Practice Brief: Ensuring the Integrity of the EHR

Editor's Note: This Practice Brief supersedes the August 2013 "Integrity of the Healthcare Record: Best Practices for EHR Documentation" and the May 2015 "Assessing and Improving EHR Data Quality" Practice Briefs.

Nearly 20 years have passed since the landmark release of the Institute of Medicine's (IOM) report *To Err is Human: Building a Safer Health System.* This report estimated the number of people dying in hospitals yearly due to preventable errors to be at least 44,000. John James, in the September 2013 Journal of Patient Safety, estimated that there were between 210,000 and 440,000 preventable hospital deaths a year.[1]

The goal of the electronic health record (EHR) is to help healthcare professionals produce and use quality data for evidence-based knowledge management and decision-making for patient care. The EHR has the potential to minimize medical errors if the data are accurate and meet quality criteria. EHRs are comprised of many different technologies. EHR governance by means of clear policies, standards, procedures, and functionalities should be established for all systems and applications that interface with the EHR, and define who owns and has responsibility for maintaining and creating the data dictionary for each system and module.

Poor documentation, inaccurate data, and insufficient communication can result in errors and adverse incidents.[2] Inaccurate data threatens patient safety and can lead to increased costs, inefficiencies, and poor financial performance. Furthermore, inaccurate or insufficient data impedes reimbursement, payments, strategic planning, and health information exchange (HIE), as well as hinders clinical research, performance improvement, and quality measurement initiatives. The impact of poor data on patient care has increased with the implementation of ICD-10-CM/PCS, the Promoting Interoperability Program (previously known as the "meaningful use" EHR Incentive Program), accountable care organizations, and value-based purchasing.

With the continued advancement of EHRs there is increasing concern that poor documentation integrity could lead to compromised patient care, care coordination, quality reporting, payment errors, and research, as well as fraud and abuse. Providers and suppliers must rely on proper documentation to justify the validity of coded services when claims are rejected. As the predictive analytic capabilities of third-party payers evolve, the documentation within the medical record projects a greater focus on the integrity of data that supports billing functions and revenue generation. This Practice Brief discusses the challenges of maintaining quality data in the EHR and offers best practice guidance for ensuring the integrity of healthcare data.

Capturing Data at the Point of Care

The quality of clinical documentation at the point of entry is critical for all secondary uses of the data. EHR quality is dependent upon the data collected at the point of registration and follows through with each participant in the patient's care. Clinical documentation practices need to be developed and standardized to facilitate data quality, accurate data capture, and encoding while reflecting the individuality of each patient. In an EHR, it is imperative these content standards are built into the foundation of the data capture tools.

After building content standards into documentation tools, the next critical step is training. The frontline clinical and administrative staff members who are creating entries in the EHR need guidance to understand the data standards and definitions to make choices that accurately reflect the patient's circumstances. Without understanding the importance and meaning of data standards through appropriate training, data integrity will be lost. An example of a content standard is the Health Level Seven (HL7) Reference Information Model (RIM), which is a visual representation of clinical content as discrete objects and data elements that can be generated, shared, and used in a lifecycle of events between participants.[3]

Establishing consistent data models will ensure the integrity and quality of the data maintained in the EHR. A data model is a representation of the data to be stored in a database and the relationships between the tables and data fields which can then be carried out using object-oriented or entity relationship approaches.[4]

AHIMA's Data Quality Management Model, available online in AHIMA's HIM Body of Knowledge, discusses the business processes that ensure the integrity of an organization's data throughout the information lifecycle, from collection, application, and warehousing to analysis.

Ensuring Data Accuracy

Quality patient care and safety improvement goals can be enhanced and better achieved through the application of documentation guidelines and data standards. Documentation and data content within an EHR must be accurate, complete, concise, consistent, timely, and universally understood by data users. It must also support the legal business record of the organization by maintaining these parameters. It is critical that both structured and unstructured data meet a standard of quality if they are to be meaningful for internal and external use, such as continuum of care and secondary purposes. Factors such as ease of use and design can facilitate adherence to documentation guidelines and standards, as discussed in the Practice Brief titled "Fundamentals of the Legal Health Record and Designated Record Set."

Documentation policies and guidelines for both paper and electronic documentation must be established in compliance with governmental, regulatory, accreditation, and industry standards, including those for accuracy, timeliness, copy functionality, and privacy and security. Organizational EHR governance managing the use of best practice alerts and hard stops is recommended to ensure accurate and complete documentation, while limiting overuse to avoid alert fatigue and delays in patient care. Strong facility controls and governance can help ensure documentation guidelines are followed and compliance requirements are met. For example, consider the varying use of abbreviations and acronyms across facilities and states. If an abbreviation is used incorrectly or is not understood by the reader and then acted upon, it could have a negative impact on the treatment of the patient.

