Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 update)

Save to myBoK

Editor's note: This update replaces the 2007 practice brief "Guidelines for EHR Documentation to Prevent Fraud."

Electronic documentation tools offer many features that are designed to increase both the quality and the utility of clinical documentation, enhancing communication between all healthcare providers. These features address traditional well-known requirements for documentation principles while supporting expansive new technologies. Use of these features without appropriate management and guidelines, however, may create information integrity concerns such as invalid auto-population of data fields and manufactured documentation aimed to enhance expected reimbursement. Processes must be in place to ensure the documentation for the health information used in care, research, and health management is valid, accurate, complete, trustworthy, and timely.

There are a number of existing rules and regulations on documentation principles and guidelines that primarily address documentation authorship principles, auditing, and forms development in a paper health record. New guidelines are being sought by the healthcare industry that ensure and preserve documentation integrity in an age of electronic exchange and changes in the legal evidentiary requirements for electronic business and health records.

With the continued advancement of electronic health records (EHRs), there is increasing concern that a potential loss of documentation integrity could lead to compromised patient care, care coordination, and quality reporting and research as well as fraud and abuse. This practice brief provides guidance for maintaining documentation integrity while using automated EHR functions.

Ensuring Documentation Integrity

Documentation integrity involves the accuracy of the complete health record. It encompasses information governance, patient identification, authorship validation, amendments and record corrections as well as auditing the record for documentation validity when submitting reimbursement claims. EHRs have customizable documentation applications that allow the use of templates and smart phrases to assist with documentation. Unless these tools are used appropriately, however, the integrity of the data may be questioned and the information deemed inaccurate—or possibly even perceived as fraudulent activity. Established policies and procedures such as audit functions must be in place to ensure compliant billing.

Without safeguards in place, records could reflect an inaccurate picture of the patient's condition, either at admission or as it changes over time. The provider must understand the necessity of reviewing and editing all defaulted data to ensure that only patient-specific data for that visit is recorded, while all other irrelevant data pulled in by the default template is removed. For example, the automatic generation of common negative findings within a review of systems for each body area or organ system may result in a higher level of service delivered, unless the provider documents any pertinent positive results and deletes the incorrect auto-generated entries.

Appendix B, available in the online version of this practice brief in the AHIMA Body of Knowledge, illustrates examples of worst and best case scenarios observed in documentation practices for healthcare delivery. These scenarios show how the ability to copy previous entries and paste into a current entry can lead to a record where a provider may, upon signing the documentation, unwittingly attest to the accuracy and comprehensiveness of substantial amounts of duplicated or inapplicable information, as well as the incorporation of misleading or erroneous documentation. The scenarios 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.[1-4] From a billing perspective, defaulting or copying and pasting clinical information with previous existing documentation from other patient encounters in a different health record facilitates billing at a higher level of service than was actually provided.

Providers must recognize each encounter as a standalone record, and ensure the documentation within that encounter reflects the level of service actually provided and meets payer requirements for appropriate reimbursement. The integrity of this information is vital. As Michelle Dougherty, MA, RHIA, CHP, noted in her testimony to the Office of the National Coordinator for Health IT's (ONC) HIT Policy Committee, "If clinical documentation was inaccurate when used for billing or legal purposes, it was wrong when it was used by another provider, another provider at transition, a researcher, the public health authority, or quality reporting agency."[5] The documentation may need to include any health information such as labs, changes in medications, or updates to any chronic health conditions impacting an encounter that was reviewed by the provider during the visit.

Time's Ticking for Information Governance

Data quality and record integrity issues must be addressed now, before widespread deployment of health information exchange (HIE). Poor data quality will be amplified with HIE if erroneous, incomplete, redundant, or untrustworthy data and records are allowed to cascade across the healthcare system. Healthcare organizations must manage information as an asset and adopt proactive decision making and oversight through information asset management, information governance, and enterprise information management (EIM) to achieve data trustworthiness. AHIMA defines information governance as "the accountability framework and decision rights to achieve EIM. EIM is defined as the infrastructure and processes that ensure information is trustworthy and actionable."

The multitude of federal and state health information exchange initiatives are making information governance and the integrity of EHRs more challenging every day. An accurate information governance program will ensure the accountability of how information is managed and the information's integrity.

Legal Issues Surrounding EHRs

HIM professionals consistently identify the following documentation practices as problematic in EHRs. These practices contribute to data quality and information integrity issues. Risky documentation practices that create the potential for patient safety, quality of care, and compliance concerns—such as those described below—may leave an organization vulnerable to patient safety errors and medical liability.

Template Documentation Challenges

Documentation templates can play an important role in improving the efficiency of data collection, ensuring all relevant elements are collected in a structured format. However, these templates also have limitations:

- Templates may not exist for a specific problem or visit type. This issue 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.
- Atypical patients may have multiple problems or extensive interventions that must be documented in detail.
- Templates designed to meet reimbursement criteria may miss relevant clinical information. Templates may also encourage over-documentation to meet reimbursement requirements even when services are not medically necessary or are never delivered.

Cloning, Copy/Paste Practice Problems

Cloned documentation continues to be a significant problem that creates unnecessary redundancy and at times inaccurate information in the EHR. Some EHR systems are designed to facilitate cloning with such popular features as "make me the author" to assume the content of another person's entry, "demo recall" to copy forward vital signs, "copy and paste" to replicate information from a previous visit, or the use of "smart phrases"—a function that pulls in specific identical data elements. Automated insertion of previous or outdated information through EHR tools, when not modified to be patient-specific and pertinent to the visit, may raise significant quality of care and compliance concerns—creating a potential for medical liability issues.

Organizations must develop policies designed to address inappropriate use of these tools to minimize non-compliance. Common documentation risks that can result from cloning features include:

- Vital signs that never change from visit to visit
- Information "copied and pasted" from a different patient's record
- Documentation from another provider including their attestation statement

- Identical verbiage used repeatedly for all patients seen by a provider for a specific timeframe with little or no modification regardless of the nature of the presenting problem or intensity of the service; at times, such verbiage includes contradictory indications (i.e., use of pronoun "he" instead of "she," indication that patient has no pain when the documentation includes a record of pain)

Providers must recognize that every patient is unique and must ensure that the health service provided is documented distinctly from all others.

Dictation Errors without Validation

Organizations using voice recognition without a validation step in place are experiencing significant data quality problems and documentation errors. Organizations should have in place a process to ensure providers review, edit, and approve dictated information in a timely manner. Since these documents are often used and exchanged, the importance of accurate and quality documentation in EHR systems is critical.

EHRs have created tremendous changes in the provider's workflow and documentation process. Best practices for documentation that ensures quality have not been well defined for EHRs and are not well understood by providers. Innovations are needed to improve documentation tools and techniques; a back-to-the-basics focus on the importance of data accuracy and quality must take priority before widespread deployment of interoperable health information exchange occurs.

Healthcare fraud has signalled sharper focus on specific avenues for improper claims or billing, including EHRs. The Office of Inspector General's 2012 Work Plan included a focus on fraud vulnerabilities specifically presented by EHRs, making it the first work plan in which the agency explicitly named EHRs a a target for review.

Patient Identification Errors

Documentation integrity is at risk when the wrong information is documented on the wrong patient health record. Errors in patient identification can affect clinical decision making and patient safety, impact a patient's privacy and security, and result in duplicate testing and increased costs to patients, providers, and payers. Patient identification errors can grow exponentially within the EHR, personal health record, and HIE network(s) as the information proliferates.

