Electronic Health Records

Detecting and Responding to Fraud, Waste, and Abuse Associated With the Use of Electronic Health Records

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Content Summary

This booklet provides information on methods to identify and address improper payments and potential fraud, waste, and abuse associated with the use of electronic health records (EHRs). The booklet concludes with how to investigate and correct EHR-related fraud and abuse, and how to refer violations to law enforcement.

It is important for providers and others who maintain or use electronic health records (EHRs) to take measures to prevent and detect fraud, waste, and abuse that can be associated with them. Preventive measures that providers can take to promote the appropriate use of EHRs are discussed in the fact sheet "A Compliance Program for Electronic Health Records" posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the Centers for Medicare & Medicaid Services (CMS) website. Once preventive measures are in place, providers and others should implement methods to detect and respond to instances of improper use.

These methods include internal monitoring, auditing, investigation, and referral. Monitoring is an ongoing effort that seeks to identify incidents that might indicate unauthorized access to EHRs or fraud, waste, and abuse. Auditing is a periodic review of sample data to determine whether providers and others are meeting standards. If either monitoring or auditing shows possible wrongful conduct, the provider should conduct a timely investigation to establish a basis for a response. An appropriate

response may include repayment of improperly paid funds, employee discipline, and referral to a regulatory agency or law enforcement. If the investigation demonstrates weaknesses in the detection system or in policies, corrective action should include changes to address these weaknesses.

Methods of Detection

Methods for detecting unauthorized EHR access and fraud, waste, and abuse include internal monitoring, auditing, and investigation.

Internal Monitoring

Providers who use EHR systems should have strong monitoring programs in place.[1, 2] Monitoring is an ongoing effort that occurs during normal operations and is intended to verify day-to-day compliance with policy.[3, 4]

Risk Areas for Monitoring

Base general compliance monitoring programs on careful identification of the areas that are at the greatest risk of noncompliance.[5] Likewise, base programs to monitor EHR systems on the risk areas related to EHRs. One of the biggest risks is the risk of unauthorized access to, or dissemination of, EHRs. To identify possible instances of unauthorized access, monitoring programs should identify situations in which a patient:

- Has the same last name as the user;
- Is well-known (for example, a political figure or celebrity);
- Is being treated for a newsworthy disease (for example, AIDS);
- Was admitted as the result of an accident that may lead to insurance payments or litigation (for example, a motor vehicle accident); or
- Is a current or terminated employee.[6]

EHR System Features to Monitor

The risk of fraud, waste, or abuse arises from improper use of features such as cut and paste, copy and paste, or templates. A recent report by the U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) found that only 24 percent of all hospitals have policies governing the use of the copy-paste feature in EHR software.[7] The ways in which these features can lead to fraud, waste, and abuse are discussed in the booklet "Program Integrity Issues in Electronic Health Records: An Overview" posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

There are several ways to detect some types of improper use. One way is to program the EHR system to cause copied and pasted information to appear in a distinct color to identify it in both electronic and printed formats.[8] Another way is to use the EHR system to identify alterations and deletions completed after the event occurred.[9]

Audit Logs

Track the times of alterations and deletions through the system's audit log. The log should automatically "track changes within a record chronologically by capturing data elements, such as date, time, and user stamps, for each update to an EHR."[10] All EHR systems certified by the Office of the National Coordinator for Health Information Technology (ONC) are required to include a log.[11] Since certified systems include audit logs, HHS-OIG suggests that entities reviewing provider records for compliance should use them.[12] For the same reason, providers should use audit logs in monitoring their EHR systems.

HHS-OIG recommends never disabling EHR audit logs. They should remain operational.[13] If providers find the need to disable the log in unusual circumstances, such as a critical system need or a natural disaster, policy should specify these circumstances, identify the persons who are authorized to disable the log, and require that the person disabling the log be identified and the circumstances documented. Policy should also require that no auditable events, such as data entry, take place while the log is disabled.