Data integrity policies and procedures must be created and followed. These policies may include, but are not limited to, registration processes, standards for handling duplicate records, and processes for addressing overlays (writing over one person's demographic information with another person's information). It is important to implement policies and procedures to maintain the integrity of the data throughout the patient encounter for all information entered into the EHR, whether by people or other electronic systems. Individuals dedicated to the continuous auditing of the medical record, as well as automated processes that monitor the EHR system proactively and identify errors as they are created, play an important role in fine-tuning processes and ensuring the overall quality of the data. Alerts may be built into the EHR to identify potential errors and bring these to the attention of the provider, others treating the patient, or staff who monitor the record for data integrity issues.

Data Quality Best Practices

To realize the advantages of the implementation of health information technology and HIE in the combined goals of improving quality of care and ensuring the financial integrity of the organization, best practices for ensuring quality healthcare data become the foundation.

Some key factors that must be considered for best practices to support data quality include:

- Security of access
- Data dictionaries (metadata)
- Standards of terminology
- Policy and procedures
- Information governance

Security of information—or access to create, use, and amend data—begins with role-based access that is defined and enforced with administrative safeguards. Clear policies that define information access by a specific role or relationship to patient type limits authority to enter, access, update, and delete data along with the means to audit such activities. A regulatory stipulation of the Health Insurance Portability and Accountability Act (HIPAA) defines the limitation of access to patient information with the minimum necessary rule, which states that staff should only have access to the information they need to do their job. Technology can assist with access control, but there still needs to be coordination with individual stakeholders and processes to ensure accuracy and availability of the data for patient care.

Standards of terminology support consistency in data collection. The data dictionary ensures the consistent use of data elements and terminology to improve the use of data and storage within a database management system. Data definitions should be clearly communicated to all staff accessing the record, especially those responsible for reporting data. The data dictionary can also be built into various information systems to promote data consistency throughout the enterprise. Information governance requires ongoing ownership and maintenance of the data dictionary.

The development and distribution of standards of terminology, including clinical vocabularies, classification code sets, and nomenclatures, facilitates interoperability for the exchange of clinical data and to improve the retrieval of health information from data storage. Barriers to interoperability and data quality result when there are inconsistent naming conventions, definitions, varying field length for the same data element, and/or varied element values, which can all lead to problems such as poor data quality and misuse of data in reporting. For example, the date of a patient's admission may be referred to as the "date of admission" in one system and "admit date" in another.

HIM Role in Enterprise Information Management

The traditional role of the HIM professional as the legal custodian of health records in terms of organization, content, maintenance, and authorized release has taken on new dimension with the advent of electronic health records and the movement toward more comprehensive information governance approaches.

As data strategies incorporating data quality assurance to ensure optimal data quality become necessary, the HIM professional's role expands to include data governance. The importance of managing information as an asset means HIM professionals would like to see their roles evolve to have an enterprise-wide presence that encompasses such duties as helping to bridge data gaps for clinical documentation and supporting operational information demands.

Data quality should be a constant focus for HIM professionals. As the custodian of the health record, the HIM professional is tasked with authenticating and certifying the legal health record for legal issues. Compliance with billing requirements necessitates a medical record that supports the claims submitted. Clinical documentation improvement supports the accurate representation of a patient's clinical status translated into coded data which advances to such secondary uses as quality reporting, physician report cards, reimbursement, research, public health data, and disease tracking and trending.

Healthcare organizations must manage information as an asset and adopt proactive decision-making and oversight. This can be achieved through information asset management, information governance, and enterprise information management (EIM) to achieve data trustworthiness. AHIMA defines information governance as "an organization-wide framework for managing information throughout its lifecycle and for supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."[5] AHIMA further defines EIM as "a subdomain of information governance that includes the policies and processes for managing information across the organization, throughout all phases of its life: creation and capture, processing, use, storing, preservation, and disposition. It also includes management of enterprise practices for information sharing, release and exchange practices, chain of custody, and long-term digital preservation."[6] The multitude of federal and state health information exchange initiatives require information governance and the integrity of EHRs to support confidence in record sharing.

Key Areas of Awareness for Effective Use of EHR Systems

To fully leverage the potential of an EHR system to improve data quality—as well as to understand the potential limitations a system might have—it is imperative that HIM professionals have a broad understanding of EHR functionality in addition to a thorough understanding of the specific EHR system in use at their organization. Data strategies and an effective data quality program that incorporate data integrity processes must be in place to ensure optimal data quality. In addition to having an information governance program and executive sponsorship, consideration should be given to the following areas:

1. Patient Identification

Documentation integrity and patient safety are at risk when information is accessed and documented in the wrong patient's record. Therefore, it is essential to ensure that the patient is registered under the correct name so that health information is associated with the patient to whom it pertains from the beginning. EHR systems should have alerts and prompts that notify the user when the potential for an incorrect association exists. For example, the registration system and the EHR system should alert users when several patients have similar names and dates of birth, such as in the case of multiple same-birth siblings. Access controls strictly limiting who can enter and update or change key demographic elements, such as name or date of birth, must also be in place. Errors in patient identification can affect clinical decision-making, impact a patient's privacy and security, and result in duplicate testing and increased costs. Errors can grow exponentially within the EHR, spreading to patient portals, as well as to health information exchange networks. Matching demographic information supplied by the patient to what is in the registration system and/or EHR may not be sufficient. Additional identifiers or use of biometrics, such as patient photographs, palm vein scanning, or fingerprinting should be utilized, when possible, to ensure more accurate patient matching.

