Guidelines for EHR Documentation to Prevent Fraud

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Electronic documentation tools offer exciting new time-saving and validity checking features designed to enhance communication for all health record users. They address traditional, well-known requirements for documentation principles, while supporting expansive new HIM capabilities. However, use of these features without appropriate management and guidelines may cause invalid autopopulation of data fields, manufactured documentation to enhance expected reimbursement, and other undesirable outcomes.

There are a number of existing regulations and laws on documentation principles, as well as rapidly accumulating experiences translating core HIM principles into the electronic realm. Existing resources address documentation authorship principles, auditing, and forms development, and new ones are emerging to ensure and preserve documentation integrity in an age of electronic identity theft and changes in the legal evidentiary requirements for electronic business and clinical records.

From these, AHIMA's e-HIM® work group developed documentation guidelines to inform EHR users and software developers of the potential for fraudulent activity and assist them in developing preventive measures. These guidelines also help support the creation of functional standards. This article outlines the guidelines to prevent EHR documentation fraud. Additional materials, including appendices, guidelines for electronic documentation, a resource list, a checklist for fraud prevention vigilance, and three case studies, are available online in the FORE Library: HIM Body of Knowledge.

Healthcare Fraud

Healthcare fraud is defined as an "intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party."[1] EHR users should not expect unintentional deception or misrepresentation to be viewed more gently by payers, evaluators, or litigators. However, one of the many changes HIPAA legislation rendered is that the standard is now "known or should have know." This shifted burden significantly by including the concept that those submitting claims have a due diligence obligation to proactively identify and prevent fraud, as the burden now is that the deception or misrepresentation need not be known or intentional but should have been known. An indication of the seriousness of this issue can be found in the Foundation of Research and Education's "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities," bolstered by the increasing number of media articles that focus on compliance issues surrounding an EHR.[2] (Appendix A includes a list of resources with additional information about electronic documentation compliance.)

Identified Areas of Concern

There are four areas of concern regarding the EHR environment:

- **Authorship integrity:** borrowing record entries from another source or author and representing or displaying past as current documentation and (in some instances) misrepresenting or inflating the nature and intensity of services provided.
- **Auditing integrity:** inadequate auditing functions that make it impossible to detect when an entry was modified or borrowed from another source and misrepresented as an original entry by an authorized user.
- **Documentation integrity:** automated insertion of clinical data and visit documentation using templates or similar tools with predetermined documentation components with uncontrolled and uncertain clinical relevance.
- **Patient identification and demographic accuracy:** automated demographic or registration entries generating erroneous patient identification, leading to patient safety and quality of care issues as well as enabling fraudulent activity involving patient identity theft or providing unjustified care for profit.

The case studies in appendix B serve as discussion starters and educational handouts for compliance training to avoid the concerns listed above.

Authorship Integrity

Authorship Accuracy and Comprehensiveness. Authorship is the origin of recorded information that is attributed to a specific individual or entity.[3] EHRs must allow more than one party to add additional text to the same entry and retain and display the authorship of each entry. For instance, a nurse or alternate user may begin a patient's encounter note and later on, the examining physician adds comments.

In systems that require a single authorization for visit notes, the entire note may be attributed to the physician, and entries or observations by alternate users may be edited or deleted before final physician authentication despite the alternate users' authentication. Another example includes flowcharts allowing entries by multiple individuals over a period of time and requiring only one signature at the end of the encounter, thus losing the identities of caregivers who posted interim data.

In these situations it may be impossible to verify the actual provider of care or the amount of work performed by each person providing services. When records are analyzed and clinical codes reported for billing, the claim may reflect the wrong provider and level or type of care. One method of healthcare fraud involves using unlicensed individuals to perform services, while submitting claims under the provider number of a legitimate provider. It is the user's duty to ensure that all documentation authorship is accurately recorded in all approved uses of the documentation tools available.

