Fact Sheet

Documentation Integrity in Electronic Health Records

Introduction

With the ongoing implementation of electronic health record (EHR) systems, it is important that documentation integrity be at the forefront. Documentation integrity involves the accuracy of the complete health record. It encompasses information governance, patient identification, authorship validation, amendments, and record corrections. It also includes auditing the record for documentation validity when submitting reimbursement claims.[1]

Software Features and Capabilities

A "Base EHR" is a digital version of a patient's health history. A provider can share a patient's EHR securely with several other providers across different organizations at once, and all authorized providers may contribute relevant information to support clinical decision-making.[2] Although there is a wide range of EHR software features and capabilities, this fact sheet will focus on those features and capabilities related to program integrity.

EHR software includes features and capabilities that allow for customized documentation, including the ability to copy and paste or use templates and smart phrases. When used appropriately, EHR software features offer great benefits to providers, patients, and others. The software can help them more efficiently document more complex examination records and create better and more complete notes.[3]

The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) identified EHR software features, such as record cloning and copy and paste, among the common EHR features improperly used to facilitate fraud, waste,

and abuse.[4] In 2011, the American Health Information Management Association noted that, despite high expectations for EHRs to improve patient health care, "the use of the copy functionality has the potential to negatively affect the integrity of the health record."[5] EHR features such as macros and templates allow for auto-fill of information that can create unintended documentation errors in the medical record. Safety and security features in the EHR system that users can disable, such as drug-interaction warnings for patient safety, audit logs, and access restrictions, can also affect the integrity of EHR documentation.

Preserving Documentation Integrity

Ensuring the integrity of EHR documentation is important to help prevent fraud, waste, abuse, and improper payments. It is critical that EHR systems include software capabilities aimed at ensuring that integrity. The 2015 final rule for Health IT certification, effective January 2016, adds 45 Code of Federal Regulations Section 170.315, which codifies several important integrity features. See subparagraph (d) Privacy and Security for complete description. Some highlights include:

- User authentication and access management/authorization;
- Auditable events and tamper resistance, including a record of the audit log and encryption status, who changed the statuses and when, and the limited number of users who are authorized to change those statuses;
- Optimal security settings are set by default;
- Inability to change, overwrite, or delete audit log events;
- Ability to detect if the audit log has been altered; and
- Ability to time-out access after a specified period of nonuse.[6]

Providers and others are encouraged to customize their EHR systems to include these software features.

The requirement to have an audit log operational whenever the EHR technology is available for updates or viewing was recommended in a report commissioned by ONC[7] and by HHS-OIG in its 2013 report on hospital EHR technology.[8] According to HHS-OIG, the EHR system audit log should always be operational, should be stored as long as clinical records, and should never be altered.[9]

Another method of ensuring EHR documentation integrity is to develop administrative and clinical documentation policies and procedures and standards of conduct that provide a framework for proper use. Policies and procedures with clearly defined roles and responsibilities, as well as identification of specific individuals accountable for the

accuracy and integrity of information, will help preserve the integrity of documentation in EHRs. Periodically monitoring and auditing EHR documentation, establishing clear channels for reporting errors in documentation, and promptly correcting any known errors are also effective ways of mitigating EHR documentation integrity risks.

Providers and others are encouraged to present targeted training on policies and procedures related to properly using EHR software features, specifically those that protect EHR documentation integrity. Training should communicate individual responsibilities and the capabilities and functions of the EHR system to each individual who works with EHRs. The training should also explain responsibilities for maintaining the integrity and accuracy of information.[10]

Conclusion

Documentation integrity in EHRs is important to help prevent fraud, waste, abuse, and improper payments. Providers and others should use program integrity-related EHR software features and capabilities to ensure the integrity of the EHR documentation. Some EHR features may create information integrity concerns; however, providers and others can mitigate these concerns by implementing proper policies and processes.

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

2 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 April 4, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

3 Silverstone D.E., & Lim M.C. (2014, February). Ensuring Information Integrity in the Electronic Health Record: The Crisis and the Challenge. Ophthalmology, 121(2), 435–437. Retrieved April 4, 2016, from http://www.aaojournal.org/article/S0161-6420(13)00705-7/abstract

4 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. Retrieved April 4, 2016, from http://oig.hhs.gov/testimony/docs/2014/cantrell_testimony_06252014.pdf

5 Silverstone D. E., & Lim M.C. (2014, February). Ensuring Information Integrity in the Electronic Health Record: The Crisis and the Challenge. Ophthalmology, 121(2), 435–437 (cited from Warner, D. and Wiedeman, L.A., Managing Copy Functionality and Information Integrity in the EHR, Journal of AHIMA, March 2012). Retrieved April 4, 2016, from http://www.aaojournal.org/article/S0161-6420(13)00705-7/abstract

6 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 Information Technology to Protect Electronic Health Information Created, Maintained, and Exchanged, pp. 62751–752). Retrieved April 4, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

7 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. ES-5). Retrieved April 4, 2016, from https://www.rti.org/sites/default/files/resources/enhancing_data_quality_in_ehrs.pdf

8 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. 15–16; Appendix A). Retrieved April 4, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

9 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 April 4, 2016, from http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf

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

Disclaimer

This fact sheet 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 fact sheet was prepared as a service to the public and is not intended to grant rights or impose obligations. This fact sheet 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