Failure of organizations to employ front end solutions that include measures like sophisticated matching algorithms or other methods such as use of biometrics, photography, or fingerprinting can put the organizations at risk.[6] Special alerts can be designed and implemented within an EHR to avoid potential safety issues, such as when a patient blood type or allergy does not match the patient undergoing treatment.

Organizations must have a patient identity integrity program that includes performance improvement measurements that monitor the percentage of error rates and duplicate records within its electronic master patient index. Policies and procedures must ensure that key demographic data are accurate and used to link records within and across systems. Policies must address the initial point of capture as a key front end verification.

Authorship Integrity Issues

Authorship attributes the origin or creation of a particular unit of information to a specific individual or entity acting at a particular time. When there are multiple authors or contributors to a document, all signatures should be retained so that each individual's contribution is unambiguously identified.[7] Some EHR systems allow more than one individual to add text to the same progress note entry or flow sheet. If the EHR does not have functionality to enable both providers to document and sign, it may be impossible to verify the actual service provider or the amount of work performed by each provider.

Integrity of Amendments

As outlined in the AHIMA toolkit "Amendments in the Electronic Health Record," addendums, corrections, deletions, and patient amendments should be included in the record as defined by HIPAA. In order to support the integrity of the health record, EHR systems need to allow providers to make amendments, have the ability to track corrections, and identify that an original entry has been changed. The functionality to do this can be a combination of EHR applications along with policies and procedures that outline when changes need to be made, what changes can be made, who can make the changes, and how these changes will be tracked and monitored.

The original entry must be viewable, along with a date and time stamp, the name of the person making the change, and the reason(s) for the change. Without this information, 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.

The EHR functionality 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.

All users are responsible for ensuring that documentation authorship is accurately recorded in all approved uses of the available documentation tools, and for making sure that any changes or deletions made outside of routine record use are maintained in the EHR system. Appendix C, available in the AHIMA Body of Knowledge, provides guidance on steps to prevent fraud in EHR documentation.

Healthcare Fraud and Abuse

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, to the entity or to some other party."[8] The intentional fabrication of medical records in order to improve reimbursement may be considered fraudulent. This fabrication could result from overuse of "copy and paste" functionalities or misuse of templates originally designed for documentation efficiency.

Healthcare abuse describes incidents or practices which are not usually fraudulent but are not consistent with accepted medical or business practices that may result in unnecessary costs to payers. These unintentional practices may involve repeated billing and coding errors that over time may be considered fraudulent if patterns of continued practice are found upon external review.

When misrepresentation occurs—whether it is intentional or unintentional—the staff member that has responsibility for ensuring an accurate claim has the obligation to proactively identify and prevent fraud. All providers involved in the patient's care must be held accountable to ensure the integrity of the documentation is compliant with existing law and that the level of service reported meets all payer billing, coding, and documentation requirements. According to the Medicare Claims Processing Manual, "Medical necessity is the overarching criterion for reimbursement… and the volume of documentation should not be the primary influence upon which a specific level of service is billed."[9]

Audit Integrity

Audits are essential to ensuring that the health record documentation present supports the level of service reported, that all payer requirements for reimbursement are met, and that only authorized users are accessing or making entries to patient medical records.

Audit trails must include the name of the user, the application triggering the audit, the workstation, the specific document, a description of the event being audited (i.e., amendment, correction, or deletion), and the date and time. The audit trail must capture what is amended (including deletions) within the health record and provide auditors with a starting point for compliance audits.

EHRs that lack adequate audit trail functionality create uncertainty in the integrity of health record documentation, and may create legal liability for the organization while inadvertently making or protecting criminal activity. There may also be no way to determine if and when corrections or amendments were made to the documentation, who made the changes, or the nature of the changes. In addition to the normal unintentional errors that may occur in documentation, audit trail functionality can help to detect situations where an alteration of records is meant to prevent the discovery of damaging information.

Organizations may utilize the audit trail functionality of the EHR system to identify and trend utilization of health records. The functionality typically allows users to generate reports for a specified time frame by provider or provider type, with the results sent directly to a compliance committee or the organization's governing body.

Compliance Education

Organizations may need to devote more strategy to ensure providers are well-informed about compliance and legal risks. This starts in the EHR training process. Organizations may need to develop initiatives in EHR education to make sure they do not risk compliance problems.

Staff education on best practices for documentation should focus on the integrity of the health record. The education program must be monitored, maintained, and offered quarterly or annually. Answering questions of who, what, why, and how will help to ensure individuals have a solid understanding of the organizational practices and measures that maintain individual best practices. Education geared toward understanding who, what, why, and how must include:

- The definition of who (entities or individuals) could commit fraud
- Both universal and organizational best practices with regards to security and log-in, validity of data, authorship/authentication, use and storage of data, and data transmittals
- The importance of continual education
- Strategies for applying fraud prevention best practices on a daily basis

Recommendations for Maintaining Integrity

Organizations should have policies and procedures in place that prevent fraud as a result of deliberate falsification of information. At minimum, organizations should consider these four primary conditions:

- Desire and commitment to conduct business and provide care in an ethical manner
- Purchasing systems that include functions and capabilities to prevent or discourage fraudulent activity
- Implementing and using policies, procedures, and system functions and capabilities to prevent fraud
- Inclusion of an HIM professional such as a record content expert on the IT design and EHR implementation team to ensure the end product is compliant with all billing, coding, documentation, regulatory, and payer guidelines

Ensuring documentation integrity in the record is a fundamental practice. Organizations should use the guidelines and checklists in Appendices C and D to assess their compliance. These appendices contain:

- Steps organizations can take to prevent falsification of EHRs
- Guidelines for selecting EHR system 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

Appendices

Four appendices are available in this online version of this practice brief.

Appendix A: Resource List

AHIMA. “EHRs as the Business and Legal Records of Healthcare Organizations (Updated).” (Updated November 2010).

AHIMA. “Legal Health Record Leadership Model.”

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

AHIMA EHR Practice Council. “Developing a Legal Health Record Policy.” *Journal of AHIMA* 78, no. 9 (Oct. 2007): 93–97.

AHIMA Testimony of Michelle Dougherty, MA, RHIA, CHP to the HIT Policy Committee Hearing on Clinical Documentation. Panel 4: *Role of Clinical Documentation for Legal Purposes*. February 13, 2013.

ASTM. E2017 - 99(2005) Standard Guide for Amendments to Health Information. Available online at www.astm.org/Standards/E2017.htm.

CMS Conditions of Participation for Hospitals. §482.24(c) Standard.

The Federal Rules of Civil Procedure. Last accessed 2/27/13 http://www.law.cornell.edu/rules/frcp/.

The Joint Commission. January 2013 Ambulatory Standards Manual E-dition; January 2013 Hospital Standards Manual e-Dition. Record of Care, Treatment and Services section.

President's Council of Advisors on Science and Technology (PCAST). (December, 2010) Realizing the full potential of health information technology to improve healthcare for Americans: The path forward. Accessed 2/27/13 http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

Public Law 104-191 104th Congress. *Health Insurance Portability and Accountability Act*. Accessed 2/2712 http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/HIPAALaw.pdf.

Public Law 111-5, 111th Congress. *American Recovery and Reinvestment Act of 2009*, Title XIII: Health Information Technology Section 13001. Accessed 2/27/13 http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf.

Public Law 111-148, 111th Congress. *Patient Protection and Affordable Care Act*. Accessed 2/27/13 http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf.

US Department of Health & Human Services. Office of Inspector General. Work Plan 2012. http://www.mc.vanderbilt.edu/documents/DCCI/files/OIG%20Work-Plan-2012.pdf.

