHRs will ultimately depend on the nature, depth, and scope of the education provided on EHR system design and use.

Statutes, Regulations, and Guidance

Number 3 in the top 10 management challenges for the U.S. Department of Health and Human Services in 2015 is "the meaningful and secure exchange anduse of electronic information and health information technology."

Statutes and Regulations

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorized the Secretary of the U.S. Department of Health and Human Services (HHS) to create a rule that protects the security and privacy of individually identifiable health information.[19] The Secretary did so, adopting standards known as the Privacy Rule.[20] Since EHRs contain such health information, providers maintainingthese records must comply with the privacy and security requirements of the Privacy Rule.

Later legislation focused on promoting EHR use. The Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act of 2009,[21] promoted using health information technology to improve health care quality, safety, and efficiency. The stated goals of the Act include the development of a nationwide health information technology infrastructure that:

- Allows for the electronic use and exchange of information;
- Ensures security of patient health information;
- Improves health care quality and reduces medical errors and health disparities;
- Reduces health care costs;
- Provides appropriate information to help guide medical decisions;
- Improves coordination of care among different providers;

- Promotes early detection, prevention, and management of chronic diseases; and
- Brings about widespread EHR adoption by 2014.[22]

To encourage standardization of EHR content, systems, and interoperability, the HITECH Act established the health information technology certification program and the Medicare and Medicaid EHR incentive programs.[23, 24] Eligible professionals and other providers participating in the Medicare[25] or Medicaid[26] program that want to receive the incentive payments must adopt certified EHR technology and must show increasing levels of meaningful use of the technology on a schedule established by the Centers for Medicare & Medicaid Services (CMS).[27]

Participation in the certification and incentive programs is voluntary. Failure to demonstrate meaningful use for an applicable reporting period will result in reduced Medicare reimbursements for eligible professionals, eligible hospitals, and critical access hospitals.[28] However, the Patient Access and Medicare Protection Act authorized more flexibility in applying for a hardship for the EHR incentive program for 2017 payment adjustments.[29] More information is posted to https://www.healthit.gov/providers-professionals/ehr-incentives-certification on the Office of the National Coordinator for Health Information Technology (ONC) website.

HHS's 2015 final rule for Health IT certification criteria and EHR definition became effective in January 2016. The purposes of the new comprehensive rule are to foster better interoperability of EHR systems and to support Stage 3 of CMS' EHR Incentive Program, among other purposes. The rule adds 45 CFR Section 170.315 2015 Edition Health IT Certification Criteria, which codifies many best practices expected from EHR systems discussed in a previous version of this EHR toolkit. Standards include features like immediately identifying drug-drug or drug-allergy interactions when the provider enters a new medicine into the patient's record, including the diagnostic reason for a prescription with the prescription order, and maintaining a record of when someone enables or disables the audit log along with a list of users who are able to do so.[30]

The new rule also expands and clarifies the "Common Clinical Data Set"—demographic and clinical information that should be included in all patients' EHRs for better interoperability. This includes such data as name, sex, date of birth, race, ethnicity, and preferred language; smoking status; health problems; medications and related issues; laboratory tests, values, and other vital signs; and information about past procedures, care plans, and goals.[31]

Additionally, laws exist to punish those who seek to compromise the integrity of EHRs or use EHR systems to perpetrate Federal health care fraud. These laws include the False Claims Act[32, 33, 34] the Health Care Fraud Statute,[35] the criminal provisions of HIPAA,[36] the Civil Monetary Penalties Law,[37] and the exclusion provisions of the Social Security Act.[38] Under these and other Federal and State

laws, persons and entities that use EHRs to commit fraud against Federal health care programs are subject to civil monetary penalties, exclusion from participation in Federal health care programs, and criminal fines. Individuals who commit such fraud are also subject to imprisonment. The Affordable Care Act has added to the effectiveness of these laws by:

- Increasing criminal penalties for health care offenses involving losses of $1 million or more;
- Clarifying that specific intent to violate the law is not required for conviction under the Health Care Fraud Statute; and
- Mandating suspension of provider payments when there is a reasonable suspicion that they have engaged in fraud.[39]

Guidance From HHS-OIG

The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG), has issued several reports dealing with EHRs. One of these reports explains that each EHR system's audit log automatically records changes in EHRs, "capturing data elements, such as date, time, and user stamps, for each update to an EHR." HHS-OIG recommends keeping the audit log turned on so that it can capture data regarding all such changes. HHS-OIG also recommends that outside auditors should use the logs to support investigations of potential fraud.[40] The 2015 final rule addresses these recommendations by adding subparagraphs (e)(1)(i) and (h) to 45 CFR Section 170.210 and incorporating the American Society for Testing and Materials' standard for health information system audit logs.[41, 42] The sections on monitoring, auditing, and investigating later in this document discuss using the audit log to monitor and investigate fraud, waste, and abuse related to EHRs.

Program Integrity Vulnerabilities

Summary of a Case Study

EHR technology can make it easier to commit fraud by making it possible to obtain access to, sort, retrieve, and export a large amount of data quickly. A case involving an emergency room (ER) employee recruited by a chiropractic clinic manager to steal information from EHRs illustrates the harm possible when someone uses an EHR system for fraudulent purposes. For over 3 years, the ER employee viewed hundreds of thousands of patient records. He identified 12,000 patients involved in traffic accidents, used the EHRs to assemble related contact and injury information on these patients, and then sold the information to the clinic

manager. The manager then had clinic employees contact the patients and solicit them for chiropractic and legal services.

The ER discovered the fraudulent activities of the employee when one of the hospital's nurses called to complain about a solicitation call she received on behalf of her daughter, who was involved in a motor vehicle accident. After an investigation, the ER employee and the clinic operator faced criminal charges. The ER employee and the clinic manager pleaded guilty to conspiracy and wrongful disclosure of individually identifiable health information.[43, 44] More information about this case is available in "Detecting and Investigating Unauthorized Access to Electronic Health Records—A Case Study," which is part of the EHR Toolkit posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

Transition to EHRs From Paper Records or EMR

Vulnerabilities during the transition to EHRs include transferring existing data errors, which, in turn, cause false claims; inadequate record transition security, storage, and disposal; and inflation of the number of records transitioned to EHRs to meet meaningful use criteria.[45] Providers should also be aware that authentication and authorization systems can weaken during transition.[46]

