Information Integrity in the Electronic Health Record

American Health Information Management Association

ISBN: 978-1-58426-332-6
AHIMA Product No.: ONB180011

AHIMA Staff:

Claire Blondeau, MBA, Senior Editor

Katie Greenock, Editorial and Production Coordinator

Ashley Sullivan, Assistant Editor

Ken Zielske, Director of Publications

American Health Information Management Association
233 North Michigan Avenue, 21st Floor
Chicago, Illinois 60601-5809
ahima.org

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF CASE EXAMPLES

Foreword

In October 2007, AHIMA's House of Delegates approved the "Resolution on Quality Data and Documentation in the Electronic Health Record." This resolution affirms that "EHR systems are an important tool and provide a significant opportunity to improve documentation and patient care when properly designed and used," but they may also "contain design features and functions that can potentially contribute to suboptimal quality of healthcare data and documentation."[1] The resolution challenges health information management (HIM) professionals to apply their skills and knowledge in data capture methods, compliance, performance measurement, revenue cycle management, and data quality management. It also encourages professionals to collaborate on multidisciplinary teams including physicians, information technology (IT) professionals, informaticists, information managers, and others to ensure the quality of data, documentation, and information in the electronic health record (EHR).

Information integrity in the EHR has a direct correlation to quality patient care. Allied health professionals can support patient care by ensuring appropriate policies and procedures are in place. To assist in that endeavor, this paper provides guidelines for ensuring information integrity in EHR systems.

Authors

Wannetta Edwards, MS, RHIA
Lesley Kadlec, MA, RHIA
Karl Koob, RHIA, CPEHR
Cynthia Rupe, RHIA, CPHQ, CPC
Mary Stanfill, MBI, RHIA, CCS, CCS-P, FAHIMA
Jennifer Sundby, MA, RHIA
Lou Ann Wiedemann, MS, RHIA, CPEHR

Acknowledgements

Cecilia Backman, MBA, RHIA, CPHQ
June Bronnert, RHIA, CCS, CCS-P
Jill S. Clark, MBA, RHIA
Kerry F. Costa, RHIA
Jane DeSpiegelaere, MBA, RHIA, CCS
Angela Dinh, MHA, RHIA, CHPS
Denise Dunyak, MS, RHIA
Mary Meysenburg, RHIA
Nicole Miller, RHIA
Arnita Snead Perry, RHIA
Helayne Sweet, MS
Diana Warner, MS, RHIA, CHPS
Lydia Washington, MS, RHIA, CPHIMS

[1] "Resolution on Quality Data and Documentation in the EHR." Approved by the House of Delegates October 2007. Available online at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035781.hcsp?dDocName=bok1_035781

Introduction

Quality patient care is dependent on the availability and quality of patient information. Poor documentation, inaccurate data, and insufficient information can result in poor patient outcomes and increased healthcare expense. Indeed, inaccurate data can threaten the very lives a healthcare organization is trying to improve. In addition, poor documentation can affect the full spectrum in the continuum of care and inaccurate information may cascade to a variety of healthcare organizations, including primary care providers, specialists, ancillary service providers, and so on.

Information in the health record should clearly and concisely relay the full story of the care that is delivered. Sound information management practices are required to achieve this. The challenges of information integrity in the electronic health record (EHR) are different than those with paper records. For example, with an EHR there is the potential for data to be overwritten. Other examples include the different methods that must be employed to make corrections, complexities associated with updating information in interfaced systems, and redundancies that can result from the use of copy/paste functionality. These challenges, which do not exist with paper medical records, pose significant risk for information integrity. In the EHR environment health information management (HIM), information technology (IT), and health informatics (HI) professionals face the challenge of managing information filtering in from multiple disparate systems, in various media, across multiple interfaces. As stated in Connecting for Health's Common Framework, "data problems represent the dark side of the tremendous potential offered by the adoption of health IT systems."[2] An effective EHR implementation should provide a positive impact on the quality of care, patient safety initiatives, and further organizational efficiencies. This can be achieved by ensuring information integrity practices represent the combined skills and knowledge of key stakeholders. HIM, IT, and HI professionals are among the key stakeholders and should assume a proactive role in the selection, adoption, implementation, and use of EHRs.

Quality data and documentation within the EHR are nonnegotiable.[3] This paper will address many factors that impact information integrity in the course of using and managing EHR systems. Information integrity includes systems, processes, and people issues to ensure the accuracy, reliability, and quality of data. Information integrity is focused on the infrastructure to ensure dependability and trustworthiness of information and is a much broader concept than data integrity. Information integrity encompasses the entire framework in which information is recorded, processed, and used.