Vigoda, Michael. "e-Record, e-Liability: Addressing Medico-Legal Issues in Electronic Records." *Journal of AHIMA* 79, no. 10 (Oct. 2008): 48–52.

Wiedemann, Lou Ann. "Deleting Errors in the EHR." *Journal of AHIMA* 81, no.9 (September 2010): 52-53.

Appendix B: Case Studies: Integrity of the Healthcare Record

Case Study 1

Issue: Electronic Tools That Enable Borrowing Data from another Source

Electronic tools make it easy 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. Failure to build in technical or policy and procedural safeguards creates an environment in which documentation manufacturing is encouraged and fraudulent entries are possible—thereby compromising data integrity. There also are instances in which borrowed documentation cannot be tracked to the original source, creating both legal and quality of care concerns.

The scenarios below illustrate how technology may be used effectively to achieve either positive results (illustrated in the best case example) or undesirable outcomes (illustrated in the worst case examples). Health record documentation elements can be repetitive because some conditions and situations are frequently encountered and similar processes are followed. Health interventions also follow a standard course. However, each patient is unique, making each health service distinct from all others. Documentation created for one patient or a specific visit is most often not suitable for others, and copying text entries from one record to another should be carefully controlled.

Worst Case Examples

Professional Services

While Patient A was a patient at Medical Center A, a number of medical tests and diagnostic evaluations were performed in an outpatient clinic over a two-week period. Concern arose about the health plan claim, so Patient A requested a copy of his medical records along with the bill for services. The statement included evaluation and management codes consistently reported at the highest level of service (level 5).

Because Patient A is a retired auditor for health plans, he examined the documentation and discovered that the medical history was pulled through within departments, between departments, and in subsequent visits with the same provider using the electronic health record (EHR) system, even when the visits did not include the clinician taking a history. The health plan was billed for a high level of service (of history) for each hospital outpatient clinic visit.

Patient A is concerned that the EHR does not have the functionality (or it is not used) to show that the history (or any documentation component) obtained during a previous encounter was copied and reused as documentation for subsequent visits to support physician intensity of service. After many attempts to have services billed at the correct level (what Patient A insists is really a level 2 or 3 evaluation and management when the pulled through data are not considered for service intensity), he contacts the fraud division of the health plan about his concerns.

Academic Medical Center and Physician Services

Patient B was admitted to Medical Center A for a workup to determine the cause of hypertensive episodes. She has undergone mitral valve replacement with a porcine graft and also requires a pacemaker to regulate and stabilize her heart rate.

The physician progress notes in a hospital-based EHR were copied and pasted multiple times by the attending physicians, consulting physicians, and residents by using a convenient macro feature available in the software. The teaching physicians regularly copy and paste the residents' notes as their own, which saves time in a very busy environment and covers the Medicare requirement of teaching physicians personally performing services for reimbursement.

A new resident misdiagnosed adrenal insufficiency and recorded the incorrect diagnosis in Patient B's record. Because of the normal routine for borrowing documentation from other sources, the physicians copied and pasted this documentation and relied on the erroneous assessment several times, resulting in an increased level of evaluation and management services complexity for the Medicare claim and at the same time creating a patient safety and quality of care issue. Ultimately, Patient B died from a medication error after administration of steroids to treat the adrenal insufficiency the patient didn't have, and the case is now in litigation.

Behavioral Health Services

Across the street at Mental Health Center A, a state department of health surveyor identified Nurse A repeatedly documenting the same text on progress notes completed for several patients on her caseload. Nurse A explained that when completing notes for patients receiving medication management services, she always copied and pasted entries between patient records. She stated that medication dosage was an exception most of the time because they are more variable. Nurse A used this shortcut for documentation as one way to get her charting completed in the EHR before the end of her shift.

The state surveyor calls this pattern of documentation "cookie cutting." This practice involves copying and pasting the same text from one record to another, neglecting to document the variations accurately from one patient to another. For example, the patient's response to the medication may be different, regimen compliance may be different, and request for follow-up date and time may also be different. This practice by Nurse A and other nurses from Mental Health Center A resulted in a large focused review conducted by the Medicaid Fraud Division along with fines and penalties for payment for care that was not rendered at the level of service claimed.

Best Case Example

Both the hospital and clinic associated with Medical Center A use an EHR system. The EHR has specific patient safety and documentation integrity tools built into its design. Memorial provides orientation to all medical students and residents providing patient care services on how to use the tools for accurate and complete documentation. Because it is very important that only those services personally provided or supervised by teaching physicians generate a bill for services, the computer-generated templates guide all of the participants in patient care to the correct place and format for recording observations within the record. These entries always include a date/time stamp and the author of the note. Teaching physicians must sign on to the system so the appropriate authentication is attached to their chart entries, and any templates must be modified to reflect specific conditions and observations unique to the service. Teaching physicians must be physically present to report services for health plan claims. Medical necessity and intensity of service documentation are unique to each visit, so when EHR templates and macros are not modified, they are clearly identified both by a different screen color and by a watermark across the text saying “Unmodified Documentation Template.” Info buttons provide the documentation guidelines and reporting requirements for teaching physicians and are available at the click of a mouse. Alerts are generated when a copy or paste function is used warning the EHR user about plagiarism and the risk of copying documentation out of context in a legal document.

Medical Center A also created a full slate of documentation guidelines, policies, and procedures surrounding use of the EHRs and related tools for capturing information. Special emphasis was placed on the prohibition of pulling forward information from previous visits as a basis for increasing the level of evaluation and management for billing. There are now clear protocols about the completion of an entry or record—when information displays (or not) to users and when the record gets locked down for either pulling forward or copying text content to another location. Situations and examples are provided that describe the appropriate use of pulled forward and copied entries taken from other sources. Policies about the use of scribes or surrogates making entries in an EHR are created and monitored for compliance. All designated scribes or surrogates have the ability to create entries but require countersignature authorization from the supervising clinician before they display to other users of the EHR system.

Mental Health Center A also started a clinical documentation improvement program that included appropriate use of nursing documentation templates suitable for recording medication management. These templates create the framework for required documentation unique to each patient. They include built-in edits to ensure correct recording of dosages by comparing nurse entries with the issuing pharmacy instructions and the original scripts.

Discussion Questions:

1. Which of the guidelines included in appendix C of the January 2007 AHIMA e-HIM practice brief “Guidelines for EHR Documentation to Prevent Fraud” could be used to discourage evaluation and management upcoding because of the pull-forward or copy-and-paste habits of the physicians on staff at Medical Center A?
2. What other adverse effects may result from the cookie-cutter approach used at Mental Health Center A?
3. There are times when pulling forward of entries from previous visits into current records is appropriate. What are some examples of this practice in electronic environments that is a fully legitimate and desirable method for documentation?

Case Study 2

Issue: Data Integrity

A wide spectrum of data is collected in healthcare and must be collected accurately, completely, and consistently. Data integrity is of extreme importance because it is used to identify and track patients as they move from one level of care to another. Data are used to verify the identity of an individual to ensure that the correct patient is receiving the appropriate care and to support billing activity. According to Johns in *Health Information Management Technology: An Applied Approach*, (2nd edition, page 851) “Data integrity means that data should be complete, accurate, consistent and up-to-date. Ensuring the integrity of healthcare data is important because providers use them in making decisions about patient care.”

The scenarios below are examples of worst case and best case examples associated with data integrity. Because of the large amount of data collected in healthcare, data integrity can be compromised repeatedly. Information can be entered incorrectly or in incorrect formats in various healthcare settings, so procedures must be defined to ensure that data are collected consistently regardless of the medium being used.