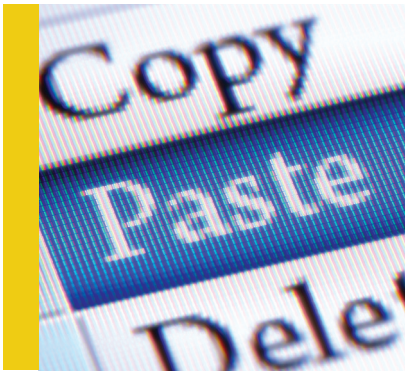
Transition from paper-based records or EMR to EHR can cause problems. Data errors may occur during manual transfer, or scanning may result in incomplete capture. Electronic transfer of EMR to EHR requires software to match data fields in the EMR to data fields in the EHR. Mismatched fields lower the quality of the EHR and can lead to submitting false claims. Storage and disposal of records transitioned to EHR can create security issues if someone does not secure paper records while awaiting disposal. Problems also arise if EMR record systems lose security features, such as password protections or access restrictions, which normally help control submission of claims for services not provided. Providers transitioning from paper-based records to EHR may be vulnerable to not having a complete picture of a patient's health history or the inability to share relevant patient records in real time, creating problems for coordinating care.[47]

Definitions

Understanding the program integrity risks associated with the daily use of EHRs starts with defining some common EHR features.

- **Copy and Paste:** Selecting data from one location and reproducing it in another, also called "cloning,"[48] "cookie cutter,"[49] "copy forward," and "cut and paste."[50] Clinical plagiarism occurs when a physician copies and pastes information from another provider and calls it his or her own;[51, 52, 53]

- **Automated Change of Note Author:** Automatically changing authorship of a note written by someone else to the current user of the note;
- **Templates:** Using predefined text and text options to document the patient visit within a note;
- **Macros:** Expanding text associated with abbreviations or specific keystrokes;
- **Populating via Default:** Generating content without positive action or selection by author;[54]
- **Audit Log:** Tracking EHR access information, including the username, workstation, event description (for example, amendment, correction, or deletion), and date and time;[55]
- **Upcoding:** Using documentation to upgrade the level of care provided; and
- **Fabrication:** Copying information or creating text to show that treatment occurred at a higher level than was delivered.



Improper Use of EHR Features and Capabilities

Promoting EHRs as a way to improve communication between providers, advance patient care, and improve patient safety is valid when used properly. However, when used improperly, EHR software can work against these goals and make it easier to commit fraud, waste, and abuse. For example, copying and pasting an extensive patient history completed by another physician into current notes can create a false impression of which provider completed the history and make it easier to commit fraud by providing a way to alter information to inflate claims. This section describes some examples of improper use of EHR features and capabilities.

Copy and Paste

Health care professionals have stated that copying and pasting notes can be appropriate and eliminate the need to create every part of a note and re-interview patients about their medical histories.[56] However, HHS-OIG identifies "illegitimate use of cut-and-paste record cloning" as a problem.[57] HHS-OIG's 2016 Compendium of Unimplemented Recommendations found that only about one-fourth of hospitals had policies governing the use of the copy-paste function in EHR software.[58] Defaulting or copying and pasting clinical information from different health care records of the same patient facilitates billing at a higher level of service than was actually provided.[59] For example, in a summary of one company's recent self-disclosure settlement, HHS-OIG said the EHR contained cloned patient progress notes and that they upcoded several services.[60]

Author Identification

"Abuse" describes incidents or practices that may not be fraudulent but are inconsistent with accepted medical or business practices or may result in unnecessary costs.[61] Some such incidents directly relate to EHR software features, such as allowing multiple providers to add text to the same progress note without allowing each provider to sign, making it impossible to verify the actual service provider or the amount of work performed by each provider.[62, 63]

Templates, Macros, and Population via Default

Some EHR systems use templates that complete forms by checking a box,[64] macros that fill in information by typing a key word,[65] or functions that auto-populate un-entered text. Problems can occur if the structure of the note is not a good clinical fit and does not accurately reflect the patient's condition and services. These features may encourage overdocumentation to meet reimbursement requirements even when services are not medically necessary or never delivered.[66]

Altering Dates When Entries Are Made or Amended

To protect the integrity of the EHR, the new 2015 EHR final rule requires EHR system audit logs to conform to American Society for Testing and Materials (ASTM) E2147-01(2013) specification for audit and disclosure logs. This ensures that the EHR system has the capability to identify the date and time of changes made to an original entry, such as amendments and corrections; the author of the change; and the reason.[67, 68] Some systems automatically assign the date to an entry. Others allow authorized users to change the entry date to the date of the visit or service. Some systems allow providers to make undated amendments without noting the change of an original entry. If there is no date and time on the original entry or subsequent amendments, documentation to support services provided may be in question. Additionally, if providers cannot determine the order of events, it can affect the quality of patient care.[69]

Upcoding

Some providers use deception to obtain improper payments. The Center for Public Integrity report "Cracking the Codes" says providers have added $11 billion to their Medicare fees over the past 10 years by using more highly compensated codes more often.[70] Some EHR systems prompt physicians on what additional documentation is necessary to justify using a higher billing code, even when existing documentation is sufficient to justify the code entered.[71] In 2012, a joint letter from the U.S. Department of Justice and HHS to several national hospital associations expressed concern that some providers might be using EHR systems to upcode the documented intensity of care provided as a method of improperly increasing profit. Both departments indicated their willingness to use the available tools to detect upcoding and prosecute

offenders.[72] As an example, the owner of a Missouri home health care company was sentenced to prison for directing employees to make false statements in medical records about the number of therapy visits, the diagnosis codes, and the patients' health conditions.[73] The company made these changes to increase payments from Medicare. Changing information about health conditions can harm the patients' health by misleading other providers.

In 2014, the United States Attorney for the Southern District of New York alleged that a billing company and New York City used an EHR system to manipulate coding. In a False Claims Act lawsuit, the government alleged several specific fraud schemes. One of those was using computer programs to identify diagnosis codes that Medicaid was likely to reject in EHRs. The program replaced those codes with a generic diagnosis code that Medicaid would accept. This practice allegedly resulted in millions of dollars in improper payments.[74]

Fabrication

EHRs can also make it easier to fabricate documentation and hide the fraud.[75] Users can copy, paste, and edit large amounts of text with much less effort than fabricating it by hand.[76] The 2012 joint letter mentioned previously conveyed concern that some providers might be using EHR systems to clone medical records.[77] Recent prosecutions support these concerns. For example, in 2013 a pediatric dentist in Texas[78] and a supervisor of a mental health services provider in Florida[79] were found guilty of fabricating records to support bills for nonexistent services.