Before exploring best practices for ensuring information integrity in the EHR it is important to note that an organization's first step toward information integrity begins even before an EHR is implemented, in the transition planning and system selection process. Selecting and implementing an EHR can be costly and time-consuming with

[2]Connecting for Health. "Background Issues on Data Quality." April 2006. Available online at www.connectingforhealth.org/commonframework/docs/T5_Background_Issues_Data.pdf.
[3] AHIMA. "Quality Data and Documentation for EHRs in Physician Practice." *Journal of AHIMA* 79, no.8 (August 2008): 43-48.

many inherent risks for the organization. According to Trish Greenhalgh, lead author at University College of London's Department of Open Learning, "Depressingly, outside the world of the carefully-controlled trials, between 50 and 80 percent of electronic health record projects fail—and the larger the project, the more likely it is to fail."[4]

Organizations should ensure due diligence in selecting an EHR. This begins with adequate preparation and planning for the request for proposal (RFP).[5] The implementation of a new system alone will not correct workflow inefficiencies nor guarantee end user buy-in. Individual factors such as the amount of end user involvement in system planning, training, ability to accept change, and clear documentation of current processes can prevent failed implementation projects. This advanced planning will lead the organization down the road to a successful vendor selection process.

Organizations should define a core team of individuals who are responsible for discussing, planning, and prioritizing the organization-wide EHR system implementation. The core team should include those who are knowledgeable of best practices for information integrity. For example, an HIM professional can provide the core team with payer guidelines or legal ramifications surrounding the use of copy functionality. Someone on the core team should also be knowledgeable of workflow patterns that will affect data capture, and activities surrounding the transition from paper to electronic processes.

The implementation process itself also has a significant impact on information integrity. Testing of the system and/or individual applications is a crucial part of the implementation process. All systems, workflow patterns, and anything related to documentation and information flow within the EHR system must be tested.[6] During the implementation phase the vendor may initiate testing. However, the responsibility to thoroughly test the system throughout the implementation process resides with the healthcare organization.

Once an EHR system is implemented, how the system is actually used, in terms of information capture, how interfaces are managed, and many other practices, will determine whether healthcare providers can in fact trust the information contained in the EHR to help them deliver quality care. This paper explores best practices to ensure information integrity in the course of using and managing an EHR system, whether fully electronic or in a hybrid state, and covers practices for multiple processes from capturing information all the way through the continuum to sharing information.

---

[4] Fierce EMR Newsletter, December 17, 2009 http://www.fierceemr.com/story/study-80-percent-ehr-projects-fail/2009-12-17.

[5] AHIMA. "RFP Process for EHR Systems (Updated)." *Journal of AHIMA* (Updated March 2010). Available online in the AHIMA Body of Knowledge (BoK) at www.ahima.org.

[6] AHIMA. "Quality Data and Documentation for EHRs in Physician Practice." *Journal of AHIMA* 79, no.8 (August 2008): 43-48.

Part I: Information Capture

Information capture policies and procedures are critical to achieve information integrity as they will assist in preventing and correcting data entry errors. The quality of data input determines the quality of information output, or in other words, garbage in results in garbage out. Each healthcare organization must explicitly define information capture methods that will be utilized, including who is authorized to document within the electronic health record (EHR). Written policies and procedures should specify the EHR applications or modules each discipline may document within.[†] There are organizational tools to assure all documenters are entering data correctly and in a timely manner. These tools include, for example:

- Data Dictionary (DD)
- Data Entry Standards
- Data Entry Guidelines
- Data Entry Procedures
- Appropriate Business Rules
- Appropriate Security Policies and Procedures

Efficient and effective information capture begins with efficient and effective data entry at the point of origin. This section will explore information capture mechanisms employed in an EHR and will provide guidance on data entry practices.

Structured Data Entry

Structured data is entered directly into the EHR at the point of origin, often by the care provider. It can be accomplished through a variety of mechanisms including typing on a keyboard or clicking to select an item from a pick list, as well as more technical methods such as optical character recognition (OCR), magnetic ink character recognition (MICR), reading of bar codes, and radiofrequency identification (RFID).