Worst Case Examples

Clinical Notes with Difficulty in Date Association

A patient was seen by a clinician on September 1, 2013, just before lunch. Once the patient was examined, the clinician got sidetracked and was not able to enter his note on the date the patient was seen. During the visit, the patient discussed a possible reaction to a prescribed medication. On September 5, 2013, the clinician was back on duty after a long weekend; upon review of the record, he realized that he did not make an entry on September 1, 2013.

As the clinician began documenting, he decided that he wanted the date to reflect the actual date the patient was seen. He changed the date to September 1, 2013, at 11:30 a.m. He proceeded to enter the documentation as best he could. He remembered and documented the symptoms the patient described surrounding the potential medication reaction.

When another clinician reviewed the record, he saw the new note. This second clinician worked over the weekend and did not recall seeing this information but sees now that the date displayed is September 1, 2013, at 11:30 a.m. This alarmed the clinician, as he prescribed the medication that the patient had indicated a possible reaction to in the past.

Note and Event Entries—Date/Time Stamp

A facility has multiple biomedical peripherals connected to the EHR such as portable ECGs and intravenous infusion pumps. The main system has a synchronized clock for display with date and time stamping on notes, laboratory results, etc. Performance measures established by the Joint Commission on Accreditation of Healthcare Organizations, ORYX, and the Centers for Medicare and Medicaid Services (CMS) are monitored, tracked, and reported. Some payments are tied to quality of service. Indicators for chest pain include requiring that the ECG be performed within 10 minutes of arrival in the emergency room.

A patient is brought to the emergency room at 23:55 on September 1, 2013. An ECG is started and completed according to orders entered at 23:57 on September 1, 2013. The ECG is uploaded, read, and interpreted. At 00:30 on September 2, 2013, the clinician completes her documentation of the assessment and orders admission for acute myocardial infarction.

After a retrospective review of the case, the ECG is reported as being ordered at 23:57 but not completed until September 2, 2013, at 00:45. This is 15 minutes after the note entered by the clinician stating the ECG was done and showed ST-elevation myocardial infarction. Not only has this case fallen out for performance measures but it will also have difficulty standing up in court. It could possibly fail a third-party review if the outpatient was treated and released because the chest pain was thought to be gastrointestinal in nature. An audit might determine the ECG was not a covered service if done after the time of discharge.

In addition, the facility might not receive proper credit (or in the reverse if the clock times show it was done on time, but it really wasn't) and either receive wrongful payment or no payment when reimbursement is based on quality indicators. The linkage of peripherals needs to have the clocks on each system synchronized to support the integrity of the data collected for the care provided.

Touch Pads in Long-Term Care

Nursing Care Facility A implemented an EHR to streamline documentation so that the resident assessment instrument (RAI) is integrated with the assessment process/protocol (RAP) and the Minimum Data Set (MDS). A special feature of the software ensures optimal reimbursement for skilled beds through a point-of-care system that prompts nursing personnel to enter data elements.

The nurses and nursing assistants enjoy the convenience of the touch pad technology and the time the new system saves them for charting. However, the director of nursing has discovered that the system is creating documentation inconsistent with actual patient conditions. The MDS being transmitted to CMS is overstating the type of care for therapy units and suppressing one of the reportable quality indicators (residents with pain). The documentation in the records supports the optimized payment from Medicare for the skilled-care patients, but the director of nursing is very concerned about the consequences of using it.

Best Case Examples and Solutions

Clinical Notes with Difficulty in Date Association

Text entries into the EHR have a hard-coded date/time stamp that cannot be altered by the author. However, the clinician making a late entry can associate the date of the visit/service by using a second date/time field option, which allows for dates of reference for both a late entry and the date the care was provided. The ability to make amendments to the EHR is defined by business rules and policy. Entry errors are defined and reported accordingly.

Documentation Tools in a Teaching Hospital

University Hospital A uses an EHR for both the hospital and the clinic. The EHR has specific patient safety and documentation integrity tools built into the design. University Hospital A provides an orientation to all medical students and residents on how to use the documentation tools so the information collected is always accurate and complete.

It is very important that only those services personally provided or supervised by teaching physicians generate a bill for services. The computer-generated templates guide all users to the correct place and format to record observations, including a date/time stamp and the author of the note. Teaching physicians must sign on to the system so the appropriate authentication is attached to their chart entries, and any templates must be modified to reflect specific conditions and observations unique to the service. Teaching physicians must be physically present to report services for health plan claims. Medical necessity and intensity of service documentation are unique to each visit.

The templates and macros in the EHR not modified are clearly identified both by a different screen color and by a watermark across the text that says "Unmodified Documentation Template." Info buttons providing documentation guidelines and reporting requirements for teaching physicians are available to the physicians at the click of a mouse. Alerts are generated when a copy or paste function is used to warn the end user about plagiarism and the risk of copying documentation out of context in a legal document.

The authority for developing templates and implementing documentation content and formats is spelled out in policy (bylaws) and is done through collaboration of EHR and HIM/medical record committees at the facility.

Clinical Notes with Difficulty in Date Association

The date that a note is entered into the EHR is hard coded. However, clinicians have the ability to associate the note with a date of service to reflect a reference date of when they saw patients as well as an indication of a late entry. Both of these dates are important to best practices in HIM.

Note and Event Entries—Date/Time Stamp

The facility made a conscious effort to ensure a standard for date and time stamps. To accomplish this goal, the facility inventoried all interfaced applications and biomedical equipment. Each equipment vendor was contacted to determine the best method of synchronizing peripherals to the main system, which minimized or eliminated users having to keep track of the time themselves. However, some equipment may need to be checked at the beginning of shifts or at 00:01 as the staff do with crash carts, etc.

Touch Pads in Long-Term Care (Best Case)

Nursing Care Center A implemented an EHR to streamline documentation so that the RAI is integrated with the RAP and the MDS. A special feature of the software ensures optimal reimbursement for skilled beds through a point-of-care system that prompts all personnel to enter data elements. Each section of the MDS requires various personnel to provide coded data supported by their patient-specific documentation in the EHR.

Clinical, nonclinical, and medical staff have all found the convenience of the touch pad technology to be a time savings for both charting and completing their portion of the MDS. The software for collecting the MDS data has built-in hierarchy for the user (physician or nurse assistant) and for most data elements. For example, any activities of daily living (ADLs) or sleep patterns checked off by a nurse assistant would be accepted, but if a physician or nurse documented items relative to ADLs during the same MDS reporting period, a pop-up window would ask, "Section X has information already entered for ADLs; do you want to proceed?" This prompt allows the nurse or physician to proceed or to double-check what the nurse assistant previously recorded.

Orders in EHR

The orders section in an EHR can be a large database. Prescriptions must have specific fields associated with them to identify the details of the individual order—which physician placed the order; the date, time, reason, or diagnosis associated with the medication; status, etc.

Diagnosis on Note Different Than Final Diagnosis Coded and Billed

The provider may document a diagnosis that attaches itself to a template note. The coder may decide from the physician's documentation that the diagnosis should be coded more specifically. Thus, the diagnosis in the EHR template note might be different than what was coded and billed.

Discussion Questions:

1. What procedures can be established to ensure that medication reactions described by a patient are documented in an accurate and timely manner to prevent medication errors and negative medication reactions?
2. When dealing with disparate systems, what time-safe rules can be established to prevent staff from being able to enter data after a subsequent visit has been documented without systematic alerts to notify specific end users of a late entry or a change in documentation?
3. What steps can an agency take to develop an electronic process to perform thorough data quality audits at specified time intervals?
4. In a teaching facility, what documentation guidelines can be established to ensure that documentation completed by residents and interns is countersigned by tenured medical staff to prevent inconsistent documentation and billing discrepancies that can lead to fraudulent billing activities?