In a different type of fabrication scheme, the Chief Financial Officer (CFO) of a Texas hospital chain ordered hospital employees and its software vendor to convert paper records to EHRs long after the hospital had discharged patients, and in some cases, after the end of the fiscal year. Then the hospital chain fraudulently claimed that they met the meaningful use requirements for the EHR Incentive Program. As a result, the hospitals received over $16 million under the Medicaid and Medicare EHR Incentive Programs. The CFO was ordered to repay nearly $4.5 million to the Medicare EHR Incentive Program and was sentenced to 23 months in prison.[80, 81]

Unauthorized Disclosure

Health information technology allows a malicious user to obtain and transfer patient information much faster than with paper records. For example, in the case of the hospital ER employee discussed previously in this booklet, the employee viewed more than 763,000 patient records in almost 3 years.[82] Other mistakes that can lead to waste, abuse, and identity theft include failure to encrypt laptops[83] and thumb drives,[84] with a resulting disclosure of personal health information (PHI).

Preventing EHR Fraud, Waste, and Abuse

In July 2014, CMS announced its plan to work with the ONC to develop a comprehensive strategy to detect and reduce EHR fraud.[85] Providers can play a large role in preventing fraud, waste, and abuse related to EHRs, and improper access to EHRs, by maintaining an operational audit log, encrypting all entries, adopting policies to regulate changes and access to EHRs, and training staff on these policies.

Anti-Fraud Software

Providers should consider purchasing EHR system software that incorporates important anti-fraud features or upgrades or modifies their existing systems to incorporate those features. Most important among such features is an audit log that remains operational whenever the records are available for updating or viewing.[86] There is no requirement in the 2015 Edition Health IT Certification Criteria for ensuring audit logs are operational around the clock, but there are several security requirements in 45 CFR Section 170.315(d)(2) to protect the integrity of the health information:

- The log must record actions specified in the ASTM E2147-01 specification (i)(A);
- The log must record its status and the encryption status as enabled or disabled (i)(B)–(C);
- The log may be disabled only by a limited group of users (iii); and
- The log must not be capable of being changed, deleted, or overwritten (iv).[87]

Therefore, providers should review the 2015 Final Rule in detail and consider purchasing or upgrading to an EHR system with the capabilities outlined in the rule.

Software to Prevent Unauthorized Access

Although illegitimate access to EHRs takes place more often from authorized system users than outside individuals, providers still need to take measures to protect data in transit and in storage from theft or alteration. A 2015 report from Microsoft Research showed that they could access PHI from nearly all of the small and large hospitals they attempted to hack.[88] Other anecdotal evidence indicates encryption still lags behind.[89]

"Ransomware" is a relatively new trend that hackers use to encrypt a health organization's EHR and other computer systems, and then demand payment for the encryption key. Government and private databases that store patient information are

vulnerable to hackers. In 2016, hackers gained access to the EMRs and other systems of a California hospital, encrypted the records, and demanded a 40 bitcoin (about $17,000) ransom payment for the access key.[90] Some of the records were part of an EHR system. Ransomware attacks recently hit other hospitals in California, Indiana, and the District of Columbia.[91] The lesson for providers is properly encrypt EHR systems, have a foolproof firewall, and keep the system secure from unauthorized outside access.

Standards and Policies

Additionally, when adopting appropriate software, providers can mitigate EHR risks by implementing standards of conduct and proper use policies. Standards of conduct should convey the expectation that employees will act in an appropriate and lawful manner, and failure to do so could result in termination. Policies should clearly state who can access EHRs and when, which system features (for example, copy and paste, auto-populate) to use in which sections of a record, and who can disable audit logs. CMS requires that EHRs provided to Medicare program integrity contractors clearly identify any record change and "provide a reliable means to clearly identify the original content, the modified content, and the date and authorship of each record modification."[92]

The new 2015 Rule cited earlier leaves the decision to allow disabling the audit log up to the provider. Providers should establish policies describing the conditions that may require disabling the audit log, reasons for disabling it, and the start and end times the log was disabled. They should clearly communicate those policies to staff, along with consequences for abusing the privilege or sharing access codes with unauthorized persons. The provider may consider factors cited by ONC in 2014 when it considered whether to require that logs remain operational or in the discussion in the 2015 Final Rule. ONC noted that disabling logs might be necessary in cases of emergency or disaster, to permit correction of system performance issues, or to implement updates.[93, 94] Additional policy discussions to prevent EHR fraud are found in the "Compliance Checklist for Electronic Health Records," included in the EHR Toolkit posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

Training

Training can be an effective mechanism for risk mitigation. When staff members receive training on the expectations and requirements for EHR system access and use, as well as the consequences for improper use, it reduces the potential for risk. While vendor training covers software features and capabilities, all staff needs further training to cover the policies and procedures on appropriate use of safety and security features and those that protect EHR documentation integrity. This training should provide guidance on how to use such features as copy and paste and templates in ways that do

not compromise the accuracy of the records. The training should inform employees of other ways ignoring EHR policies can harm patients. Employees should learn that improper use could lead to disciplinary action or criminal charges. Providers should train employees within 90 days of hire and on an annual basis. This provides all staff with knowledge about policy and procedure changes and statutory, regulatory, and subregulatory requirements that guide the use of EHR features.

Monitoring and Auditing for Program Integrity

Identifying EHR Program Integrity Problems and Solutions

A January 2014 HHS-OIG report on fraud safeguards in hospital EHR systems recommended that CMS work with contractors to "identify best practices and develop guidance and tools for detecting fraud associated with EHRs."[95] This booklet and the other products in the EHR Toolkit assist in identifying some best practices and tools. This section discusses best possible practices for detecting EHR fraud through continually monitoring internal operations and periodic audits of specific functions and areas of concern. This section also describes suggested best practices and recommendations for investigating suspected fraud, waste, and abuse.

Monitoring EHRs to Detect Potential Fraud, Waste, and Abuse

"Monitoring aims to ensure that policies and procedures are in place and are being followed." It is an ongoing effort that should be part of everyday procedures.[96] Monitoring of EHRs should consist of regular reviews of EHR data that could indicate fraud, waste, or abuse such as:

- Interruption of the audit log function;[97]
- Suspicious frequency, change, or purpose of edits and audits;
- Frequent or unusual access or changes to data;[98] and
- Entry of duplicate text from the health record of one provider's patient to that of another provider (clinical plagiarism).[99, 100, 101]

An audit log can help detect record alterations "to prevent the discovery of damaging information."[102] As seen in the case study previously discussed in this booklet, turning off EHR system security features, such as the audit log, access restrictions, and warnings, is possible and can result in an inadequate and incomplete audit log. Monitoring the audit log can help identify compromised data integrity. Additional

items to monitor are included in the "Conducting Internal Monitoring and Auditing" job aid for providers, which is part of the EHR Toolkit posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

Currently available fraud detection software for EHRs can perform pattern matching, predictive modeling, and anomaly detection. Pattern matching can identify beneficiaries who were treated by the same provider at multiple locations or unusually high utilization of particular services at locations associated with particular providers. A study has shown that storing relevant data in a dedicated database and then using statistical and machine-learning methods to identify suspicious record access events can make automated monitoring of access to EHRs more robust[103] Regardless of used methods a designated person should review data on a specified schedule.[104] As with any routine inquiry, those who are responsible for compliance should review results regularly.