Structured data is a desirable information capture method because it produces codified data that is computable, that is it can be readily queried, analyzed, and reported.[7] Organizations can take full advantage of this documentation method by establishing clear and concise data values that are enforced through the use of built in edits, dropdown lists, or checkboxes that require the end user to chose specific data points. For example, an organization may choose to designate the problem list as a structured data entry field. In this case, an end user would enter a problem that has been coded in the system (with a code from a standard such as ICD or SNOMED CT for example). In doing so, the organization can search and query problem lists to identify the organization's patient population by diagnoses captured on the problem list. The pick list associated with a structured data entry field may be referred to as the "data dictionary." For more

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

[7] Fenton, Susan H. "Structured or Unstructured? Options for Clinician Data Entry in the EHR." *Journal of AHIMA* 77, no.3 (March 2006): 52.

information on data dictionaries, including defining and using them, refer to the AHIMA practice brief "Guidelines for Developing a Data Dictionary."[8]

Organizations utilizing EHRs that have multiple different data entry options must clearly identify which data fields will be designated as structured data entry fields. Furthermore, for each structured data entry field they must clearly define acceptable entries in the data dictionary and identify whether data entry is required or optional.† Required structured data entry fields will require end users to enter the necessary data before the user is able to continue on to the next data field. Optional structured data entry fields permit the end user to leave the data field blank and continue on, or enter data as appropriate for the particular case. For example, an organization may identify the referring physician data field as optional. In this instance, a registration clerk can skip this data field when registering a patient where there is no referring physician. This presents a risk for errors however, as missing data would result if there is indeed a referring physician and the clerk skips the field, forgetting to enter that data.

Organizations should develop validation methods for structured data entry, such as queries or pop-up windows prompting a user to double check, and they should define the frequency in which the method will be utilized. Such methods will assist the organization in ensuring structured data entry is employed consistently among end users and thus ensuring information integrity. When required structured data entry fields are employed, there should be an associated process to identify missing or erroneous information. This can be done either concurrently, retrospectively, or both. Concurrent queries can be identified so the end user cannot move forward within the application without completing the data entry field. For example, an organization may define admission diagnosis as a required structured data entry field. In this case, the registration clerk must choose a diagnosis from the associated list, any attempts to skip the field or enter free text data will result in a system prompt to complete the field with accurate data.

Some examples of where system edits might generate useful queries include:

- Correct field length (that is, social security number less than nine digits)
- Invalid values (that is, age over 110 or less than zero)
- Self validating codes (that is, ICD-9 and CPT compatible for sex or site)
- Numerical or text fields (that is, no numerical fields for addresses)
- Correct date values (that is, discharge date before admission date)

Organizational defined exception reports are normally used for administrative purposes. They can be set up to run at a specific time to provide a list of potential data errors. In defining the process, someone is assigned to review the list, determine if there are indeed any errors, and ultimately correct them. In the earlier example, the organization identified referring physician as an optional structured data entry field. In this case, the organization

[8]AHIMA e-HIM Work Group on EHR Data Content. "Guidelines for Developing a Data Dictionary." *Journal of AHIMA* 77, no.2 (February 2006): 64A-D. Available online in the AHIMA Body of Knowledge (BoK) at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_030582.hcsp?dDocName=bok1_030582.

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

could develop a retrospective query to create a list of cases where this data field is blank. The query could be set to automatically generate a report each night at the time of the midnight census. The night shift registration manager could be assigned to review the report, verify there was no referring physician, and/or enter the referring physician if one is identified. This process results in more accurate information. It also generates information about outcomes that should be used for trending accuracy rates of the relevant staff and to identify training opportunities.

Some examples of exception reports include:

- Quantitative Analysis for missing data (for example, registration report identifies patients admitted the prior day lacking telephone numbers)
- Use of check digits (for example, HIM bill hold report identifying accounts that may need modifiers)
- Transaction history (for example, preregistration report identifies patients whose admission dates have passed, to determine if a second account was incorrectly created)

As noted earlier, structured data entry is advantageous because it produces computable data. However, there are limitations of this data capture mechanism. As with any method, structured data entry does not guarantee data entry errors will not occur. End user training is important and should at least include the following elements:

- Recognition of required versus optional fields
- Appropriate utilization of drop down screens or checklists
- How to select the correct data from associated lists
- A review of inappropriate practices that can result in inaccurate data

A significant limitation of structured data entry is that the end user can only enter data in the structure defined for the data field. In many instances, the entry must be selected from the codified list that is associated with the data field. This can make it difficult to capture unique aspects of a case, or to record the unusual or unexpected as only anticipated values are likely to be included in the predefined list. Thus structured data entry is not appropriate for all information that must be recorded in the EHR and it is not the only data entry mechanism employed.