Application of Guidelines:

These case studies have been prepared along with guidelines to provide further references. See guidelines 1-3.

Case Study 3

Issue: Patient Identification and Demographic Data: Automated Patient Registration Data Elements/Patient Safety Risks

Failure of an EHR system to provide appropriate safeguards against medication errors, including the wrong patient, the wrong drug, or failure to consider all available data, can contribute to poor quality care. Examples of automated patient registration data elements and patient safety issues illustrate the need for identity management safeguards.

Worst Case Example

Dr. Rogers is ordering a prescription by using electronic order entry for a nursing home resident in the geriatric outpatient clinic at City Hospital A on October 15. The patient with dementia presents to the clinic with a nursing assistant from Nursing Care Facility A, she is registered as Ethel Mertz, and her health records are placed in queue for Dr. Rogers.

Nursing Care Facility A had been contacted the previous day to gather information for the appointment. The registration clerk from the hospital asked only for the patient's name then used the lookup feature in the EHR system to locate existing health records and place them in Dr. Roger's authorized access list for the upcoming appointment. The City Hospital A system automatically populates registration data and places patient records in an authorized access queue for scheduled patients in the clinics on the day of the visit.

The nurse has downloaded a printout from the EHR system for Dr. Rogers to use in the examination room while caring for the patient, but he doesn't see that the Ethel Mertz in the record is 27 years old and has an address in another city. It's easy to locate Ethel's record in the system by typing in the first three numbers of her Social Security number (also stamped on the fee ticket) used to bill Medicaid for services. The clinic staff has already verified that Ethel is eligible for Medicaid.

The physician order entry software provides the capability for default self-selection upon entering the first three letters of the drug. The physician wanted to order Norfloxacin for an eye infection. As soon as "Nor" was entered, the software prompted for Norflex, which was accepted. The prescription/medication order was received in the pharmacy and was filled for Norflex, which is a muscle relaxant rather than an antibiotic. Both are oral medications, although muscle tightening or spasms could result from Norflex. The order was signed electronically, the medication was made available for the nursing assistant to pick up, and the patient was returned to the nursing facility.

The patient with an infection requiring treatment with Norfloxacin began taking Norflex and returned to the emergency room later the same week with septic shock due to a very serious bacterial infection of the left eye. When the emergency room staff accessed her health record, there was no entry for a geriatric clinic visit on October 15, so the findings from her care were not available.

City Hospital A filed a Medicaid claim for Ethel Mertz and was paid for a clinic visit on October 15 with pharmacy charges for a Norflex prescription. Unfortunately, the Nursing Care Facility A patient's name is Ethel Merts, age 93. She has a number of chronic health problems, takes a number of medications, and has an allergy to drugs containing quinolone.

Best Case Examples

City Hospital A uses a certified EHR system with built-in safeguards in the computerized physician order entry (CPOE) software suite to prevent medication errors.

- This system does not allow software to self-select (or default) the first alphabetical choice in the order process and requires a second validation to make sure the drug indicated is the intended substance and dose.
- This system provides the user the opportunity to finish typing before any suggestions are made by the software.
- The software provides a list of options (or drop-down menus) to the user to select from and then provides alerts or reminders from a knowledge base.
- City Hospital A does not allow use of abbreviations in ordering; the full name of the drug is always displayed to avoid any errors between similar medications.
- The system also provides a warning message at the time of signature for contraindications and potential adverse effects.

During the ordering process used at City Hospital A's outpatient clinic, Mrs. Merts's physician is asked by the EHR system to verify selection of Norfloxacin because the current medication history indicates that the patient had an anaphylactic reaction to another antibacterial agent that includes quinolone. The physician selects another type of antibiotic that is equally effective and avoids the risk of an adverse reaction.

Patient Identity Management

A nursing home resident presents to the City Hospital A geriatric clinic with *Staphylococcus aureus* conjunctivitis. The nursing home had arranged the appointment with Dr. Rogers by using an online registration portal that requires verification of five critical demographic data elements to establish patient identity. Because there are two patients with similar names at Nursing Facility A, the home is careful to make sure that this patient, Mrs. Ethel Merts, is registered with her physician Dr. Rogers. Her current medication list, problem list, and allergies are uploaded to the system from the nursing home EHR. The EHR at City Hospital A sends a verification message of receipt, and Dr. Rogers has a printout of the nursing home records at the time of the examination. At any time when verification is required, Dr. Rogers is able to access the full EHR including the uploaded information provided by the nursing home.

Discussion Questions:

1. What safeguards should be built into procedures to verify patient identity?
2. What process would be used to correct the entries made incorrectly on the record of Ethel Mertz (age 27)?
3. What steps are needed to resolve the Medicaid claims issue generated on the basis of false information for Ethel Mertz?
4. What business process steps should be taken to prevent erroneous entries in a CPOE system?

Appendix C: Steps to Prevent Fraud in EHR Documentation

The following guidelines provide recommendations for organizations to reduce the likelihood of fraud when EHRs are being used.

Establish Organizational Policies

An organization communicates its ethics and commitment to complying with laws and regulations through its policies. Organization-wide policies that should be established to reduce the likelihood of fraud include the following:

- Stating the organization's commitment to complying with all laws and regulatory requirements and to operating in an ethical manner
- Prohibiting the entry of false information into any of the organization's records
- Defining individual responsibility and accountability for the accuracy and integrity of information and establishing a notification process consistent with language in the medical staff bylaws or rules and regulations when errors are discovered.
- Specifying consequences for the falsification of information.
- Requiring periodic training covering the falsification of information and information security.
- Defining management-level responsibility for the organization's information security program.

Organizations should also establish EHR- and HIM-related policies:

- Specifying administrative documentation requirements.
- Specifying clinical documentation requirements.
- Requiring the logging of activity on EHR systems.
- Covering changes (i.e., corrections and amendments) to records.
- Establishing timeframes for correcting information once the incorrect documentation is discovered.

This is a list of highly recommended policies and is not meant to be exhaustive. Organizations implementing an EHR may need to develop additional policies according to their needs.

Fraud Prevention Education Programs

Education programs need to address the different functionality of an electronic versus a paper environment specifically for individuals who have previously worked in a paper health record environment. EHR users more than likely will continue to use paper records along with the EHR, so distinctions regarding the unique fraud risks of the EHR must be conveyed. In the paper environment, data are usually static, and alterations or changes to documents are more readily apparent. In the EHR, alterations can more easily go undetected, and errors can grow exponentially. EHR fraud prevention education programs should address:

Training Requirements

- **Annual education and training:** The organization is responsible for ensuring that EHR users receive regularly scheduled education and training on the organization's policies and procedures for maintaining EHR integrity, including security and log in, validity of data, authorship/authentication, use and storage of data, and data transmittals. This training should be updated annually and can be incorporated as a separate focus area into the organization's compliance and HIPAA training.
- **Documentation of education activity:** Education programs are to be documented and become a part of the physician, provider, or employee's permanent medical staff or human resource record. In the event of any possible future issues regarding false or fraudulent entries, the organization will be able to demonstrate that due diligence was exercised in the training of its staff.
- **Mandatory requirement:** All users must complete the education program.
- **Documentation guidelines:** The education program needs to clarify and reinforce that the HIM documentation requirements and documentation guidelines accepted and established for the paper record also apply to the EHR. In addition, all regulatory and oversight agency requirements for documentation, such as for the Centers for Medicare and Medicaid Services (CMS), The Joint Commission (TJC), the Accreditation Association for Ambulatory Health Care (AAAHC), and the American Osteopathic Association (AOA) apply to the EHR as well.