Auditing EHRs to Detect Fraud, Waste, and Abuse

Audits differ from monitoring in that audits occur periodically rather than on an ongoing basis, are more focused and comprehensive, and are based on specific predetermined standards. Audits seek to verify that the ongoing monitoring efforts "have had the desired outcome."[105] Auditing is a recurring activity to determine the level of assurance that providers are meeting specific standards,[106] primarily by examining records. Internal auditors are responsible for "examining and evaluating the adequacy and effectiveness of controls."[107]

Providers should arrange for internal and external audits[108] every year.[109] Entity personnel conduct internal audits. Persons who are independent of the ongoing monitoring should do these audits.[110]

Audits, whether internal or external, should address the risk areas previously identified, and determine whether:

- There is an adequate program to monitor identified risks;
- There are adequate and properly enforced limitations on access; and
- Data is adequately encrypted when in transit and in storage.[111]

An entity can self-initiate external audits or outside parties, such as program integrity contractors, may initiate them. The law creating the CMS Center for Program Integrity (CPI) stresses that CPI reviews provider activities to determine "whether fraud, waste, or abuse has occurred, [or] is likely to occur."[112] CPI accomplishes this objective in part by retaining program integrity contractors to review provider activities, audit claims, and identify overpayments.[113] If the EHR system is a focus of the audit, the

auditor may examine the risk areas previously listed, evaluate the internal consistency of the information in the records, and determine whether medical documentation supports the claims. Additionally, the auditor may interview relevant providers and staff members regarding EHR entries.

HHS-OIG has stressed the importance of the EHR audit log to "protect against electronically enabled health care fraud" in the hospital setting.[114] HHS-OIG found that using the audit log to protect against fraud in hospitals is uncommon. In a 2012–13 survey, HHS-OIG found that most hospitals reported analyzing audit log data to detect violations of patient privacy rather than fraud. HHS-OIG visited eight of the surveyed hospitals and found that none had analyzed audit log data to prevent or detect fraud. EHR vendors indicated that hospitals seldom seek training on the audit log features that are available for such work.[115] Providers should request such training and use the resulting knowledge when performing internal monitoring.

As pointed out by HHS-OIG, audit logs are important to the work of outside auditors or program integrity contractors. In a 2014 report, HHS-OIG noted that auditors use the logs to authenticate medical records supporting claims made to Federal health care programs.[116] HHS-OIG found that an effective audit of claims based on EHRs requires use of the audit log.[117] Providers and others should keep this finding in mind when performing internal audits or investigations.

Investigating EHR Fraud

Monitoring and auditing can identify potential EHR fraud, which then requires an investigation. An investigation of EHR fraud, like any other fraud investigation, seeks to determine whether fraud occurred, which specific laws or policies were violated and how, the amount of any monetary loss, and who was responsible.[118] However, making these determinations is easier in the context of EHR-related fraud if auditors consult employees who are knowledgeable about the EHR system and the audit log. These employees may shed light on how the fraud occurred and identify specific entries used to justify or cause duplicate, fraudulent, or inflated billings.[119] The system may help identify the persons responsible, as in the ER employee case discussed previously. Additional ways to use EHR systems for investigating EHR fraud are discussed in the "Detecting and Investigating Unauthorized Access to Electronic Health Records—A Case Study," which is part of the EHR Toolkit posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

In a large practice or a managed care plan, the person who discovers the violation may be different from the person who pursues the investigation. In a small practice, the person who does the investigation may be the same person who discovered the violation. In addition, the investigation may be less in depth than might be done by a larger organization.

With the exception of the steps taken to gather information specifically related to EHRs, the investigation should follow the same basic procedures as any other fraud investigation. The investigator or compliance contact should analyze the allegation of fraud in light of relevant law and policy, secure and analyze relevant records and documents, interview persons with knowledge,[120, 121] and write an investigative report setting forth the relevant information and, if possible, identifying the persons responsible for the fraud.[122]

Corrective Action

The incorporated requirement to promptly respond to and correct detected fraud, waste, and abuse is in the "Program Integrity Requirements," a Federal rule that applies to many plans, and in HHS-OIG recommendations to providers. Prompt responses and corrective actions can include employee discipline or termination; provider discipline, termination, or removal from a network; or referral to an administrative or law enforcement agency for imposition of administrative, civil, or criminal sanctions. Contact information for sending referrals to Medicaid and law enforcement agencies, listed by state, is posted to https://www.cms.gov/medicare-medicaid-coordination/fraud-prevention/fraudabuseforconsumers/report_fraud_and_suspected_fraud.html on the CMS website. Prompt corrective action may persuade prosecutors to take action against the officers or employees committing the misconduct rather than also bringing charges against the organization when charging the individuals.[123] Likewise, in determining the amount of civil monetary penalties to impose on an organization as a result of a violation, HHS-OIG considers it a mitigating circumstance if "corrective steps were taken promptly after the error was discovered."[124] HHS-OIG has proposed an amendment to the civil penalty rules to provide that corrective action will only be a mitigating factor if the organization has disclosed the violation through HHS-OIG's Self-Disclosure Protocol and "fully coorperate[s] with OIG's review and resolution."[125] Therefore providers and others that discover EHR-related fraud should incorporate self-disclosure in their corrective action plans.

In addition to incorporating self-disclosure, providers should make specific persons responsible for implementing corrective action plans for detected EHR fraud. Providers should set forth the steps to take, the time frame for their implementation, and how to monitor implementation.

In addition, providers should determine whether preventing the violation was possible by using different software measures or policies. The compliance officer, in consultation with the investigtor and appropriate information technology professional, should make the determination. In small provider offices, the compliance contact and investigator may be the same person, and the technology vendor or an outside service provider

may need to supply the technical information. If the violation was not discovered through the existing EHR monitoring and auditing processes, the provider should consider whether additional protections are necessary to detect the type of EHR fraud that occurred. To improve prevention or detection, the provider may want to consider changing or replacing EHR software, changing policies, or adopting new policies. As EHRs become even more widely adopted and user experience increases, providers will have to adapt to reap the benefits of EHRs while continuing to prevent and detect constantly evolving forms of EHR fraud.