Free Text Entry

Free text entry, in contrast to structured data entry, is narrative text recorded in the author's own words. It may be entered directly into the EHR by the source, or indirectly via a third party. It can be accomplished by typing directly into a free text data entry field, dictation and transcription, or speech recognition applications. The simplest method allows the author to type into a text box in the EHR. Organizations employing free text

entry in the EHR must explicitly identify each free text field, define its purpose (e.g., type of transcribed report or physician progress note), and establish its length.[†]

Free text data entry fields allow a healthcare provider to record the unique aspects of a case that cannot be anticipated for inclusion in structured data fields. Free text narrative data is valuable to a person who reads and interprets the narrative on a specific case, but it cannot be queried, analyzed, and reported without sophisticated natural language processing (NLP) applications. Such applications are in development but despite advancement in recent years are still not widely employed in EHRs. NLP techniques are more common in other systems designed to work with EHRs, such as in transcription or computer-assisted coding technologies. Still, free text data entry fields are often used, for example to capture progress notes on inpatients. This data entry method allows providers to type progress notes directly into the EHR as patients are treated, eliminating legibility concerns with handwritten notes, and transcription delays.

There are also drawbacks of free text data entry however. It can be time consuming for healthcare providers to personally type all of their notes and dictation/transcription mechanisms are costly. More importantly, free text entry does not produce structured, codified data. In fact narrative data is largely "hidden," essentially "buried treasure" in an EHR. Standardization efforts are underway however to provide some additional structure by codifying narrative document types, and headers or sections within documents. The Health Story Project in conjunction with Health Level Seven (HL7) and other related organizations, developed five technical implementation guides using HL7's Clinical Document Architecture (CDA), such as HL7's IG for CDA Release 2: Consultation Notes: Draft Standard for Trial Use.[9] The standardization and adoption of these electronic documents will provide a treasure map to help unlock the valuable data hidden in narrative documents.

There are a couple additional considerations with free text data entry. These data fields within EHRs are typically limited in character length. Free text fields that are too short may not allow a provider to adequately describe a patient's condition or explain the course of treatment, thus causing potential patient care risks. The quality of the narrative data may also be a concern. A recorded narrative reflects the author's distinct dialect and writing skills and excessive use of abbreviations or slang language may render the narrative unintelligible to another provider reading the text.

Healthcare organizations that have not employed NLP applications with free text risk information integrity when free text entry:

- Is overutilized in the EHR
- Is used to create standard reports
- Narrative is ambiguous
- Documentation space is too limited

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

[9] HL7's Clinical Document Architecture available online at www.hl7.org/implement/standards/cda.cfm.

At a minimum, healthcare organizations, who are not using machine language translation tools such as NLP, must ensure free text data is used judiciously in the EHR and standard, routine reports are not generated from this data capture methodology.

Organizations must carefully consider the documentation methods that are most effective for them and employ both structured data entry and free text entry to optimize the efficiency and effectiveness of information capture in the EHR. Information that has predictable values, such as numerical data (for example, dates and lab values), should be captured as structured data. Free text entry should be used to capture the type of information that is not predictable or readily structured.† In general, healthcare organizations must define when structured data entry versus free text entry will be used in order to clearly and concisely capture the full story of the care delivered.

Copy Functionality

Though copy functionality is not an information capture method per se, it is important to discuss this functionality in light of its impact on data entry. Copy and paste functionality within EHRs allows for the easy reuse of documentation as well as easy movement of information throughout the system and even across the healthcare continuum. Use of this functionality for example would allow an end user to copy laboratory results from the lab system and paste them into the emergency department physician report housed in a separate application. Information can easily be copied from one application to another or from one report to another.

This functionality can be a great time saver for the end user. However, controls are necessary to prevent excessive use resulting in redundant information, creating information "noise." Organizations using EHR systems with copy and paste functionality should ensure the source of such copied information can be clearly identified and the system has the ability to support the audit of information that has been copied. The organization should define policies and procedures that address the appropriateness and use of this functionality in order to ensure it does not degrade the quality of documentation.

The use of copy functionality without the ability to review, test, audit, and approve the quality of the resultant documentation can present significant information integrity risks with potential legal and compliance implications. Healthcare organizations must have appropriate checks and balances in place so the use of this functionality can be systematically evaluated.† For more information and guidance on this functionality, review AHIMA's Copy Functionality Toolkit.[10]

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

[10] AHIMA Copy Functionality Toolkit. Available online in the AHIMA Body of Knowledge (BoK) at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_042564.pdf .

Clinical Decision Support Functionality

Clinical Decision Support (CDS) provides clinicians, ancillary departments, patients, and other individuals with knowledge and information designed to enhance healthcare processes and outcomes. It encompasses a variety of tools and interventions that are inserted in the clinical workflow as the end user is reviewing or entering information in the EHR. Though CDS is not an information capture mechanism, it is inserted in the information capture workflow, thus CDS is discussed here because of this relationship to information capture.

CDS functionality includes computerized clinical alerts and reminders, clinical guidelines, order sets, patient data reports and dashboards, documentation templates, diagnostic support, and clinical workflow tools.[11] Organizations should determine what CDS is appropriate and compatible with their specific EHR and implement them in conjunction with medical staff input and practice considerations.