Standardized documentation should also be considered when verifying the identity of the patients, such as a government-issued ID, and not the patient's insurance card. In addition, standardized naming convention policies or formats for using the patient's legal name must also be developed and employed (i.e., standardizing the spelling of suffixes, such as "Jr." versus "Junior" versus "JR") to help minimize the risk for error. Policies and procedures for baby naming, for unidentified emergency patients, for the use and exclusions of hyphens, and for handling celebrities or notable individuals should also be developed, including consideration of complications that could arise through use of alias names. Policies should also be developed regarding how name changes are made and how the previous name is stored, such as in the case of previously unidentified patients. In addition, policies need to be developed addressing gender changes.

Thorough training for all front-end users—especially those in registration and scheduling roles—and proactive monitoring for potential patient identification errors should be given the utmost attention to ensure proper patient identification. For more information on patient

identification and patient matching, refer to the Practice Brief "Managing the Integrity of Patient Identity in Health Information Exchange", available online in AHIMA's HIM Body of Knowledge, or the white paper "Patient Matching in Health Information Exchanges", published in Perspectives in Health Information Management.

It is also important for those who are treating the patient and documenting in the EHR to ensure that the correct patient and correct encounter is selected before documentation is started. This may be done by verifying the patient's name. When information is documented either on the wrong patient or even the correct patient but the wrong encounter, it is necessary for the documentation to be corrected. If the documentation cannot be moved to the correct medical record it may be necessary to mark it as documentation in error in the wrong record and have the documentation recreated or scanned into the correct medical record. Since such errors can create harm to the patient if not caught, it is imperative that steps are taken to avoid creating these types of mistakes.

2. Templated Documentation Tools

Standardization of data definitions and structure for clinical content may include the use of smart text or text expanders (macros) and limit the use of free text when possible. These approaches will allow for a more robust analysis and utilization of the database tools and resources that make up these systems. The organization should also create standardized paper and electronic forms and templates. Standardization will guide documentation and provide a standard for patient care, which can result in better treatment outcomes.

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 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 integrity of data used in care, research, and health management is authentic, valid, accurate, complete, trustworthy, and timely.

Practices such as repurposing data from the primary source may create redundancies throughout a patient's health record. Redundancies can cause navigation difficulty such as trying to find essential components like a specific date or time. EHR design and development should focus on "modular and reusable documentation components" which can improve efficiency, eliminate duplicative documentation, and "reduce the effort" required to write and capture meaningful, useful, and pertinent documentation.[7]

For example, templates and scripts that are designed to contain a mixture of free-text fields and dynamic system data (i.e., blood pressure results or a lab value) promote patient and encounter individuality. These templates and scripts also discourage the copying of an entire narrative note repeatedly from day to day into the narrative section of an EHR, since the system data would become outdated and irrelevant.[8] An organization committed to data quality will observe how documentation tools are being utilized in their environment. Inefficient tools will lead to end users creating work-arounds that will degrade data integrity. Using those observations to improve data capture tools and to provide ongoing staff training will help an organization achieve optimal data integrity.

3. Copy Functionality

In early 2014, the Department of Health and Human Services' Office of Inspector General highlighted copy and paste as a common EHR documentation practice, noting that it can lead to the input of false or irrelevant documentation.[9] Since bringing this to light, many EHR vendors have started evaluating and addressing copy/paste functionality. Copy functionality may also be known as "copy/paste," "copy forward," or "cloning." The importance of strong information governance and internal policies and procedures regarding the use of this type of functionality is critical. Organizational policies and procedures should be developed for proper use of EHR documentation to ensure compliance with governmental, regulatory, and industry standards, including acceptable copy/paste practices. Such practices include identification of origin, date, and author of copied information, provider responsibility for copied information, error notification, and sanctions for violating copy/paste policies.[10]

Use of copy functionality has been promoted in the clinician's EHR workflow to improve the ease of consistent use of static health information, such as past medical history. However, when misused, copy functionality can lead to redundant, misleading, inaccurate, irrelevant, inconsistent, and/or unnecessarily lengthy documentation that may jeopardize quality of care, increase risk for medical error, or result in allegations or even charges of fraud. For example, problems are likely to occur when a clinician copies and pastes progress notes from the patient's first day of care to the second, third, and further subsequent days of care without taking the time to review and edit procedures, medication, treatments administered, and/or documents pertaining to a particular date of service. In addition to the impact on quality of patient care, dangers extend to the audit arena, where retrospective case reviews may focus on the high frequency of copy/paste use, which can indicate possible fraud. Organizational polices should address corrections to copy/paste content when an addendum or amendment is made.