Security and Integrity Requirements

- **Personal responsibility for protecting system access:** All EHR users must protect their log-in or sign-in from unauthorized access. The user is prohibited from sharing individual security information with others and must report breaches of log-in or sign-in security immediately. EHR users must secure their desktops and laptops or other data access devices whenever they are away from them. Time-out screens, shut-offs and other security measures should be taken.
- **Personal responsibility for notifying management of actual or suspected problems:** EHR users are not to hesitate in notifying management of problems even if a problem is only suspected and cannot be confirmed by the EHR user. These problems may be security breaches, suspicious activity, uncharacteristic data entries, unauthorized access, data entry errors that the user is unable to correct, amendments to data that are not in line with the organization's policies and procedures for amendments, or any other activity not in accordance with the organization's policies and procedures.
- **Personal responsibility for creating accurate records:** It is particularly important to verify the patient record selected on an EHR because, unlike the paper record, once the patient is selected, the EHR screen flows may not alert the user to the patient's identification. Furthermore, the paper record is three-dimensional and has many labels and visual prompts at the fingertips, whereas patient identification on an EHR may not be prominently displayed. Education should be directed to training EHR users to verify routinely a minimum of two or three unique patient identifiers such as name, date of birth, and account number.

The EHR users are responsible for each element of data they enter into the record and must provide electronic verification of authorship/authentication, which includes data that have been copied and pasted or pulled forward from other parts of the patient's record or from sources outside of the patient's record. Each entry that is not solely authored by the user must be validated by the user in a manner similar to that for bibliographic notations and include the name, date, time, and source of the data. This requirement can be satisfied by system software design that routinely provides this validation. Compliance with these elements will ensure that the requirements for regulatory agencies and payers will be met.

- **Logging, time stamping, and fraud-prevention software:** The education sessions should explain that routine security programs are run on a regular basis and reviewed for unusual or invalid activity. As a deterrent to fraudulent activity, if the organization uses fraud prevention software, a general explanation of its purpose could be discussed.

Violations of EHR Policies and Procedures

Educational programs need to address clearly the organization's disciplinary and termination policies governing falsification of records, security and access breaches, or violations. The education program should also refer to the organization's policy for HIPAA and note should be made that EHR security is in line with protection and security of health information. Further reference should be made to various federal and state legislation and the requirements of various oversight agencies:

- Federal False Claims Act
- HIPAA
- Deficit Reduction Act of 2005
- Department of Health and Human Services Office of Inspector General (OIG) Guidance for Hospitals and Physicians
- CMS Conditions of Participation
- TJC Accreditation Requirements
- AOA Accreditation Requirements
- AAAHC Accreditation Requirements
- Medical Staff Bylaws of the Organization
- DNV Accreditation Agency

Note: the program and content outlined above are recommended as a starting point for organizations. Modifications and additions should be made as appropriate to meet organizational needs.

Establishing a Process for Logging and Auditing Activity in EHR Systems

An audit trail is a business record of all transactions and activities, including access, that are associated with the EHR. Monitoring audit trails in your system will ensure that users can be held accountable for following the organization's policies and procedures, adhering to compliance rules and regulations, and following HIM protocols for access and maintenance.

Facilities using electronic health information systems need to ensure that individuals entering information into the EHR are aware that system audit trail functionality is in place allowing them to legally access, amend, retract, correct, or edit entries that were made during the normal course of business, at or near the time the care.

Determine Which Logging Features Should Be Used and Determine System Logging Capabilities

- The system should be able to generate an audit record when auditable events happen, including but not limited to the following (which include success, attempt, and failure):
  - User login/logouts
  - Chart created, viewed, updated, or deleted
  - System security administration
  - System start and stop
  - Scheduling
  - Query
  - Order
  - Node-authentication failure
  - Signature created or validated
  - Personal health information (PHI) export (e.g., print)
  - PHI import (e.g., from external information source)
  - System administration
- The system should record within each audit record the following information when it is available:
  - Date and time of the event.
  - Component of the information system (e.g., software component, hardware component) where the event occurred.
  - Type of event (including data description and patient identifier when relevant).
  - Subject identity (e.g., user identity).
  - Outcome (success or failure) of the event.
- The system should provide authorized administrators with the capability to read all audit information from audit records in one of the following two ways:
  - The system should provide the audit records in a manner suitable for the user to interpret the information. The system should provide the capability to generate reports on the basis of ranges of system date and time that audit records were collected.
  - The system should be able to export logs into text format and correlate records on the basis of time (e.g., universal coordinated time [UTC] synchronization).
- The system should be able to provide time synchronization by using an industry standard format and use this synchronized time in all security records of time.
- The system should record time stamps by using UTC on the basis of ISO 8601-2000 (i.e., “1994-11-05T08:15:30-05:00” corresponds to November 5, 1994, 8:15 a.m., US Eastern Standard Time).
- The system should prohibit all users read access to the audit records, except users who have been granted explicit read-access. The system should protect the stored audit records from unauthorized deletion. The system should be able to prevent modifications to the audit records.
- The system should continue normal operation even when the security audit functionality is nonfunctional. For example, if the audit log reaches capacity, the system should continue to operate; issue a warning to system administrators; and suspend logging, start a new log, or begin overwriting the existing log.

Note: This section is adapted from the Certification Commission for Healthcare Information Technology Test Scripts for 2006 Certification of Ambulatory EHRs, Version 1.0, May 2006 at http://www.cchit.org/work/criteria.htm.

Assign Responsibility for Auditing of Log Entries and Reported Exceptions

- Leadership and management are ultimately responsible for developing policies and procedures that spell out and assign responsibility to professional and ancillary leadership staff to determine system functionality, system security, and system usability as well as report any system inefficiencies or discrepancies potentially resulting in fraudulent entries into the EHR.
- Leadership and management should always adhere to legal and regulatory standards and follow ethical business principles when auditing the system for integrity and trustworthiness of the data.
- The system should allow an authorized administrator to set the inclusion or exclusion of audited events on the basis of organizational policy and operating requirements and limits.

Define Retention Periods and Procedures for Log Records

- The system should generate a backup copy of the application data, security credentials, and log and audit files.
- The system restore functionality should result in a fully operational and secure state, which should include the restoration of the application data, security credentials, and log and audit files to their previous state.
- If the system claims to be available 24/7, it should have the ability to run a backup concurrently with the operation of the application.
- The audit report must include a copy of the output of the audit as well as the steps taken to produce the report.
- Retention of audit logs is based on state and/or federal laws, whichever applies to the organization. Please see AHIMA practice briefs “Update: Maintaining a Legally Sound Health Record—Paper and Electronic” from November-December 2005 and “New Electronic Discovery Civil Rule” from September 2006.

Areas Recommended for Monitoring or Auditing for Detecting Alleged Fraud and Abuse Related to EHR Documentation

There are reasons other than documentation and fraud and abuse concerns that would encourage monitoring and auditing. Each organization must determine which monitors and audits are appropriate to address the requirements of applicable laws, regulations, needs, and available resources. Each organization is also responsible for specifying the method for determining whether the activity is legitimate or suspect and any necessary consequences such as.