A CDS can take many forms; it usually runs in the background of the EHR and commonly provides prompts, additional screens, or reminders to clinical providers or ancillary staff. For example, it might include automatic system alerts to a physician of critical lab results, or remind a primary care provider of the need to order a mammogram for a specific patient. Organizations take a wide variety of approaches when implementing decision support, ranging from simply using an EHR to alert physicians when a patient is overdue for a test, to developing sophisticated protocols that provide a step-by-step guide to treatment of specific conditions.[12] In either circumstance, the CDS application has a direct impact on the information captured.

CDS applications are one of the main goals underlying the drive to increase EHR adoption industry wide. They enhance the EHR system to achieve improved organizational efficiency, and assist providers in direct patient care activities by improving communication between the members of the clinical care team. This will only occur however, if CDS prompts and alerts are reviewed and acted upon. Therefore “alert fatigue” is a major impediment.

Alert fatigue occurs when there are too many alerts causing providers to click through them without utilizing the decision support the alerts provide. For example, if physicians too often find the prompts to be meaningless or without value, they will likely begin to disregard them, perhaps without fully reviewing or considering them. In 2009, Dana Farber Cancer Institute and Beth Israel Deaconess Medical Center researchers reviewed the electronic prescriptions and associated medication safety alerts generated by 2,872 clinicians at community-based outpatient practices in Massachusetts, New Jersey, and Pennsylvania. Researchers found clinicians overrode more than 90 percent of the drug

[11] Glaser, John. *Clinical Decision Support: the power behind the electronic health record*. Available online at http://www.allbusiness.com/technology/software-services-applications-information/11468254-1.html

[12] “Supporting Clinical Decision in the Physician’s Office.” Health Data Management, October, 2009 by Howard J. Anderson, Executive Editor.

interaction alerts and 77 percent of the drug allergy alerts.[13] Organization must design alerts in the EHR wisely and judiciously in order to prevent alert fatigue.

George Reynolds, M.D., chief medical informatics officer at Children's Hospital and Medical Center in Omaha, Nebraska has a goal for the use of alerts at his organization. Reynolds' long-term goal is to make most alerts virtually unnecessary. "I don't want alerts to fire at all. I want the order sets to be written well enough that they steer doctors to the right choices."[14] In other words, well-designed structured data entry fields should work hand-in-hand with the CDS application.

In addition, an organization utilizing CDS functionality must determine how decisions made based on CDS alerts will be captured in the EHR.[†] At this time there is no legal precedent regarding the use of CDS data within the legal health record. However, in response to E-Discovery the use of CDS could potentially fall under the use of metadata and organizations may be placed in a position to explain the alert, its use, function, and standard of care in the case of litigation.

Metadata

From a system standpoint an EHR consists of the health record text, source data, and the related metadata. Metadata is structured information that describes, explains, locates or otherwise makes information or a document easier to retrieve or use, and eases the management of the information source. Metadata, often simply described as data about data, can validate and quantify the authenticity, reliability, usability, and integrity of information over time and enable the management and understanding of electronic information (physical, analogue, or digital).[15] It runs in the background of the EHR and contains descriptive information about the data. The document text, structured data field, or images are what the end user sees when viewing or printing the record. Metadata often remain in the background of the EHR and may never be seen, not even when a record is printed.

There are three main types of Metadata:

- Descriptive Metadata: Includes elements such as title, abstract, author
- Structural Metadata: Includes information such as how pages are ordered to form chapters
- Administrative Metadata: Includes information such as how the document was created and file type

IT professionals should ensure system functionality defines each type of metadata within the EHR. In addition, the Records Management and Evidentiary Support HL7 functional

[13]Merrill, Molly."Docs Succumb to Alert Fatigue" *Healthcare IT News*, March 2009. http://www.healthcareitnews.com/news/docs-succumb-alert-fatigue-study-shows.
[14] Anderson, Howard J. "Avoiding "Alert Fatigue." *Health Data Management*, October, 2009.
[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.
[15] Dougherty, Michelle. "Using the HL7 Standard to Evaluate Your Legal EHR." 2009 AHIMA Convention Proceedings, October 2009.

profile[16] provides an important tool that organizations can utilize for evaluating EHR system functionality. A comprehensive assessment should be conducted on all components, applications, or modules in the EHR that capture health record information. System assessments should be conducted prior to purchasing an EHR to assess a current system, its metadata, and the overall impact of both on information integrity. Metadata is playing an increasingly important role in E-Discovery. Organizations and providers are advised to preserve metadata as a regular business practice, and particularly in connection with ongoing litigation.[17] Healthcare organizations must evaluate metadata parameters in the EHR to determine if they meet the requirements to support the business and legal needs of the organization.