Autoauthentication or Systematic Authorship Misrepresentation. Progress notes are considered assertions of a person and are authenticated for legal admissibility in a court of law. Autoauthentication methods that do not require an author to review the entry fall short of federal and state authentication requirements and place the organization at legal risk.[4] Some providers choose not to enter their own progress notes electronically and use scribes or assistants to type entries into the system for subsequent authorization. Policies, procedures, and checks and balances must be in place to ensure that the physician or legally responsible individual reviews the health record entries and affixes an authorization compliant with existing law. Since health record documentation drives payment from health plans, inaccurate information may lead to perceived fraudulent activities.

Borrowing Data from Other Sources Including Copy-and-Paste or Pull-Forward Techniques. Electronic tools make it easier to copy and paste documentation from one record to another or pull information forward from a previous visit, someone else's records, or other sources, either intentionally or inadvertently. (The first case study in appendix B illustrates examples of worst and best case situations observed in documentation practices for healthcare delivery.)

There are studies that show that the ability to "copy previous entries and paste into a current entry" lead to a record where a clinician may, upon signing the documentation, unwittingly swear to the accuracy and comprehensiveness of substantial amounts of duplicated or inapplicable information as well as the incorporation of misleading or erroneous documentation. The studies further illustrate that, while helping to improve apparent timeliness and legibility of documentation, additional adverse effects were created by the inability to verify actual authors or to authenticate services provided at any given time.[5–8] From a billing perspective, defaulting clinical information with previous existing documentation from other patient encounters facilitates billing at a higher level of service than was actually provided.

Because of industry and regulatory payment pressures, physicians may find it necessary to document each component of the history and physical or review of systems during a patient encounter for payment and quality measurement. Time constraints and patient care demands can sometimes make it difficult for clinicians to meet the evaluation and patient management documentation requirements, creating the temptation to copy and paste. Shortcuts developed in the absence of consideration of clinical purpose can, unless clinicians are fully aware of risk and therefore undertake appropriate review, result in erroneous records and elevate the potential for fraudulent activity. Difficulties resulting from these practices include:

- Inaccurate representation of authorship of documentation
- Duplication of inapplicable information (relevant to the original case but not true for current care)
- Incorporation of misleading or erroneous documentation due to loss of context that was available to users in the original source
- Inclusion of entries from documentation created by others without their knowledge or consent

- Inability to accurately determine services and findings specific to a patient's encounter
- Inaccurate automated code generation associated with documentation

Auditing Integrity

Authentication and Amendment/Correction Issues. If an EHR lacks adequate audit trail functionality, there may be no way to determine if and when corrections or amendments were made to the documentation, by whom, or the nature of the correction or amendment. In addition to the normal unintentional mistakes that occur in documentation, there may be situations where the alteration of records is performed to prevent the discovery of damaging information or to avoid legal action. Without an adequate auditing function always "on" in an EHR system, legitimate changes may not be distinguishable from illegitimate ones, and the latter type may be accepted as fact and may be untraceable. Any changes or deletions made outside of routine record use must be maintained in the EHR system. Any uncertainty as to the integrity of the record creates legal liability for the institution while protecting criminal activity. (See appendix C, "Steps to Prevent Fraud in EHR Documentation.")

The functionality of the EHR may also determine whether or not an original note or amendment includes the correct date and time. Some systems automatically assign the date that the entry was made, while others allow authorized users to revise the date of entry to the date of the visit or service. It is imperative that any system be able to identify the date the note or amendment originated and the service date that the note or amendment references. Otherwise, the date sequence may be impossible to follow, adversely affecting appropriate patient care and resulting in questionable supporting documentation for reported services. (See case study 2 in appendix B for examples of best and worst case scenarios and discussion questions related to data integrity.)

Some EHR systems allow more than one party to add additional text to the same entry, for example, when faculty physicians are required to cosign resident notes. If the EHR does not have functionality to enable both providers to document and sign, it may be impossible to verify the actual provider of care or the amount of work performed by each person providing services. When records are analyzed and clinical codes reported for billing, the claim may reflect the wrong provider or incorrect level or type of care.