The ability to limit copy functionality in an EHR system is vital for the accuracy of data. Limitations of copy functionality should include measures such as:

- Clearly labeling the information as copied from another source
- Limiting the ability for data to be copied and pasted from other systems
- Limiting the ability of one author to copy from another author's documentation
- Limiting the ability to copy data from another unique patient
- Allowing a provider to mark specific results as reviewed
- Allowing only key predefined elements of reports and results to be copied or imported
- Monitoring a clinician's use of copy and paste
- Monitoring the EHR audit trail when copy and paste is used

More information on policies and procedures related to copy functionality is available in the Copy Functionality Toolkit (2016 update) in AHIMA's HIM Body of Knowledge.

4. Corrections and Amendments

Policies must outline who may amend or correct the medical record, when record amendments can be made, and how medical records may be amended. The organization should also have policies related to requests by the patient to amend the medical record, which is covered under HIPAA regulations. An organization should develop specific guidelines that outline what HIM or other staff may amend/correct versus what must be sent back to the author for correction, as well as how to process a request for amendment when the author is no longer employed by the organization or not reachable when the data needs to be corrected immediately. For example, HIM staff may be allowed to change demographic data such as a date of birth upon verification, but all clinical amendment requests must be sent back to the author for updates.

Any amendment to the content of the health record must be approved by the author of the entry, and previous versions should be accessible through a revision history or audit process. Since information in the medical record may flow to other systems such as patient portals and health information exchanges, the organization should have processes to ensure that amendments/corrections have been made to those systems as well. More information on policies and procedures related to corrections and/or deletions is available in AHIMA's "Amendments in the Electronic Health Record Toolkit", available online in AHIMA's HIM Body of Knowledge.

5. Standalone Devices

Whenever possible, patient treatment information from standalone devices (radiation therapy systems, diagnostic cardiac testing systems, etc.) should be incorporated into the EHR through a direct interface or cold feed. However, certain devices or equipment that contain health data might not interface with the EHR. In those cases, the information can be scanned into the EHR or, when appropriate, a summary of results can be entered into text fields. The lack of availability of health information contained in standalone devices can potentially impact data quality by restricting certain types of data from view or making the viewing of data difficult. In such cases, it is important to assess what standalone data is not integrated into a single EHR view and ensure those who have a need to know such information can access it. This may also be true of information that existed in prior EHR systems but was not migrated to the current EHR.

Organizations must closely monitor standalone systems to ensure data quality and accuracy between the EHR and the standalone system. For example, scanning results into a document imaging system for viewing, or possibly embedding a link from the EHR directly to the standalone system, may be necessary to ensure that all the data is available when needed. Having information in disparate systems with no link or viewing ability could lead to patient safety concerns.

6. Legacy Systems

Legacy systems must be carefully evaluated before undergoing a data transmission or migration to the EHR. Many organizations have legacy systems that contain patient information or that feed information into the current EHR. Testing of data migration with validation needs to occur in a test environment before migration should occur. Prior to retiring a legacy system, a thorough assessment of stored data must be undertaken and a data mapping plan to migrate required data elements must be developed. A legacy system may also feed data to an EHR or be retired by converting data into an EHR to eliminate system redundancy. An organization should follow its retention guidelines for medical records for the legacy system. If all the medical record information is migrated to another system or storage method, the legacy system could then be retired and the new storage method would then be subject to the retention guidelines. Tools must be maintained to allow users to view/read the information from the legacy system throughout the retention period.

When an error in data is discovered, the error should be corrected in the source system, when possible, as well as in any systems that contain the erroneous data, such as a data warehouse that feeds other information systems in the enterprise. Clear policies and procedures for determining the source of truth when differences exist between interfaced and integrated systems is critical. This includes any legacy systems that have not been evaluated, cleansed, and converted.

7. Hybrid Health Record

The move toward a more integrated EHR may occur in stages due to the cost and significant impact a "big bang" implementation can have on an organization. This may create inconsistent methods for documentation, with some health information residing in the EHR and some remaining on paper. Providers and clinical staff locating documentation for patient care or staff performing data review, data abstraction, and coding of services also face inconsistency in finding pertinent information. In such cases, a concise training plan must be established to clearly communicate and manage the data while in a hybrid state. A record matrix may also be established to keep track of the dates that certain aspects of documentation moved from paper to an electronic state, from being interfaced to being documented directly in the EHR, or conversion from one system to another system.

In addition, the hybrid record can also foster the use of "shadow charts," charts that are created to contain copies of clinical information for use within a clinical site, where the primary source for original documentation is maintained in the primary health record. Shadow charts can lead to the misfiling of original documentation, leading to an incomplete primary health record. Organizational policy should provide clear guidance as to the approved use or elimination of shadow charts.

8. Problem List

The problem list is a comprehensive list of the patient's current, previous, and resolved medical conditions. It can facilitate continuation of care between patient encounters and between providers and others involved in the treatment of the patient. To ensure that the problem list is accurate, an organization should have a clear policy and guidance regulating the structure of the problem list as well as its use. The policy should include who can document in the problem list and who can add/resolve or inactivate documentation on the problem list. Guidance should also include timeliness of original and updated documentation on the problem list, which should be made as changes to the patient's diagnoses and treatment occur. It is important to note that information from the problem list may carry over to other documentation and systems, such as patient portals and health information exchanges, so accuracy and integrity is of the utmost importance. See the "Problem List Guidance in the EHR" Practice Brief, located online in AHIMA's HIM Body of Knowledge, for more information.