Organizations risk information integrity if the metadata contained within the system and any applicable data dictionary are not consistent with organizational and regulatory business rules. If metadata is not appropriately implemented within the system, there may be significant information integrity concerns. The metadata include business rules governing each data field. Healthcare organizations must ensure EHR system metadata functionality is understood and is consistent with the organization's current business rules. In addition, organizations should review and update metadata and corresponding data dictionaries on a regular schedule.

[16]The HL7 RMES profile is available online at: http://xreg2.nist.gov:8080/ehrsRegistry/faces/view/detailFunctionalProfile.jsp?id=urn:uuid:75cb7051-678e-40aa-9365-908d5ab43340

[17] Richmond Journal of Law & Technology Volume XIV, Issue 3

Part II: EHR System Management and Use

Management and use of electronic health record (EHR) systems has a direct impact on information integrity. For instance, interfaces between applications require careful management to ensure data are transferred and shared as expected without degradation or loss and an accurate master patient index (MPI) is also critical for information to be associated with the correct patient.

This section of the paper explores practices for managing these processes to ensure the accuracy of clinical information in the EHR. The use of error reports, designed to assist organizations in identifying and correcting inaccurate data, will also be explored. In addition this section provides guidance for planning and implementing EHR system updates and upgrades, and for maintaining a legal health record and information security.

Managing Interfaces

The EHR system is often comprised of multiple systems that work together to present unified views to the end user. For example, it is not uncommon for an organization to have a separate registration system, radiology system, laboratory system, and such. Large healthcare organizations may have hundreds of interfaces between computer applications and disparate information systems. The patient health record is likely comprised of information compiled via interfaces from a variety of systems. To streamline workflow and improve patient care, healthcare providers must be able to trust information presented by the EHR. Thus interfaces between systems require careful management to ensure data are transferred as expected without degradation or loss.

To maintain information integrity, when using multiple interfaced systems, data created or revised in one system must be seamlessly transmitted to update pertinent interfaced systems and the source system must be explicitly identified. For example, demographic information created in a patient registration system should be available in the clinical information system, in the laboratory system, in the radiology and pharmacy systems, and such. A common approach to address this challenge is the utilization of interface engines that support Health Level Seven (HL7) message routing standards.[18]

Depending on system requirements, the data transferred may retain its original format (rich text font), ASCII text, or it may be transferred as HL7 documents with formatted headers and body. Newer document formats include extensible mark-up language (XML) and Clinical Document Architecture (CDA) XML documents. XML documents have an advantage over text because they are able to display or print with formatting, for example via a template, including bold, underline, and application of logos. XML can also store a file in a fraction of the space required by rich text files. Organizations must understand the interface engine technology within their EHR systems, receiving system requirements, and formatting requirements.

[18]Information regarding HL7 message routing standards can be found at: http://www.hl7.org/implement/standards/v3messages.cfm

Figure 1 depicts the cascade of data through multiple systems via system interfaces. Each system receives data from the preceding system, thus data quality in one system directly impacts the data quality in another system.