As stated before, autoauthentication, defined as signing multiple documents at one time without opening the documents, falls short of federal and state authentication requirements and could place the organization at legal risk.[9] Some providers use scribes or assistants to type entries into the system for subsequent authorization. In some situations, the physician or other provider gives his or her access codes to assistants to allow direct entry of the notes. The system recognizes the author as the physician or the other authorized provider of care, instead of the assistant. Checks and balances must be in place to ensure that the physician or other legally responsible individual has reviewed the health record entries and authenticated them compliant with existing law.

Documentation Integrity: Automated Insertion of Clinical Data

Documentation templates are sometimes employed to enter default common findings into health record documents. For example, the automatic generation of common negative findings within a review of systems for each body area or organ system. Template users (often physicians) should document pertinent positive results and delete incorrect autogenerated entries.

The primary reason templates are used is to save time. A physician not fully aware of the consequences of defaulting information in templates may fail to take the time necessary to review all defaulted data for changes and leave incorrect information in the record. This can lead to an inappropriate clinical picture, and the accuracy of the entire documented entry may be questioned. Documentation can be especially suspect when used as the basis for service justification or other payment concerns without evidence of clinical relevance.

EHR systems must allow limited automatic creation of information. In the hands of criminals, autogenerated documentation for health records can enable rapid and plausible claims to both government and private health plans for payment. Clinical coding professionals rely on documentation for code assignments used on health plans. If the documentation isn't true, the codes do not accurately reflect the circumstances of the healthcare service even when the codes are completely consistent with the documentation in the record. The "dirty data" resulting from inappropriate use of these tools compromises both good patient care and data-mining capabilities.

Templates often provide clinical information by default and design. When used inappropriately, they may misrepresent a patient's condition and might not reflect changes in a condition.[10] These tools may also include defaults such as "reviewed past, family, and social history" for frequent visits, which is often not indicated or performed each time. Unless the physician or other authorized provider removes the defaulted documentation from the visit note, a higher level of service than actually is provided could be assigned as well as a higher level of service claimed than might be appropriate for the service.

All templates and autogenerated entries, such as laboratory results, have the potential to be problematic. Accordingly, management oversight is necessary. Appropriate care must be taken that the data captured and stored are accurate, complete, and associated with the correct patient record and encounter.

One example of a beneficial feature of EHR systems is the autopopulation of discrete clinical data (i.e., laboratory results) in the appropriate data fields rather than requiring a physician or other authorized provider to document the results with a progress note. Anecdotal information indicates that data generated as close as possible to the point of care are the most accurate and least likely to be connected with healthcare fraud.

Patient Identification and Demographic Data

Some EHR systems include capabilities for additional efficiency in health service financial management transactions and billing processes. Demographic and insurance information may be defaulted for a patient's encounter. Based on a setting or type of service, the system can automatically assign a registration status or discharge disposition. Audit functions must be implemented to ensure that appropriate and legitimate information results and errors can be tracked for correction and staff training purposes. Health plan or payer policies may include patient care setting adjustments such as an office, hospital, or outpatient department for physician services. If a registration status is incorrectly assigned, the location of service and technical, professional, or global billing may be inappropriately reimbursed.

Patient identity theft is also an area of vulnerability for healthcare organizations. In the wrong hands, Medicare, Medicaid, and other health plan claims data coupled with the ability to manufacture supporting documentation creates the risk of false claims and criminal activity. Patient safety and quality of care issues arise when physician order entry systems fail to provide appropriate safeguards to identify fraud and abuse or business agreements involving data management violate patient privacy or allow unscrupulous providers to provide care that is unnecessary or fails to meet community standards for quality. (Review case study 3 in appendix B for examples of common situations and discussion questions.)

Solutions for Success in Fraud Prevention when Using EHR Features

Appendix C, "Best Practices for Fraud Prevention," combined with the checklist provided in appendix D form the basis for action to prevent misuse of electronic documentation tools used for undeserved financial gain.