Although tamper resistance is not required for certification by ONC, providers should use tamper-resistant audit logs.[14] If the audit log is disabled and someone makes untracked entries and changes to the EHRs before the log again becomes operational, the monitoring program should identify entries that are unattributed to anyone. It should also identify any unexplained gaps in system activity. Less than 50 percent of hospital audit logs record how the individual entered the data (for example, direct text entry).[15] Audit log features and policies are further discussed in the booklet "Program Integrity Issues in Electronic Health Records: An Overview" posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

Other Monitoring Tools

Other automated processes in addition to the audit log can be used to make monitoring EHRs more effective. A common indicator of improper use of EHRs is the appearance of identical text in different patient records[16, 17] or the same patient record.[18] Using software commonly employed by academic institutions to detect plagiarism in student work automates the identification of these instances.[19] In a study published in 2013,

researchers used such software to measure the extent of copying and pasting in an intensive care unit.[20]

Automated fraud-prevention software can identify EHR-related fraud, waste, and abuse. One type of software performs predictive modeling, which "statistically analyzes known frauds in historical claims data and looks for similarities in new claims." Another detection process is anomaly detection, which "looks for outliers in behavioral patterns."[21] Such outliers would include practitioners with higher utilization of specific services, such as X-rays, than similarly situated practitioners. Other outliers would be claims consisting of "never" events, such as prostate-specific antigen screening for a female beneficiary.

Monitoring for Small Practices

A small practice will not likely have sophisticated monitoring or fraud-prevention software, but the practice can still have an effective monitoring program. A monitoring program could consist of a billing person and a medically trained person manually reviewing a set number of randomly selected claims and accompanying EHRs every week. To maintain the integrity of the process, the medically trained person should not review any records in which they made entries. To avoid overburdening any of the providers in the practice, the providers could take turns performing these reviews. This is consistent with the approach HHS-OIG recommends for small practices in performing periodic audits, noted later in this section.[22] Regardless of whether a small practice, a managed care plan, or others are doing the monitoring, it is essential that a person specifically assigned to this duty reviews the items identified as suspect on a set schedule.[23]

Other Opportunities to Monitor

In addition to performing an ongoing review for indicators of potential fraud, waste, or abuse, monitoring should also include regular review of complaints or tips from employees, providers, patients, or others. Ways to facilitate receipt of this information are:

- Have open lines of communication between employees and the compliance officer or, in a small plan or practice, the designated compliance contact;[24]
- Establish methods, such as a hotline or a dedicated online site, to accept complaints or tips from patients, employees, providers, or others who suspect EHR fraud;[25] and
- Adopt EHR systems that allow patients to comment in their EHR[26] and automatically generate a notification that can lead to further review.

If review of the information identified by the monitoring program indicates possible fraud, waste, or abuse, the information should be the subject of a preliminary investigation and, when appropriate, referred as discussed later on in this document.

Internal Auditing

An effective plan to detect EHR-related fraud, waste, and abuse requires both internal monitoring and auditing. Perform internal claims audits for general compliance by periodically examining a sample of claims and associated records to determine whether the practice is meeting compliance standards.[27] Likewise, an EHR audit should examine a sample of the claims, associated EHRs, and audit log entries in light of standards for documentation, coding, and billing.

Managed care companies and large practices may have a dedicated department to perform internal audits. Small practices do not have such departments, but they can still perform effective internal audits. HHS-OIG suggests that in a small practice, the billing person and one medically trained person could perform an internal claims audit by reviewing a random sample of at least five records, and the accompanying claims, per provider.[28] More information on internal monitoring and auditing to detect fraud, waste, and abuse associated with EHRs is available in the job aid "Conducting Internal Monitoring and Auditing" posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

Preliminary Investigation of Suspected Offenses Related to EHRs

Detection is not an end in itself. As set forth in the Federal rules governing compliance in Medicaid managed care plans,[29] and in the HHS-OIG compliance guidance for small practices, after detecting an incident of possible fraud, waste, or abuse, it is important to do a preliminary investigation to confirm a violation took place.[30]

A managed care plan or large provider can investigate suspected incidents of fraud, waste, and abuse through a dedicated office such as a special investigation unit. Small practices do not have such units, but they can still do a preliminary investigation by assigning this duty to the compliance contact or other designated person. A preliminary investigation simply requires identifying and reviewing the relevant documents, talking with people who have relevant knowledge, evaluating the results in light of the relevant law and policies, and setting forth this information in a written report. Someone other than its author should review the report to determine whether the practice received an improper payment and whether a law violation may have occurred.

Prompt Response and Corrective Action

If warranted by the investigation, managed care plans and providers should take corrective action, which can include returning funds that were improperly paid, taking disciplinary action, changing or updating computer software and systems, and revising policies.[31] When making changes, all-employee training should be required. In the case of employee misconduct, corrective action could include retraining, disciplinary action, or termination. It is important that the disciplinary action taken is appropriate to the misconduct.