Figure 1. Data cascades through multiple systems via system interfaces

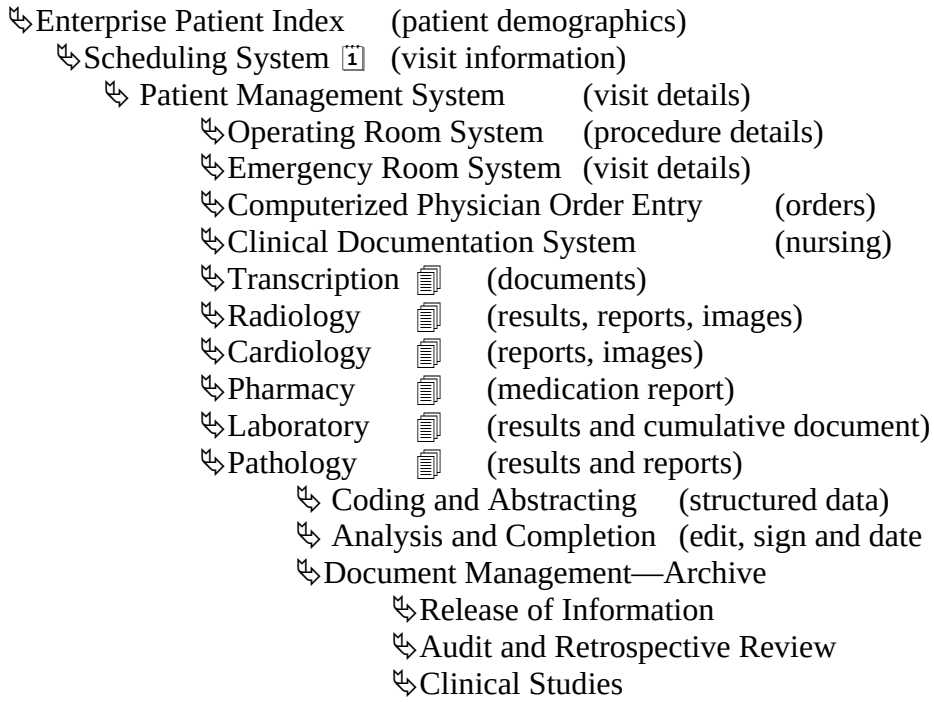

Figure 1 illustrates that if an error occurred in the scheduling system it would perpetuate in the patient management system, and likely the operating room module, emergency room system, computerized physician order entry module, clinical documentation module, transcription, and so on. If a registration person selects the wrong patient from the MPI for example, there can be a cascade of clean-up and repair to ensure the patient data is corrected throughout the entire patient record. In this example, the error could impact as many as 17 instances of patient data, unless it is caught and corrected early.

An interdisciplinary team is needed to ensure information integrity is maintained across multiple interfaces. The team should be comprised of the persons responsible for users that contribute data to one or more systems (for example, registration, patient management, and clinical system managers), ancillary systems managers that interface data (for example, radiology, laboratory), and those who manage data quality (for example, departmental data managers and/or data analysts).

Interfaced data must often traverse networks and temporary storage locations as it moves from its origin to destination systems. It is not uncommon to have an original document that is transferred to multiple systems. Figure 2 demonstrates how a single document is transferred to multiple systems.

Figure 2. A single document transferred to multiple systems.

- Transcribed History and Physical (original resides in transcription system)
  - HIM Reports (sent via interface to the HIM report application within the EHR)
    - History and Physical (filed under the History and Physical data tab in HIM Reports)
  - Physician Report View (viewed by physician via report application)
  - Document Imaging System (extrapolated from EHR to the HIM document imaging system for long term storage)

Data can be transferred in batch or real time mode, depending on the system and end user requirements. Regardless of the data type, format, and transfer mode or schedule, system managers must have a process to confirm that data has interfaced and transferred without alteration or degradation from the source to all intended destinations.[†] System managers typically verify the following to ensure data were properly received:

- Data transferred from source system—date, time, patient identifier
- Data received at destination—date, time, patient identifier
- Data that failed either on transfer or receipt—date, time, patient identifier

The review process should offer the end user a means to track failures in each system, via error logs at the batch and individual data level. The corrupted data identified on error logs will need to be recompiled, resent, or recovered manually. It is important to identify failures, including erroneous or missing data, as soon as they occur. Imagine if an interface were not working properly for a long period of time, the downstream effects could be disastrous, impacting multiple users and several functions within the healthcare organization, including patient care.

Corrections and changes to healthcare documentation in electronic systems must also be managed carefully to ensure information in the source system is synchronized with information in destination (interfaced) systems. Table 1 presents some options for managing information changes that must be shared across multiple systems via interfaces, and outlines the associated ramifications and risks that must be mitigated with each option. Each healthcare organization must determine the best option to utilize and then be sure to address the ramifications and mitigate the associated risks.

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

Table 1. Options for managing corrected information across interfaces.

Option	Resultant Ramification	Risk
All changes/updates are pushed out to relevant interfaced systems	Document must be created, edited, and signed in the same system. This may or may not adhere to the provider's workflow	Multiple copies of documents are transferred
Final version of document is maintained in document management system	Document created in one system, with possibility for editing, signature, and addendums in another system	Provider treats patient without current version of document
Documents are labeled in receiving systems as preliminary, with notations referencing which system has the final copy	The final copy may only be available in the source system; receiving systems may remain a preliminary status indefinitely	Provider treats patient without current version of document if accessing the information in a receiving system
Document transferred to clinical repository as HL7 text document. Updated, amended documents may reside in other systems	Document will be easily accessed by providers. The document may have different appearance than original, legal copy	Provider may have difficulty finding information because it looks different

Managing the Master Patient Index

An accurate MPI is critical to EHR system management and use. The MPI provides the first link in the organization's EHR because it creates a unique identifier for every individual encountered in the care system. It also becomes important in data capture functions, as registration personnel access the MPI to locate the unique identifier (or create a new entry) that will be associated with all data and information on the patient for the current encounter. An accurate MPI provides the consistent link and location of a patient's health information across the organization, and potentially across an enterprise or within a health information exchange (HIE); thus creating a longitudinal record that facilitates interoperability between multiple systems, clinical care providers, and organizations. The MPI database can further assist organizations by indexing healthcare plan members, guarantors, subscribers, physicians, healthcare practitioners, payers, and employees. Healthcare organizations must develop clear and concise policies and procedures for managing and maintaining the MPI to ensure clinical information is associated with the correct individual in the EHR.