9. Disaster Recovery/Business Continuity

Organizations often experience both scheduled and unscheduled downtime with an EHR system. Therefore, policies and procedures should be in place to guide users on documentation during this time. Testing of downtime procedures should occur on a regular basis. For business continuity, testing downtime procedures after system upgrades should occur as well. Many organizations have a view-only backup system in place in which the documentation for the most recent period is available (i.e., last 30 minutes or two hours of care prior to downtime). During downtime an organization must decide if users will move to paper documentation (depending on length of downtime). If paper documentation is used, then it must also be decided what information will be recovered electronically once the system is back up and what may be scanned into the EHR, depending on how long the EHR system was on downtime.

Training is the Foundation for a Culture of Quality Data

The quality and integrity of the data element cannot be established and maintained without a human element, so an effective and continuous training program becomes the driving force in achieving a culture of data stewardship and compliance throughout the organization.

For health information systems, a comprehensive training program can provide the necessary skills for the workforce in achieving the work goals and objectives of the organization. Having sufficient test cases available in a system is key so all aspects of job requirements can be used in a test environment. Testing and training should not occur in a production environment. For the workforce, effective training provides the employee with the knowledge and tools in performing task completion according to established policy. For the organization, training and human resource development—aligned with the strategic plan—benefit the organization by ensuring maintenance of a workforce possessing the skills for current and future organizational needs.

Achieving an effective training program requires planning to assess training needs through analysis. Once the assessment is completed, the next step is to develop a plan with training materials and mode of delivery, then test the effectiveness of the plan, implement the training activities, monitor the effectiveness, and, finally, revise as needed.[11]

Opportunities for EHR Policy Training

The timing of training is an additional important factor to consider. Training for use of an EHR and its component devices and software is a multifaceted process, starting with new employee orientation. This instruction sets the foundation by introducing the employee to the basics of the administrative, physical, and technical safeguards in place in the organization and the expectations of the employee related to information use and governance.

Departmental orientation for new employees requires a focus on the role-based tasks, along with specific policies and procedures for compliance with those tasks as well as associated responsibilities related to computer system access and other equipment within the department. For staff development training, organizations may need to devote more strategy to ensure providers and staff are well-informed about compliance and legal risks. 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, The Joint Commission, the Accreditation Association for Ambulatory Health Care, the American Osteopathic Association, and Det Norske Veritas GL Health apply to the electronic record as well. Periodic staff education, through in-service and continuing education programs that focus on best practices for documentation to support the integrity of the health record, provide an opportunity to reinforce established policy and introduce regulatory and guideline changes that necessitate new policies and procedures.

Documentation of the education activity as part of the physician, provider, or employee's permanent medical staff or human resource record verifies the employee participation and establishes accountability for following organizational policy. 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.

Maintaining EHR Integrity

To ensure a high level of integrity of the EHR, organizations should consider:

- Implementation of a formalized, organization-wide information governance program
- 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 EHR integrity is a fundamental practice. Organizations should use the guidelines within this Practice Brief as well as the detailed checklist in Appendix A, available online in AHIMA's HIM Body of Knowledge at http://bok.ahima.org to assess compliance.

HIM's Evolving Role

The role of the HIM professional is evolving from managing the content of the health record to managing overall EHR data standardization and harmonization, both within the organization and with external organizations through health information exchanges. The new role of the HIM professional will involve leadership in the development of information and/or data governance programs, EHR quality models within the organization, and an expansion of auditing and monitoring programs. Audit programs will help identify points throughout the data collection process that are at risk. HIM professionals can contribute positively to all these efforts through their understanding of the processes underlying the clinical and financial data streams that comprise the EHR. Many HIM professionals will continue to find a natural migration to leadership roles in technology departments or vendor environments to share their knowledge from another perspective.

HIM professionals have always worked to ensure data in the health record meets quality standards for accuracy, timeliness, consistency, and completeness. The ability to use these skills reinforces the importance of HIM engagement in auditing and monitoring documentation practices contributing to critical EHR design decisions, as well as discussions surrounding data collection, data management, and data analysis and reporting. Information governance programs, along with HIM stewardship, ensure the use and management of health information is compliant with jurisdictional law, regulations, standards, and organizational policies. As stewards of health information, HIM roles and functions strive to protect and ensure the ethical use of health information.[12] The migration of healthcare records from paper to electronic puts HIM professionals in a unique position to lead efforts to evaluate and improve EHR data, which will be central to the acceptance of the EHR and the migration to a future state with new technologies and interoperability.