- Abnormal patterns of activity:
    - Spike in the number of people accessing a particular record or document.
    - Sudden variation in the magnitude or types of changes made in a record.
    - Unusual repetition of particular entries in a record.
    - Entries or other transactions occurring at unusual times of the day or days of the week.
- Routine documentation monitoring:
    - Review of problem lists and medication lists against prior lists for consistency.
    - Audit providers’ orders for medications and ancillary services to determine if a provider properly documented the reason(s)/diagnosis(es) for the test(s)/medication(s) ordered.
    - Audit to determine whether transcription/dictation reports are downloaded to and appear in the correct patient and correct visit date fields.
- Routine coding monitoring and auditing:
- Monitoring the computerized assignment of codes according to applicable coding system guidelines.
    - Ensuring the documentation supports the code assigned.
    - Noting unusual changes in the frequency of use of certain types of codes, etc.
- Auditing of EHR access and documentation to ensure users are authorized according to privileges and business rules.
- System-generated warning messages related to attempted unauthorized access.
- Monitor software upgrades and system changes to verify that security settings, user privilege settings, and logging parameters were not disabled or modified as a result of the upgrade or change.

Possible Techniques for Auditing or Monitoring:

- Standard sampling techniques backed by rigorous claims audits involving external validation procedures.
- Use test vignettes to evaluate the legal record for amendments, attestation, authorship, integrity, and nonrepudiation.

System Audit Trails:

The HIPAA Title II security rule CFR Part 136.316(b)(1) (taken from the March 26, 2013, Federal Register) is the source for this paragraph. It mandates audit trails be maintained within the EHR. Internal audit processes must be in place, and regular system activity reviews must be completed for logins and accessing files. Security incidents must be monitored and resolved. Keep in mind that logging and auditing processes may affect the performance of a system, and an organization may need to purchase additional hardware, memory upgrades, and/or bandwidth to support these audit requirements. Audit data must continuously be reviewed and analyzed, processes that may also require additional resources.

Sample Business Rules for EHR Systems

Establishing business rules is very similar to the process historically occurring in the medical record committee, and in medical staff bylaws, rules and regulations. Business rules implement these processes and designate who can document what in the record and how the documents are to be handled.

This business rule presented here should not be considered a complete business rule, nor does it represent all of the business rules needed for an EHR system. Business rules are specific to an organization and its EHR system configuration.

Business rules authorize specific users or groups of users to perform specified actions on documents in particular statuses.

- A completed clinical document can be viewed by a user.
- An unsigned clinical document can be edited by a provider who is also the expected signer of the note.
- An unsigned clinical document can be deleted by the appropriately authorized personnel.

Business rules apply to document definition, user class, or user role. You can then add, edit, or delete rules, as appropriate.

Document Definition:

Advance Directive	Title
Advance Directive	Document Class
Adverse Reaction/Allergy	Title
Adverse Reaction/Allergy	Document Class
Clinical Documents	Class
Clinical Warning	Title
Clinical Warning	Document Class

List Business Rules by Document for Clinical Documents:

- An untranscribed clinical document may be entered by a user.

- An unreleased clinical document may be released by a transcriber.
- An unsigned clinical document may be edited by an author/dictator.
- An unsigned clinical document may be edited by an expected signer.
- An unsigned clinical document may be signed by an expected signer.
- An unsigned clinical document may be signed by a provider who is also an expected cosigner.
- An unreleased clinical document may be edited by a transcriber.
- An uncosigned clinical document may be cosigned by an expected cosigner.
- An unsigned clinical document may be signed by a student who is also an expected signer.
- An unsigned clinical document may be edited by an expected cosigner.
- An untranscribed clinical document may be entered by a nurse.
- An uncosigned clinical document may be sent back by a provider who is also an expected cosigner.
- An amended nurse’s note may be edited by a nurse or an author/dictator.
- An amended nurse’s note may be edited by a nursing supervisor or an author/dictator.

Status of Business Rules: Actions Permitted for a Given Document Definition and Status:

Amended

> The document has been completed, and a HIPAA issue has required its amendment.

Completed

> The document has acquired all necessary signatures and is legally authenticated.

Deleted

> The document has been deleted but the audit trail is retained.

Incomplete

> This status applies to document definitions only.

Purged

> The grace period for purge has expired and the report text has been removed from the online record to recover disk space. Note: only completed documents can be purged. The chart copy of the document should be retained for archival purposes.

Uncosigned

> The document is complete, with the exception of co-signature by the attending physician.

Undictated

> The document is required and a record has been created in anticipation of dictation and transcription, but the system hasn’t been informed of its dictation.

Unreleased

> The document is in the process of being entered into the system but hasn’t been released by the originator (i.e., the person who entered the text online).

Unsigned

> The document is online in a draft state, but the author’s signature hasn’t yet been obtained.

Untranscribed

> The document is required, and the system has been informed of its dictation, but the transcription hasn’t yet been entered or uploaded.

Unverified

> The document has been released or uploaded, but an intervening verification step must be completed before the document is displayed.

Business rules are complex, and there are additional rules for inheritance of business rules, inheritance along the document definition line, overriding business rule inheritance, inheritance along the user class line, and inheritance and addenda, etc.

Selecting EHR System Features to Prevent Fraud

Organizations should consider selecting EHR systems with the following capabilities:

Access Control:

Verifying authorship hinges on two concepts: authentication and access management. In the simplest terms, identity and access management can be defined as an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control their users' access to critical electronic applications and resources while protecting confidential personal and business information from unauthorized users. Authentication and access management can be executed either through the EHR software, or it can be controlled through a separate, or layered, software application.

- **User authentication:**
  Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. The purpose of authentication is to show authorship and assign responsibility for an act, event, condition, opinion, or diagnosis. Entries in the healthcare record should be authenticated by the author.[1] The method of authentication should be considered in selecting an EHR system.
  - Three basic elements can be used for authentication:
    - Something the user is such as some form of biometric identifier (e.g., fingerprint or retinal pattern, DNA sequence voice pattern, signature recognition).
    - Something the user has such as an identification card, security token, or software token.
    - Something the user knows such as a password or a personal identification number (PIN).
  - If biometric authentication is not available, then a dual-element authentication should be considered as a reasonable control policy.

Extensive privilege assignment and control features:

Access management, also known as authorization, is the process of verifying that a known person has the authority to perform a certain operation. Verification of the identity of a user or other entity is a prerequisite to allowing access to information systems.[2] When an organization selects an EHR system, the organization should be able to control access through role-based descriptors and individual identification and the ability to configure multiple access management levels.

Logging of All Activity:

The ability of the organization to maintain a legal medical record in the electronic environment is a paramount consideration in the selection and use of an EHR system. The EHR must have the ability to record all activity that occurs within the system. (See Section B.) A good EHR system must include a robust and complete logging and auditing function.

Data Entry Editing:

- **Verify validity of information on entry when possible:**
  The ability of the system to either warn or not allow impossible information, such as a hysterectomy CPT code for a male patient or a prostate examination for a female. These systems can be more sophisticated to not allow or at least prompt or warn the user of less likely events or occurrences, including using billing codes that do not meet the medical necessity criteria for payers.

- **Check for duplication and conflicts:**
  The system that will not allow duplication of patient identification numbers or codes and one that will warn of conflicting medical management options, such as life-threatening drug interactions may be useful. The ability of a system's prompt capability should be thoroughly explored by the clinical users because there is emerging evidence of a phenomenon known as "prompt fatigue." A system without the ability to control the prompt occurrence can lead to lack of use or even misuse by the providers entering information.
- **Control and limit automatic creation of information:**
  The ability to create documentation automatically, whether through a copy-and-paste or pull-forward function, selection of generic documentation, or use of "auto-neg" or other documentation by exception functions should be avoided. In most circumstances, such features should be disabled. These features, although they are time-savers, are dangerous to the organization and the individual practitioner because they foster the ability to commit fraud, intentionally or unintentionally. They are also a source of "dirty data" that will compromise good patient care and data-mining capabilities.
- **Monitor corrections and additions to the medical record:**
  Corrections, amendments, clarifications, and additions to a medical record are a normal part of clinical documentation. These changes to the EHR should always be made available to the user of the record unless such changes are detrimental (e.g., incorrect information was originally recorded about the patient). The EHR should have the ability to handle these events easily and thoroughly, and of most importance, properly, as outlined in CMS guidelines; federal, state, and local laws; and hospital bylaws and accreditation standards.