Conclusion

Properly implemented and supported EHR systems can:

- Improve quality and coordination of care;
- Reduce costs;
- Better preserve information from natural or manmade disasters;
- Better protect patient privacy; and
- Reduce the incidence of fraud.

To obtain these benefits, providers must incorporate and use fraud prevention features in their EHR software and adopt appropriate policies that mitigate the risks of improper use.

Additional Resources

Information about health information technology, including the use of EHRs, is available at https://www.healthit.gov/ on the Health IT website.

Information about the Office of the National Coordinator for Health Information Technology is posted to http://www.hhs.gov/about/orgchart/onc.html on the HHS website.

The 2015 Final Rule for EHR certification is posted to https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf on the Government Publishing Office website.

Information about the EHR Incentive Programs and Certification Programs, including "meaningful use" criteria, is posted to https://www.healthit.gov/providers-professionals/ehr-incentives-certification on the Health IT website.

Additional EHR implementation resources are posted to https://www.healthit.gov/providers-professionals/implementation-resources on the Health IT website and https://www.cms.gov/eHealth on the CMS eHealth website.

To see the electronic version of this booklet and the other products included in the "Electronic Health Records" Toolkit posted to the Medicaid Program Integrity Education page, visit https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the CMS website.

Follow us on Twitter #MedicaidIntegrity

References

1 U.S. Department of Health and Human Services. Office of the National Coordinator for Health Information Technology (ONC). (2014). Federal Health IT Strategic Plan 2015–2020 (p. 4). Retrieved March 22, 2016, from https://www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf

2 U.S. Department of Health and Human Services. Office of Inspector General. (2016, April). OIG'S FY 2015 Top Management and Performance Challenges Facing the Department of Health and Human Services (p. 9). Retrieved April 12, 2016, from http://oig.hhs.gov/reports-and-publications/top-challenges/2015/2015-tmc.pdf

3 National Association of Medicaid Directors. (2012, March). Rethinking Medicaid Program Integrity: Eliminating Duplication and Investing in Effective, High-Value Tools (p. 3). Retrieved March 22, 2016, from http://medicaiddirectors.org/wp-content/uploads/2015/08/namd_medicaid_pi_position_paper_final_120319.pdf

4 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.102 Definitions, pp. 62741–62742). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

5 Garrett, P., & Seidman, J. (2011, January 4). EMR vs EHR–What Is the Difference? Office of the National Coordinator. Health IT Buzz. Retrieved March 22, 2016, from https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/

6 HealthIT.gov. (2014). Benefits of EHRs. Improved Care Coordination. Retrieved March 22, 2016, from https://www.healthit.gov/providers-professionals/improved-care-coordination

7 Friedberg, M., Chen, P., Van Busum, K., Aunon, F., Pham, C., Caloyeras, J., Mattke, S., Tutty, M. (2013). Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy (p. 34). Retrieved March 22, 2016, from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR439/RAND_RR439.pdf

8 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (p. 17). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

9 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (p. 17). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

10 Centers for Medicare & Medicaid Services. (2015, December 4). Medicare Program Integrity Manual. Chapter 3: Verifying Potential Errors and Taking Corrective Actions (Revision 628; pp. 20–21). Section 3.2.3.5. Retrieved March 22, 2016, from https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c03.pdf

11 U.S. Department of Health and Human Services. Office of the Secretary. (2013, February 5). Report: Recovery Auditing in the Medicare and Medicaid Program. Fiscal Year 2011 (p. 16). Retrieved March 22, 2016, from http://www.kslaw.com/library/publication/HH021113_RAC.pdf

12 MedicalRecords.com. EMR Privacy and Security. Retrieved March 22, 2016, from http://www.medicalrecords.com/emr-privacy-and-security

13 U.S. Department of Health and Human Services. The Office of the National Coordinator for Health Information Technology. (2007, June). Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems (p. 4-9) Retrieved March 22, 2016, from http://www.rti.org/pubs/enhancing_data_quality_in_ehrs.pdf

14 U.S. Department of Health and Human Services. The Office of the National Coordinator for Health Information Technology. (2007, June). Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems (p. 4-3). Retrieved March 22, 2016, from http://www.rti.org/pubs/enhancing_data_quality_in_ehrs.pdf

15 Lynn, J. (2010, January 22). EMR Benefit You Wouldn't Expect. EMR & HIPPA. Retrieved March 22, 2016, from http://www.emrandhipaa.com/tag/emr-audit-logs/

16 Agency for Healthcare Research and Quality. (2014, April). A Robust Health Data Infrastructure (Section 6.5). [AHRQ Publication No. 14-0041 EF]. Retrieved March 22, 2016, from https://www.healthit.gov/sites/default/files/ptp13-700hhs_white.pdf

17 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (pp. 17–18). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

18 Stack, S. J. (2012, August 13). Prescription Abuse Laws Can Create a No-Win Situation for Doctors. American Medical News. American Medical Association. Retrieved March 22, 2016, from http://www.ama-assn.org/amednews/2012/08/13/edca0813.htm?utm_source=nwltr&utm_medium=heds-htm&utm_campaign=20120813

19 Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191, §§ 262, 264, 110 Stat. 196. Retrieved March 22, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

20 45 C.F.R. §§ 160, 164. Retrieved March 22, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=18481baf40df2326606fc3db9b9407fe&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl

21 American Recovery and Reinvestment Act of 2009. (2009). Pub. L. 111-5, Div. A, Tit. XIII, and Div. B, Tit. IV, 123 Stat. 115 (pp. 226, 467). Retrieved March 29, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

22 American Recovery and Reinvestment Act of 2009. (2009). Pub. L. 111-5, Div. A, Tit. XII, and Div. B, Tit. IV, 123 Stat. 115 (pp. 230–32, 246–47). Retrieved March 29, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

23 American Recovery and Reinvestment Act of 2009. (2009). Pub. L. 111-5, Div. A, Tit. XII, and Div. B, Tit. IV, 123 Stat. 115 (pp. 246–57, 467–94). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

24 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.315 2015 Edition Health IT Certification Criteria, pp. 62747–62755). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