Plans and providers should refer potential criminal violations to the appropriate agency for further investigation. States may require contracting managed care plans to refer such incidents to the State Medicaid agency (SMA) program integrity unit, to the State Medicaid Fraud Control Unit, or to another designated agency. Based on HHS-OIG guidance to SMAs, referrals from providers and others to law enforcement or a regulatory agency should include a written report of the investigation and copies of the relevant documents and policies.[32] After the referral, providers and others should be prepared to accommodate law enforcement requests for access to the EHR system and for additional information about how the system works.

Conclusion

Monitoring and auditing can help identify EHR-related incidents that might indicate fraud, waste, and abuse or unauthorized access to EHRs. Investigate identified incidents to establish whether wrongful conduct occurred. The provider should take corrective action if wrongful conduct is verified, which can include repayment, changes to systems and processes, employee discipline, and referral to a regulatory agency or law enforcement.

To see the electronic version of this booklet and other products 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 Meeks, D.W., Smith, M.W., Taylor, L., Sittig, D.F., Scott, J.M., & Singh, H. (2014, June 20). An Analysis of Electronic Health Record-Related Patient Safety Concerns (p. 1). Journal of the American Medical Informatics Association. Retrieved April 5, 2016, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4215044/

2 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 April 5, 2016, from http://www.compliance.com/wp-content/files_mf/jhcc_091014_kusserow.pdf

3 Meeks, D.W., Smith, M.W., Taylor, L., Sittig, D.F., Scott, J.M., & Singh, H. (2014, June 20). An Analysis of Electronic Health Record-Related Patient Safety Concerns (p. 1). Journal of the American Medical Informatics Association. Retrieved April 5, 2016, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4215044/

4 Centers for Medicare & Medicaid Services. Medicare Learning Network. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slides 27, 28). Retrieved April 5, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf

5 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437–38. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

6 American Health Information Management Association. (2014, March). Privacy and Security Audits of Electronic Health Information (2014 Update). Retrieved April 14, 2016, from http://library.ahima.org/PB/PrivacySecurityAudits

7 U.S. Department of Health and Human Services. Office of Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (p. 14). Retrieved April 13, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

8 American Health Information Management Association. (2009, January). Auditing Copy and Paste. (pp. 26–29). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=87789

9 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). (pp. 58–62). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

10 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). Retrieved April 5, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

11 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(e)(1)(i). Retrieved April 5, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

12 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. 9–10). Retrieved April 5, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

13 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. 3, 15). Retrieved April 13, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

14 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(e)(1)(i). Retrieved April 5, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

15 U.S. Department of Health and Human Services. Office of Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (p. 14). Retrieved April 13, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

16 U.S. Department of Health and Human Services. Office of Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 14–16). Retrieved April 5, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

17 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). (pp. 58–62). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

18 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). (pp. 58–62). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

19 Skrocki, M. (2013, August 5). Can Plagiarism Detection Tools Catch EHR Upcoding? Government HealthIT. Retrieved April 5, 2016, from http://www.govhealthit.com/news/how-plagiarism-detection-tools-could-catch-ehr-upcoding

20 Thornton, J.D., Schold, J.D., Venkateshaiah, L., Lander, B. (2013, February). Prevalence of Copied Information by Attendings and Residents in Critical Care Progress Notes. [Abstract]. Retrieved April 5, 2016, from http://journals.lww.com/ccmjournal/Abstract/2013/02000/Prevalence_of_Copied_Information_by_Attendings_and.2.aspx

21 Harris, K. (2013, October). Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, (pp. 14–15). California Department of Justice. Retrieved April 5, 2016, from http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf

22 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

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

24 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59443–44. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

25 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59444. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

26 U.S. Department of Health and Human Services. Office of Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 3–5, 13–15, 18–19, Appendix A). Retrieved April 5, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

27 Centers for Medicare & Medicaid Services. Medicare Learning Network. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 27). Retrieved April 5, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf

28 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

29 42 C.F.R. § 438.608. Retrieved April 5, 2016, from http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=ad31122e097dee68a5353d923848f54e&ty=HTML&h=L&r=SECTION&n=se42.4.438_1608

30 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59443. Retrieved April 5, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

31 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved April 5, 2016, from http://oig.hhs.gov/compliance/compliance-guidance/index.asp

32 Centers for Medicare & Medicaid Services. CMS-MIG Performance Standard for Referrals of Suspected Fraud From a Single State Agency to a Medicaid Fraud Control Unit. Retrieved April 5, 2016, from https://www.cms.gov/FraudAbuseforProfs/downloads/fraudreferralperformancestandardsstateagencytomfcu.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