These features are not intended to be a complete list of necessary or desired EHR system capabilities. Their inclusion in an EHR system will assist in preventing the potential for falsifying documentation in the patient record.

Appendix D: Electronic Health Record Integrity Checklist

EHR System Name: _______________

EHR Integrity Assessment	**Yes**	**No**	**N/A**	**Comments**
1. Does the organization communicate its ethics and commitment to complying with laws and regulations through its policies?				
A. The organization has policies and procedures that indicate the organization's intent to comply with all laws and regulatory requirements and to operate in an ethical manner.				
B. The organization has policies and procedures that define and prohibit the entry of false information into any of the organization's records.				
C. The organization has policies and procedures that define individual responsibility and accountability for the accuracy and integrity of information and for notifying management of errors which are discovered.				
D. The organization has policies and procedures that define specific consequences for the falsification of information.				

E. The organization has policies and procedures that define mandatory periodic training covering the falsification of information and information security.				
F. The organization has policies and procedures that define management level responsibility for the organization's information security program.				
2. Does the organization establish EHR and HIM related policies?				
A. The organization has policies and procedures that specify administrative documentation requirements.				
B. The organization has policies and procedures that specify clinical documentation requirements				
C. The organization has policies and procedures that define required logging of activity on EHR systems.				
D. The organization has policies and procedures that define how changes, i.e., corrections and amendments, are made to all records.				
3. Does the organization establish and maintain an education program? The education program must be designed to communicate the organization's policies, the individual's responsibilities, and the capabilities and functions of the EHR system to each individual who works with electronic health records.				
4. Does the EHR education program meet the following objectives?				
A. The organization has procedures that will inform all individuals associated with the organization of the organization's policies.				
B. The organization has policies and procedures that explain staff responsibilities for maintaining the integrity and accuracy of information.				
i. The organization has policies that define personal responsibilities for protecting system access information.				
ii. The organization has policies that define personal responsibility for the creating accurate records.				

iii. The organization has policies and procedures that define staff responsibility to notify management of problems which are discovered.				
C. The organization has policies and procedures that cover the proper use and features and functions of the EHR system.				
D. The organization has policies and procedures that address methods for preventing erroneous entry of information and the importance or preventing errors.				
E. The organization has policies and procedures that define penalties for falsifying any organizational records.				
F. The organization has policies and procedures to provide instruction on how to use the system security features for preventing unauthorized access to systems.				
G. The organization has policies and procedures that inform all EHR users that their activities are being logged by the system.				
H. The organization has policies and procedures that address software design and other techniques that may be used to cause system users to enter false information.				
EHR System Features				
1. Organizations utilize existing HL7 RM-ES standards to review the EHR functions for record integrity				
A. Minimum metadata set for record lifecycle events;				
B. Authentication, authorization and access controls;				
C. Attestation and non-repudiation;				
D. Alteration, amendment and correction;				
E. Health record output – quality, accuracy, usability and rendering of the official record of care				
F. Patient identity validation				

2. Does the EHR system provide access control functions?				
A. The organization has policies and procedures that define the management of user authentication.				
B. The organization has policies and procedures that define the management of extensive privilege assignment and control features.				
3. Does the EHR system have the capability to attribute the entry, modification, or deletion of information to a specific individual or subsystem?				
4. Does the EHR system have the capability to log all activity (refer to the section on Logging of Activity on EHR Systems for specific logging requirements)?				
5. Does the EHR system have the capability to use a common date and time stamp across all components of the system?				
6. Does the EHR system have data entry editing capabilities?				
A. The organization has policies and procedures to validate information on entry when possible.				
B. The organization has policies and procedures to check for duplication and conflicts.				
C. The organization has policies and procedures to control and limited automatic creation of information.				
EHR Implementation				
1. Organization has an HIM professional on the IT design and implementation TEAM to ensure end product is compliant with all regulatory and payer billing, coding and documentation requirements.				
2. Does the EHR system establish a process for logging of all activity on EHR systems?				
A. The organization has policies that determine which logging features should be used.				

B. The organization has procedures in place to enable system logging.				
C. The organization has procedures that assign responsibility for auditing of log entries and reported exceptions.				
D. The organization has policies that define retention periods and procedures for log records.				
E. The organization has defined policies relating to system performance issues.				
3. Does the EHR system define and implement the business rules relevant to the responsibility of each functional role and each type of information?				
4. Does the EHR system preserve data produced in response to a specific request, or can it be re-created reliably?				

Notes

1. Helbig, Susan. “Copying and Pasting in the EHR-S: An HIM Perspective.” 2004 IFHRO Congress and AHIMA Convention Proceedings. October 2004. Available in the HIM Body of Knowledge,www.ahima.org.
2. 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.
3. Hammond, Kenric W. et al. “Are Electronic Medical Records Trustworthy? Observations on Copying, Pasting and Duplication.” AMIA Annual Symposium Proceedings, 2003: 269–273.
4. Embi, Peter J. et al. “Impacts of Computerized Provider Documentation in a Teaching Hospital: Perceptions of Faculty and Resident Providers.” *Journal of the American Medical Informatics Association* 11, no. 4 (2004): 300–309.
5. AHIMA Testimony of Michelle Dougherty to the HIT Policy Committee Hearing on Clinical Documentation. Panel 4: Role of Clinical Documentation for Legal Purposes. February 13, 2013.
6. National Health Care Anti-Fraud Association. “What is health care fraud?” 2012.
7. HIMSS. “Patient Identity Integrity.” December 2009.
8. President’s Council of Advisors on Science and Technology. “Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward.” Report to the President of the United States of America, December 2010.
9. Centers for Medicare and Medicaid Services. Medicare Claims Processing Manual, Chapter 12. 2013.

Reference

AHIMA. “Information Governance.” 2013.

Prepared By

Kim Baldwin-Stried Reich, MBA, MJ, RHIA, FAHIMA, PBCI, CPHQ
Ann Botros, PhD, RHIA
Kristen Denney, MA, RHIA
Julie Dooling, RHIA
Lisa Fink, MBA, RHIA, CPHQ
Deshawna Hill, RHIA, HIT Pro-CP

Sandra Huyck, RHIT, CCS-P, CPC, CPC-H
Renii Modisette, MHA, RHIT, CCS
Mona Nabers, MBA, RHIA
Diane Premeau, MBA, RHIA, RHIT, CHP, CHC
Laura Rizzo, MHA, RHIA
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, CDIP, FAHIMA, CPEHR

Acknowledgements

Cecilia Backman, MBA, RHIA, CPHQ
Karen Fabrizio, RHIA
Barry S. Herrin, JD, CHPS, FACHE
Sandra L. Joe, MJ, RHIA
Theresa Jones, MSEd, RHIA
Patti Kritzberger, RHIT, CHPA
Katherine Lusk, MHSM, RHIA
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA
Amy Richardson, RHIA
Gail Woytek, RHIA

Original Authors

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

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA Work Group. "Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 update)" *Journal of AHIMA* 84, no.8 (August 2013): 58-62 [extended web version].