25 Limitations on Amounts of Incentive Payments, 42 C.F.R. § 495.102. Retrieved March 23, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=be3c237de2baebc9f93cc5ecfbed887c&ty=HTML&h=L&n=pt42.5.495&r=PART#se42.5.495_1102

26 Medicaid Provider Scope and Eligibility, 42 C.F.R. § 495.304. Retrieved March 23, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=be3c237de2baebc9f93cc5ecfbed887c&ty=HTML&h=L&n=pt42.5.495&r=PART#se42.5.495_1304

27 Meaningful Use Objectives and Measures for EPs, Eligible Hospitals, and CAHs for 2015 Through 2017. Retrieved April 14, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=be3c237de2baebc9f93cc5ecfbed887c&ty=HTML&h=L&n=pt42.5.495&r=PART#se42.5.495_122

28 Social Security Act, § 1848(a)(7)(A). Retrieved March 23, 2016, from https://www.ssa.gov/OP_Home/ssact/title18/1848.htm

29 U.S. Congress. (2015, December 28). Patient Access and Medicare Protection Act, § 4. Retrieved March 23, 2016, from https://www.congress.gov/bill/114th-congress/senate-bill/2425/text

30 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.315 2015 Edition Health IT Certification Criteria, pp. 62747–62755). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

31 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.102 Definitions, pp. 62742–62743). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

32 False Claims, 31 U.S.C. § 3729. Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/pdf/USCODE-2013-title31-subtitleIII-chap37-subchapIII-sec3729.pdf

33 Civil Actions for False Claims, 31 U.S.C. § 3730. Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/pdf/USCODE-2013-title31-subtitleIII-chap37-subchapIII-sec3730.pdf

34 False, Fictitious, or Fraudulent Claims, 18 U.S.C. § 287. Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap15-sec287.pdf

35 Health Care Fraud, 18 U.S.C. § 1347. Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap63-sec1347.pdf

36 Wrongful Disclosure of Individually Identifiable Health Information, 42 U.S.C. § 1320d-6. Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/pdf/USCODE-2013-title42-chap7-subchapXI-partC.pdf

37 Social Security Act § 1128A(a). Retrieved March 23, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128A.htm

38 Social Security Act § 1128. Exclusion of Certain Individuals and Entities From Participation in Medicare and State Health Care Programs. Retrieved March 23, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128.htm

39 Patient Protection and Affordable Care Act, Pub. L. No. 111-148, Title X, § 10606(b), 124 Stat. 119, 1008 (2010, March 23). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf

40 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (pp. 3, 6, 9–10). [OEI-01-11-00571]. Retrieved March 24, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

41 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.210 Standards for Health IT, p. 62745). Retrieved March 24, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

42 American Society for Testing and Materials (ASTM). (2013). ASTM E2147-01: Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems. Retrieved March 24, 2016, from http://www.astm.org/Standards/E2147.htm

43 Federal Bureau of Investigation. (2013, April 10). Davenport Man Sentenced to Four Years in Prison for Theft of Patient Information. Retrieved March 24, 2016, from http://www.fbi.gov/tampa/press-releases/2013/davenport-man-sentenced-to-four-years-in-prison-for-theft-of-patient-information

44 Federal Bureau of Investigation. (2013, January 18). Former Florida Hospital Employee Sentenced to Federal Prison for Data Theft. Retrieved March 24, 2016, from http://www.fbi.gov/tampa/press-releases/2013/former-florida-hospital-employee-sentenced-to-federal-prison-for-data-theft

45 Federal Bureau of Investigation. (2014, November 13). Former Shelby County Hospital CFO Guilty in EHR Incentive Case. Retrieved March 24, 2016, from http://www.fbi.gov/dallas/press-releases/2014/former-shelby-county-hospital-cfo-guilty-in-ehr-incentive-case

46 Dimick, C. (2008). Record Limbo: Hybrid Systems Add Burden and Risk to Data Reporting. American Health Information Management Association. Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=85533

47 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (Data Segmentation for Privacy [DS4P], p. 62648). Retrieved March 24, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

48 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (p. 2). [OEI-01-11-00571]. Retrieved March 28, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

49 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

50 Association of American Medical Colleges. (2011, July 11). AAMC Compliance Officers' Forum. Electronic Health Records in Academic Medical Centers Compliance Advisory 2 (p. 2). Retrieved March 28, 2016, from https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf

51 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (p. 17). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

52 U.S. Office of Special Counsel. (2014, June 23). Letter (p. 4). Retrieved March 28, 2016, from http://buchanan.house.gov/sites/buchanan.house.gov/files/documents/OSCVALetter.pdf

53 Lerner, C. (2014, July 8). Testimony Before the Committee on Veterans' Affairs, U.S. House of Representatives (§ 2.3). Retrieved March 28, 2016, from https://veterans.house.gov/witness-testimony/the-honorable-carolyn-lerner

54 Association of American Medical Colleges. (2011, July 11). AAMC Compliance Officers' Forum. Electronic Health Records in Academic Medical Centers Compliance Advisory 2 (p. 2). Retrieved March 28, 2016, from https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf

55 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.210(e)(1)(i), (h); p. 62745). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

56 Terry, K. (2014, January 13). Feds Must Prioritize EHR Billing Fraud, Watchdogs Say. InformationWeek Healthcare. Retrieved March 28, 2016, from http://www.informationweek.com/healthcare/electronic-health-records/feds-must-prioritize-ehr-billing-fraud-watchdogs-say/d/d-id/1113403

57 U.S. Department of Health and Human Services. Office of Inspector General. (2014, June 25). Testimony of: Gary Cantrell, Deputy Inspector General for Investigations. Hearing: Medicare Program Integrity: Screening Out Errors, Fraud, and Abuse (p. 7). Retrieved March 28, 2016, from http://oig.hhs.gov/testimony/docs/2014/cantrell_testimony_06252014.pdf

58 U.S. Department of Health and Human Services. Office of Inspector General. (2016, April). Compendium of Unimplemented Recommendations (p. 45). Retrieved April 12, 2016, from http://oig.hhs.gov/reports-and-publications/compendium/files/compendium2016.pdf

59 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

60 U.S. Department of Health and Human Services. Office of Inspector General. (2016, January 7). Provider Self-Disclosure Settlements, "01-07-2016" (para. 1). Retrieved March 17, 2016, from http://oig.hhs.gov/fraud/enforcement/cmp/psds.asp

61 Definitions, 42 C.F.R. § 455.2. Retrieved March 30, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=13172ac148373d19cb780c2e424d16f2&node=se42.4.455_12&rgn=div8