Appendices

Two appendices are available at the end of this Practice Brief:

- Appendix A: EHR Integrity Checklist
- Appendix B: Case Scenarios

Notes

1. James, John T. "A New, Evidence-based Estimate of Patient Harms Associated with Hospital Care." *Journal of Patient Safety* 9, no. 3 (September 2013): 122-128. http://journals.lww.com/journalpatientsafety/Fulltext/2013/09000/A_New,_Evidence_based_Estimate_of_Patient_Harms.2.aspx.
2. Kohn, Linda T. et al. *To Err Is Human: Building a Safer Health System.* Committee on Quality of Health Care in America, Institute of Medicine. National Academies Press, 2000.
3. Orlova, Anna. "Overview of Health IT Standards." *Journal of AHIMA* 86, no. 3 (March 2015): 38-40. http://bok.ahima.org/doc?oid=107579.
4. White, Susan. *A Practical Approach to Analyzing Healthcare Data*, Second Edition. Chicago, IL: AHIMA Press, 2013.
5. Empel, Sofia. "Way Forward: AHIMA Develops Information Governance Principles to Lead Healthcare Toward Better Data Management." *Journal of AHIMA* 85, no. 10 (October 2014): 30-32. http://bok.ahima.org/doc?oid=107468.
6. AHIMA. *Pocket Glossary of Health Information Management and Technology*, Fifth Edition. Chicago, IL: AHIMA Press, 2017.
7. Wrenn, Jesse O. et al. "Quantifying Clinical Narrative Redundancy in an Electronic Health Record." *Journal of the American Medical Informatics Association* 17, no. 1 (January/February 2010): 49-53. www.ncbi.nlm.nih.gov/pubmed/20064801.
8. Hahn, Jin et al. "Rapid Implementation of Inpatient Electronic Physician Documentation at an Academic Hospital." *Applied Clinical Informatics* 3, no. 2 (2012): 175-185. www.ncbi.nlm.nih.gov/pmc/articles/PMC3613016/.
9. McCann, Erin. "CMS Called Out for EHR Fraud Failings." *Healthcare IT News*. January 9, 2014. www.healthcareitnews.com/news/cms-called-out-ehr-fraud-failings?topic=08,28,29.
10. Office of the National Coordinator for Health Information Technology. CMS-ONC Listening Session on Coding and Billing. May 3, 2013.
11. Oachs, Pamela K. and Amy Watters. *Health Information Management: Concepts, Principles, and Practice*, Fifth Edition. Chicago, IL: AHIMA Press, 2016: pp. 752–753.
12. Dimick, Chris. "Health Information Management 2025: Current 'Health IT Revolution' Drastically Changes HIM in the Near Future." *Journal of AHIMA* 83, no. 8 (August 2012): 24-31. http://bok.ahima.org/doc?oid=106207.

References

AHIMA. "Amendments in the Electronic Health Record Toolkit." 2012. http://bok.ahima.org/PdfView?oid=105672.

AHIMA. "Copy Functionality Toolkit (2016 update)." 2016. http://bok.ahima.org/PdfView?oid=302011.

AHIMA Work Group. "Managing the Integrity of Patient Identity in Health Information Exchange (2014 update)." *Journal of AHIMA* 85, no. 5 (May 2014): expanded web version. http://bok.ahima.org/doc?oid=300436.

AHIMA Work Group. "Problem List Guidance in the EHR." *Journal of AHIMA* 82, no. 9 (September 2011): 52-58. http://bok.ahima.org/doc?oid=104997.

Davoudi, Sion et al. "Data Quality Management Model (2015 Update)." *Journal of AHIMA* 86, no. 10 (October 2015): expanded web version. http://bok.ahima.org/doc?oid=107773.

Lusk, Katherine G. et al. "Patient Matching in Health Information Exchanges." Perspectives in Health Information Management. http://perspectives.ahima.org/patient-matching-in-health-information-exchanges/.

Williams, Adrian. "Design for Better Data: How Software and Users Interact Onscreen Matters to Data Quality." *Journal of AHIMA* 77, no. 2 (February 2006): 56-60. http://bok.ahima.org/doc?oid=62323.

Prepared By

Shamsi Berry, PhD, MS, CPHI
Angela Campbell, MSHI, RHIA
Jill Flanigan, MLS, MS, RHIT
Dawn Paulson, MJ, RHIA, CHPS, CPHI
Barbara Ryznar, RPh, MSHI, RHIA, CPHI, CPHIMS, CAPM
Jami Woebkenberg, MHIM, RHIA, CPHI, FAHIMA

Acknowledgments

Melanie Endicott, MBA/HCM, RHIA, CDIP, CHDA, CPHI, CCS, CCS-P, FAHIMA
Cheryl Ericson, MS, RN, CDIP, CCDS
Kristi Fahy, RHIA

Elisa Gorton, RHIA, CHPS, CHC
Tammy Love, RHIA, CDIP, CCS
Ann Meehan, RHIA
Mari Pire-St. Pierre, RHIA, CPHI
Donna Rugg, RHIT, CDIP, CCS-P, CCS
Clarice Smith, RHIA, CHP
Anny Yuen, RHIA, CDIP, CCS, CCDS

Additional Acknowledgments

Assessing and Improving EHR Data Quality (2015 Update)

Prepared By (2015 Update)