Preventing fraud resulting from deliberate falsification of information requires three primary conditions:

- Organizational desire and commitment to conduct business and provide care in an ethical manner
- Organizations purchasing systems that include functions and capabilities to prevent or discourage fraudulent activity
- Organizations implementing and using policies, procedures, and system functions and capabilities to prevent fraud

The guidelines and checklists created by this work group and available in the FORE Library: HIM Body of Knowledge contain:

- Steps organizations can take to prevent falsification of EHRs
- Guidelines for selecting EHR systems features to reduce the likelihood for falsification
- Guidelines for implementing EHR systems features designed to reduce the likelihood of falsification
- Fraud prevention education programs (training requirements, security and integrity requirements, violation of EHR policy and procedure consequences)
- Recommendations for establishing a process for logging all activity on EHR systems (audits and audit trails recommended)
- Sample business rules for EHR systems

Notes

1. National Health Care Anti-fraud Association. "What is healthcare fraud?" Available online at www.nhcaa.org/about_health_care_fraud/Consumer_Information.
2. Foundation of Research and Education. "Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities." September 30, 2005.
3. AHIMA e-HIM Work Group on Maintaining the Legal EHR. "Update: Maintaining a Legally Sound Health Record-Paper and Electronic." *Journal of AHIMA* 76, no. 10 (2005): 64A–L.
4. Ibid.
5. Helbig, Susan. "Copying and Pasting in the EHR-S: An HIM Perspective." 2004 IFHRO Congress & AHIMA Convention Proceedings, October 2004. Available in the FORE Library: HIM Body of Knowledge.
6. Weir, CR, et al. "Direct Text Entry in Electronic Progress Notes: An Evaluation of Input Errors." *Methods of Information in Medicine* 42, no. 1 (2003): 61–67.
7. Hammond, Kenric W., et al. "Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting and Duplication." AMIA Annual Symposium Proceedings, 2003: 269–273.
8. Embi, Peter, J., et al. "Impacts of Computerized Physician Documentation in a Teaching Hospital: Perceptions of Faculty and Resident Physicians." *Journal of the American Medical Informatics Association* 11, no. 4 (2004): 300–309.
9. AHIMA e-HIM Work Group on Maintaining the Legal EHR. "Update: Maintaining a Legally Sound Health Record-Paper and Electronic."
10. Embi, Peter J., et al. "Impacts of Computerized Physician Documentation in a Teaching Hospital; Perceptions of Faculty and Resident Physicians."

Prepared by

AHIMA e-HIM Work Group Members

Danita Arrowood, RHIT, CCS
Emily Choate, CPC
Elizabeth Curtis, RHIA
Susan DeCathelineau, MS, RHIA
Barbara Drury, BA, SHIMSS
Susan Fenton, MBA, RHIA
Reed Gelzer, MD, MPH, CHCC
Alan Goldberg, JD, LLM
Pawan Goyal, MD, MHA, MS, PMP, CPHIMS
Teresa Hall, RHIT
Melissa Harper, RHIT
Patrice Jackson
Neisa Jenkins, MA, RHIA
Elaine King, MHS, RHIA, CHP
Jaclyn Kirkey, MBA, RHIA
Dorothy Knuth, RHIT, CCS-P
Susan Lee, RN, CHCQM, CCS-P, AHFI
Dale Miller
Deborah Neville, RHIA, CCS-P
Laurie Peters, RHIT, CCS
Erik Pupo
Ulkar Qazen, RHIA
Sandra Saunders, MPH, RHIA, CHP
Rita Scichilone, MHSA, RHIA, CCS, CCS-P
Patricia Trites, MPA, CHP, CPC, EMS, CHCC, CHCO, CHBC, CMP
JoAnn Von Plinsky, MS, RHIA

Linda Whaley, RN, CPC, CPC-H
Margaret Williams, AM

Article citation:
AHIMA e-HIM Work Group: Guidelines for EHR Documentation Practice. "Guidelines for EHR Documentation to Prevent Fraud" *Journal of AHIMA* 78, no.1 (January 2007): 65-68.