62 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

63 American Society for Testing and Materials. (2013). ASTM E2147-01(2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, 1.2. Retrieved March 28, 2016, from http://www.astm.org/Standards/E2147.htm

64 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

65 Association of American Medical Colleges. (2011, July 11). AAMC Compliance Officers' Forum. Electronic Health Records in Academic Medical Centers Compliance Advisory 2 (p. 2) Retrieved March 30, 2016, from https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf

66 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

67 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.210(e)(1)(i), (h); p. 62745). Retrieved March 23, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

68 American Society for Testing and Materials. (2013). ASTM E2147-01(2013) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, 1.2. Retrieved March 28, 2016, from http://www.astm.org/Standards/E2147.htm

69 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

70 Schulte, F., & Donald, D. (2014, May 19). How Doctors and Hospitals Have Collected Billions in Questionable Medicare Fees. The Center for Public Integrity. Retrieved March 28, 2016, from http://www.publicintegrity.org/2012/09/15/10810/how-doctors-and-hospitals-have-collected-billions-questionable-medicare-fees

71 Potente, R. (2014, May 1). Maximizing the Future: The Case for Mandating Fraud Prevention Tools in Electronic Health Record Software (pp. 6–7). Seton Hall University eRepository. Retrieved March 28, 2016, from http://scholarship.shu.edu/student_scholarship/547/

72 Sebelius, K., & Holder, E. (2012, September 24). Letter to American Hospital Association, et al. Retrieved March 29, 2016, from https://archive.org/stream/440929-hhs-doj-letter/440929-hhs-doj-letter_djvu.txt

73 U.S. Attorney's Office. Eastern District of Missouri. (2014, July 28). Local In-Home Healthcare Provider Sentenced on Fraud Charges. Retrieved March 29, 2016, from https://www.justice.gov/usao/moe/news/2014/july/kuehl_tina.html

74 United States Attorney's Office. Southern District of New York. (2014, October 27). Manhattan U.S. Attorney Files Healthcare Fraud Lawsuit Against Computer Sciences Corp. and the City of New York for Orchestrating a Multimillion-Dollar Medicaid Billing Fraud Scheme. Retrieved March 29, 2016, from https://www.justice.gov/usao/nys/pressreleases/October14/CSCandCityofNewYorkSuitPR.php

75 Potente, R. (2014, May 1). Maximizing the Future: The Case for Mandating Fraud Prevention Tools in Electronic Health Record Software (pp. 4–5). Seton Hall University eRepository. Retrieved March 29, 2016, from http://scholarship.shu.edu/student_scholarship/547/

76 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (p. 1). [OEI-01-11-00571]. Retrieved March 29, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

77 Sebelius, K., & Holder, E. (2012, September 24). Letter to American Hospital Association, et al. Retrieved March 29, 2016, from https://archive.org/stream/440929-hhs-doj-letter/440929-hhs-doj-letter_djvu.txt

78 U.S. Attorney's Office. Northern District of Texas. (2013, August 27). Abilene, Texas, Dentist Pleads Guilty in Medicaid Fraud Scheme. Retrieved March 29, 2016, from https://www.justice.gov/usao/txn/PressRelease/2013/AUG2013/aug27Tuan_Truong_plea.html

79 U.S. Department of Justice. (2013, July 8). Supervisor of $63 Million Health Care Fraud Scheme Sentenced in Florida to 10 Years in Prison. Retrieved March 29, 2016, from https://www.justice.gov/opa/pr/2013/July/13-crm-763.html

80 U.S. Attorney's Office. Eastern District of Texas. (2015, June 17). Former Shelby County Hospital CFO Sentenced in EHR Incentive Case. Retrieved March 29, 2016, from https://www.justice.gov/usao-edtx/pr/former-shelby-county-hospital-cfo-sentenced-ehr-incentive-case

81 U.S. Attorney's Office. Eastern District of Texas. (2014, February 6). Former Hospital CEO Charged With Health Care Fraud. Retrieved March 29, 2016, from https://www.justice.gov/usao-edtx/pr/former-hospital-cfo-charged-health-care-fraud

82 Criminal Complaint at 4, United States of America v. Dale Munroe, No. 6:12-mj-1378 (M.D. Fl. 2013). Retrieved March 30, 2016, from http://www.thehealthlawfirm.com/uploads/USA_v_Munroe.pdf

83 U.S. Department of Health and Human Services. (2013, January 2). HHS Announces First HIPAA Breach Settlement Involving Less Than 500 Patients. Retrieved March 30, 2016, from http://www.hhs.gov/news/press/2013pres/01/20130102a.html

84 U.S. Department of Health and Human Services. (2013, December 26). Dermatology Practice Settles Potential HIPAA Violations. Retrieved March 30, 2016, from http://www.hhs.gov/news/press/2013pres/12/20131226a.html

85 U.S. Department of Health and Human Services. Office of Inspector General. (2015, March). Compendium of Unimplemented Recommendations (p. 33). Retrieved March 30, 2016, from http://oig.hhs.gov/reports-and-publications/compendium/files/compendium2015.pdf

86 U.S. Department of Health and Human Services. Office of the Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (p. 15). Retrieved March 30, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

87 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule (45 C.F.R. § 170.315 2015 Edition health IT certification criteria, p. 62751–62752). Retrieved March 30, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

88 Hirsch, M.D. (2015, September 8). Encrypted EHR data subject to 'alarming' leakage. Retrieved March 30, 2016, from http://www.fierceemr.com/story/encrypted-ehr-data-subject-alarming-leakage/2015-09-08

89 KCPQ 13 Fox TV. (2014, August 20). 90% of Hospitals and Clinics Lose Their Patients' Data. Retrieved March 30, 2016, from http://q13fox.com/2014/08/20/90-of-hospitals-and-clinics-lose-their-patients-data/

90 Mclean, R. (2016, February 17). Hospital Pays Bitcoin Ransom After Malware Attack. Retrieved March 30, 2016, from http://money.cnn.com/2016/02/17/technology/hospital-bitcoin-ransom/index.html

91 Heath, S. (2016, April 4). EHR Downtime Results From Ransomware Attacks at CA, IN Hospitals. EHR Intelligence. Retrieved April 5, 2016, from https://ehrintelligence.com/news/ehr-downtime-results-from-ransomware-attacks-at-ca-in-hospitals

92 Centers for Medicare & Medicaid Services. (2012, December 7). Update for Amendments, Corrections and Delayed Entries in Medical Documentation. § 3.3.2.5.B. Retrieved March 30, 2016, from https://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/Downloads/R442PI.pdf