Sion Davoudi

Julie A. Dooling, RHIA, CHDA

Lisa Kogan, MS, MHA, CCS-P, CDIP

Kerry Ruben, RN, BSN, PHN

Kathleen E. Wall, MS, RHIA

Annemarie Wendicke, MPH

Acknowledgements (2015 Update)

Kathleen Addison, CHIM

Patricia Buttner, RHIA, CDIP, CCS

Jill S. Clark, MBA, RHIA, CHDA

Susan Clark, BS, RHIT, CHTS-PW, CHTS-IM

Katherine Downing, MA, RHIA, CHPS, PMP

Suzanne P. Drake, RHIT, CCS

Terri Eichelmann, MBA, RHIA

Elisa R. Gorton, MSHSM, RHIA, CHPS

Lesley Kadlec, MA, RHIA

Jeanne E. Mansell, RHIT, RAC-CT

Raymound Mikaelian, RHIA

Cindy C. Parman, CPC, CPC-H, RCC

Angela Rose, MHA, RHIA, CHPS, FAHIMA

Bibiana VonMalder, RHIT

Lou Ann Wiedemann, MS, RHIA, CDIP, CHDA, FAHIMA

Henri Wynne, MA, RHIT

Prepared by (Previous Update)

Jill S. Clark, MBA, RHIA, CHDA

Vicki A. Delgado, RHIT, CTR

Susan Demorsky, MHSA, RHIA, FHIMSS, CPHIMS

Elizabeth A. Dunagan, RHIA

Theresa A. Eichelmann, RHIA

Lois A. Hooper, RHIT

Grant Landsbach, RHIA

Ann M. Meehan, RHIA

Deborah L. Neville, RHIA, CCS-P

Sandra L. Nunn, MA, RHIA, CHP

Acknowledgements (Previous Update)

Cecilia Backman, MBA, RHIA, CPHQ

Gloryanne Bryant, RHIA, CCS, CDIP

Linda Darvill, RHIT

Julie A. Dooling, RHIT

Kim Dudgeon, RHIT, HIT Pro IS/TS, CMT

Sasha Goodwin, RHIA

Deborah K. Green, MBA, RHIA

Diane Hanson, RHIT

Sandra Huyck, RHIT, CCS-P, CPC, CPC-H

Theresa L. Jones, MSEd, RHIA

Stacy Jowers Dorris, MBA, RHIA, CPHQ

Sandra Kersten, MPH, RHIA

Doreen Koch, RHIT

Katherine Kremer, BA, RHIT

Ann Meehan, RHIA

Christina Merle, MS, RHIA

Monna Nabers, RHIA, MBA

Susan Parker, MEd, RHIA

Kim Baldwin-Stried Reich, MBA, MJ, PBCI

Theresa Rihanek, MHA, RHIA, CCS

Lisa Roat, RHIT, CCS, CCDS

Angela Dinh Rose, MHA, RHIA, CHPS, CDIP

1. Beth Shanholtzer, MAEd, RHIA

Sharon Slivochka

Diana Warner, MS, RHIA, CHPS, FAHIMA

Lydia Washington, MS, RHIA, CPHIMS

Traci Waugh, RHIA

Jane DeSpiegelaere-Wegner, MBA, RHIA, CCS, FAHIMA

Lou Ann Wiedemann, MS, RHIA, CDIP, CPEHR, FAHIMA

Gail Woytek, RHIA

Prepared By (Original)

Catherine Baxter Regina Dell, RHIT, CCS

Sylvia Publ, RHIA

Ranae Race, RHI

Contributors (Original)

Ashley Austin, RHIT

Stacie Durkin, MBA, RN, RHIA

Kathy Giannangelo, MA, RHIA, CCS

Pawan Goyal, MD, MHA, MS, PMP, CPHIMS

Shelly Hurst, RHIA, CCS

Karl Koob, RHIA

Karanne Lambton, CCHRA(C)

Therese McCarthy

Mary Rausch-Walter, RHIT

Kathy Schleis, RHIT, CHP

Jennifer Schunke, MS, RHIA

Sonya Stasiuk, CCHRA(C)

Dolores Stephens, MS, RHIT

Doreen Swadley, RHIA, MA, MBA, FACHE

Maggie Williams

Acknowledgments (Original)

Crystal Kallem, RHIT

Don Mon, PhD, FHIMSS

Michael Putkovich, RHIA

Rita Scichilone, MHSA, RHIA, CCS, CCS-P

Integrity of the Healthcare Record: Best Practices for EHR Documentation – 2013 Update

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, CPEHR, FAHIMA

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

Appendix A: EHR 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? The organization and policies and procedures that:				
a. Indicate the organization's intent to comply with all laws and regulatory requirements and to operate in an ethical manner.				
b. Define and prohibit the entry of false information into any of the organization's records.				
c. Define individual responsibility and accountability for the accuracy and integrity of information and for notifying management of errors which are discovered.				
d. Define specific consequences for the falsification of information.				
e. Define mandatory periodic training covering falsification of information and information security.				
f. Define management level responsibility for the organization's information security program.				
g. Define acceptable use of copy/paste or copy forward within the EHR.				
2. Does the organization establish EHR and HIM related policies? The organization and policies and procedures that:				
a. Specify administrative documentation requirements.				
b. Specify clinical documentation requirements.				
c. Define required logging of activity on EHR systems.				
d. Define how changes (i.e., corrections and amendments) are made to all records in both primary and secondary systems.				