93 U.S. Department of Health and Human Services. (2014, September 11). 2014 Edition Release 2 Electronic Health Record (EHR) Certification Criteria and the ONC HIT Certification Program; Regulatory Flexibilities, Improvements, and Enhanced Health Information Exchange; Final Rule. 79 Fed. Reg. 54430, 54463. Retrieved March 30, 2016, from http://www.gpo.gov/fdsys/pkg/FR-2014-09-11/pdf/2014-21633.pdf

94 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. Retrieved March 30, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

95 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (pp. 6, 9–10). [OEI-01-11-00571]. Retrieved March 30, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

96 Kusserow, R. P. (2014, September–October). Claims Processing Ongoing Monitoring and Auditing: Improves Revenue and Prevents Costly Errors (pp. 45–46). Journal of Health Care Compliance. Retrieved March 30, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf

97 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (p. 3). [OEI-01-11-00571]. Retrieved March 30, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

98 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Appendix C, Areas Recommended for Monitoring or Auditing for Detecting Alleged Fraud and Abuse Related to EHR Documentation. Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

99 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (p. 17). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

100 U.S. Office of Special Counsel. (2014, June 23). Letter (p. 4). Retrieved March 30, 2016, from http://buchanan.house.gov/sites/buchanan.house.gov/files/documents/OSCVALetter.pdf

101 Lerner, C. (2014, July 8). Testimony Before the Committee on Veterans' Affairs, U.S. House of Representatives (para. 2-3). Retrieved March 30, 2016, from https://veterans.house.gov/witness-testimony/the-honorable-carolyn-lerner

102 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

103 Boxwala, A., Kim, J., Grillo, J., & Ohno-Machado, L. (2011, May 2). Using Statistical and Machine Learning to Help Institutions Detect Suspicious Access to Electronic Health Records. Journal of American Medical Informatics Association, 18(4), 98. Retrieved March 30, 2016, from http://jamia.oxfordjournals.org/content/18/4/498

104 Taitsman, J., Chief Medical Officer, HHS-OIG. Remarks at the Affordable Care Act Provider Compliance Programs: Getting Started Webinar (2014, June 26).

105 Kusserow, R. P. (2014, September–October). Claims Processing Ongoing Monitoring and Auditing: Improves Revenue and Prevents Costly Errors (p. 46). Journal of Health Care Compliance. Retrieved March 30, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf

106 U.S. Government Accountability Office. (2011, December). Government Auditing Standards. §§ 2.10, 2.11 (pp. 18–19). Retrieved March 30, 2016, from http://www.gao.gov/assets/590/587281.pdf

107 Association of Certified Fraud Examiners. (2014). Fraud Examiners Manual § 1.260. Austin, Texas.

108 Specific Requirements, 42 C.F.R. § 438.608(b). Retrieved April 1, 2016, from https://www.gpo.gov/fdsys/pkg/CFR-2009-title42-vol4/pdf/CFR-2009-title42-vol4-sec438-608.pdf

109 Centers for Medicare and Medicaid Services. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 29). Medicare Learning Network. Retrieved April 1, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf

110 Kusserow, R. P. (2014, September–October). Claims Processing Ongoing Monitoring and Auditing: Improves Revenue and Prevents Costly Errors (p. 46). Journal of Health Care Compliance. Retrieved April 1, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf

111 IntegriGuard. (2013, March 28). Auditing the Electronic Health Record (p. 12). Auditing Community of Practice Call. Received July 29, 2014, from CMS.

112 Social Security Act § 1936(b). Retrieved April 1, 2016, from https://www.ssa.gov/OP_Home/ssact/title19/1936.htm

113 Centers for Medicare & Medicaid Services. Medicaid Integrity Program—General Information. Retrieved April 1, 2016, from https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram

114 U.S. Department of Health and Human Services. Office of the Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (p. 15). Retrieved April 1, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

115 U.S. Department of Health and Human Services. Office of the Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 11–12). Retrieved April 1, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

116 U.S. Department of Health and Human Services. Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (p. 9). Retrieved April 1, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

117 U.S. Department of Health and Human Services, Office of Inspector General. (2014, January). CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs (pp. 6, 9–10). Retrieved April 1, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

118 The Institute of Internal Auditors. (2009, December). Internal Auditing and Fraud (p. 23). Retrieved April 1, 2016, from https://www.louisiana.edu/sites/auditor/files/1011919_2029.dl_PG%20IA%20and%20Fraud.pdf

119 U.S. Department of Health and Human Services. The Office of the National Coordinator for Health Information Technology. (2007, June). Recommended Requirements for Enhancing Data Quality in Electronic Health Record Systems. Retrieved April 1, 2016, from http://www.rti.org/pubs/enhancing_data_quality_in_ehrs.pdf

120 Murphy, A. P., & Vandenberg, Q. H. (2003, September/October). How to Conduct a Fraud Investigation (p. 18). Retrieved April 1, 2016, from http://www.mhtl.com/pdf/How%20To%20Conduct%20A%20Fraud%20Investigation.pdf

121 Kusserow, R. (2013, June 11). Proven Strategies for Conducting Internal Investigations (Slide 21). [Name and email address required]. Retrieved April 1, 2016, from http://www.compliance.com/webinar-proven-strategies-for-conducting-internal-investigations

122 The Institute of Internal Auditors. (2009, December). Internal Auditing and Fraud (pp. 24–26). Retrieved April 1, 2016, from https://www.louisiana.edu/sites/auditor/files/1011919_2029.dl_PG%20IA%20and%20Fraud.pdf

123 Trostorff, D., & Chilson, M. R. (2014, February 11). 401 Managed Care Compliance: RAC, RADV, False Claims Act and OIG CMS Initiatives Medicare/Medicaid Track (pp. 34–35). Retrieved April 1, 2016, from http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Managed_Care_Compliance_Conference/2014/401_MCC_RACRADVFalseClaimsAct_2.pdf

124 42 C.F.R. § 1003.106(b)(2). Retrieved April 1, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=33c7b3300b6069e89c48826818591436&ty=HTML&h=L&r=SECTION&n=42y5.0.2.5.4.0.32.7

125 Medicare and State Health Care Programs: Fraud and Abuse; Revisions to the Office of Inspector General's Monetary Penalty Rules; Proposed Rule. 79 Fed. Reg. 27080, 27082, 27094 (proposed May 12, 2014). Retrieved April 1, 2016, from http://oig.hhs.gov/authorities/docs/2014/fr-79-91.pdf

Disclaimer

This booklet was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This booklet was prepared as a service to the public and is not intended to grant rights or impose obligations. This booklet may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

June 2016