EHR Integrity Assessment	Yes	No	N/A	Comments
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 job 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? The organization and policies and procedures that:				
a. Inform all individuals associated with the organization of the organization's policies.				
b. Explain staff responsibilities for maintaining the integrity and accuracy of information.				
i. Define personal responsibilities for protecting system access information.				
ii. Define personal responsibility for creating accurate records.				
iii. Define staff responsibility to notify management of problems which are discovered.				
c. Cover the proper use and features and functions of the EHR system.				
d. Address methods for preventing erroneous entry of information and the importance of preventing errors.				
e. Define penalties for falsifying any organizational records.				
f. Provide instruction on how to use the system security features for preventing unauthorized access to systems.				
g. Inform all EHR users that their activities are being logged by the system.				
h. Address software design and other techniques that may be used to cause system users to enter false information.				
EHR System Features				

EHR Integrity Assessment	Yes	No	N/A	Comments
1. Organizations utilize existing HL7 Records Management and Evidentiary Support (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, amendments, 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? The organization and policies and procedures that:				
a. Define the management of user authentication.				
b. 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?				
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 editing capabilities? The organization and policies and procedures that:				
a. Validate information on entry when possible.				
b. Check for duplication and conflicts.				

EHR Integrity Assessment	Yes	No	N/A	Comments
c. Control and limit automatic creation of information.				
d. Control versioning capabilities, access, and usage within the EHR.				
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 allow for a process for logging all activity on the EHR systems? The organization and policies and procedures that:				
a. Determine which EHR features for logging should be used.				
b. Enable logging using system functionality.				
c. Assign responsibility for auditing of log entries and reported exceptions.				
d. Define retention periods and procedures for log records.				
e. Relate to system performance issues.				
3. Does the EHR system allow for definition and implementation of business rules relevant to the responsibility of each functional role and each type of information?				
4. Does the EHR system allow for preservation of data produced in response to a specific request, or can it be re-created reliably?				

Appendix B: Case Scenarios

Example #1:

A 25-year-old patient came in and was registered under another patient with the same name, but a different date of birth (45 years old). It wasn't until after the patient had been discharged and the incorrect patient billed for services that the error was caught. Thinking that her identity had been stolen, the incorrect patient contacted the police who then contacted the hospital. Patient registration staff realized the issue and moved the encounter to the correct patient in the registration system, separate from the EHR. Patient registration did not follow the appropriate steps to have the record corrected, which subsequently led to information being released inappropriately as well. Once the error was identified, the record was corrected so that the wrong patient's information was

amended from the record and documented into the correct patient's medical record. However, there could be other systems that are impacted, including standalone systems, the patient portal, and information released via the health information exchange.

Example #2:

A patient was discharged from a medical unit and admitted to a rehab unit, requiring two separate encounters for billing and reimbursement. Unfortunately, documentation for the second visit was started under the first encounter and continued under the first encounter. Once the issue was identified (after discharge), it was necessary for all of the documentation in the wrong encounter to be marked in error and then rescanned to the correct encounter. Because this was outside of the time that the chart was open, any documentation that occurred electronically was not able to be moved, so all that documentation also had to be printed and rescanned to the correct encounter. The documentation error could have easily been avoided had everyone checked the encounter before documenting.

Example #3:

Patient submitted a request for an amendment (correction) to a clinical note within the patient record. Patient had a worker's compensation injury where she broke her left leg in 2016, but her medical record shows it was her right leg that was fractured. Health information management (HIM) staff received the request for amendment and per organizational policy, contacted the original author of the note to correct the entry. The request for amendment was approved by the original author and the correction was made by the author. HIM identified that through the use of copy and paste the incorrect entry appeared multiple times in subsequent clinical notes, which also needed to be corrected. HIM was then required to work with each subsequent author to ensure that all references to the "right leg" fracture were corrected to accurately reflect the left leg. HIM will continue to serve as a patient advocate as well as stewards of the clinical data and will ensure the highest level of quality is attained.

Example #4:

A new documentation tool is created for the collection of the TNM cancer staging, but when displayed in the EHR it does not display authentication of the person who made the entry. Knowing that all entries made in the EHR are tracked, and being aware of the regulatory requirement for all entries to be signed, dated, and timed, HIM staff contacted the application builder for this tool to ask that the build be modified before it is placed into production. In addition, HIM assisted with testing by producing a release of information report that properly displayed authentication of the entry. HIM involvement in the review and approval of EHR content is critical to ensure general medical record standards are met, as well organizational policy and regulatory and accreditation requirements.

Article citation:
AHIMA. "Ensuring the Integrity of the EHR." *Journal of AHIMA* 90, no. 1 (January 2019): 34-37.