The process of assigning unique identifiers, often referred to as "medical record numbers," typically begins with registration or preregistration of a patient. In this process, registration staff will either locate the patient in the MPI database or will create a new patient entry. The larger the MPI, the more patient names there are to search through to determine if the patient is already uniquely identified in the database. Many patients

within the MPI have the same name, same spelling, or same birth date. In addition, if the organization is a part of an integrated healthcare delivery system, the MPI may increase exponentially across the enterprise. For these reasons, the risk of creating duplicate patient entries is high, and managing and correcting duplicates in the MPI requires an ongoing process.

Healthcare organizations must be proactive in assisting registration personnel in the proper identification of patients. Relevant staff should be trained explicitly to correctly identify existing patients in the MPI database. For example, this training might direct registration staff to ask specific questions that will identify outdated information and prevent creating duplicate records. Such questions may include:

- Do you still live at (state address)?
- Do you still work at (state employer)?
- Is your next of kin still (state next of kin)?
- Have you ever registered at this facility under a different name? (for example, have you recently gotten married?)
- What is your legal name? Do you have a nickname?
- What is the name on your insurance card? Has your insurance changed since your last admission?

The process of merging and correcting duplicate medical record numbers is typically managed in the HIM department. However, medical record number assignments are typically done by registration staff in different departments at multiple points throughout the organization. This can make it difficult to manage the process. The HIM department should work closely with registration staff facility-wide to train and educate on the importance of a clean MPI and the cascading affect of duplicate numbers. In any case, the organization must clearly define the department or individual within the organization who is responsible for maintaining and ensuring integrity within the MPI. Healthcare organizations must be committed to ensuring the MPI is accurate and free of duplicate patient information in order to reduce risks in patient care, and to be able to share information through health information exchanges and the national health information network (NHIN).

MPI software is available and normally consists of probability matching. This type of matching allows the organization to build in specific patient demographic to reduce the number of duplicates created. For back end MPI clean-up activities there are a variety of companies that provide MPI cleanup services. These companies typically utilize software that employs elaborate algorithms to capture duplicates based on a predetermined weight of the identifiers that are employed. The outside service company can either identify and resolve duplicates, or merely identify errors and send them back to the organization to make the corrections. For more information on MPI data conversion, reconciliation, and core data elements refer to AHIMA's practice brief "Reconciling and Managing EMPIs."[19]

[19]AHIMA. "Reconciling and Managing EMPIs (Updated)." *Journal of AHIMA* 81, no.4 (April 2010): 52-57. Available online in AHIMA Body of Knowledge (BoK) at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_046942.hcsp?dDocName=bok1_046942 .

Managing Error Reports

Error, or reject, reports provide organizations with information regarding specific data requirements that were not met. They are designed to assist organizations in identifying and correcting inaccurate data. An example of an error report is a daily report that indicates which transcribed documents failed to post from an interfaced transcription system to the EHR. Another example is a report that indentifies which charges (generated in the EHR) failed to cross over to the billing system. Reports like these can be auto-generated based on rules written in the system or they can be ad hoc reports managed by users. The ability for an EHR to generate these types of reports is critical in ensuring data is handled accurately and reliably by all systems.

The number of error reports an organization chooses to review on a daily, weekly, or monthly basis will vary but should be sufficient to support information integrity. Developing too many reports would unnecessarily increase workload, possibly causing duplication of work with little return on the extra effort invested. Choosing too few reports may result in undetected data errors and increased risk, jeopardizing the quality of care. Each organization should define, by department, the error reports that will be used to ensure data and information integrity. This definition should include the timing of each report, how reports will be maintained, and who is responsible for working each report. This process ensures that corrupt data is identified and corrected before it perpetuates within the system or network.[†]

Managing System Updates

The lifecycle of an EHR system includes system updates or upgrades to software applications and databases. It also may include an update to the EHR by implementation of a new module.[20] It is crucial that these types of system changes are thoroughly tested. Organization must conduct comprehensive testing of new or upgraded EHR modules in both test and live environments. In addition, they must test how new or upgraded modules interface with existing applications and function within the organization's workflow.[†]

The most common reasons for system upgrades are customer requests and regulatory changes. Vendors often deploy system functionality updates to solve problems relayed via customer user groups or to retain a competitive edge in the market place. Vendors also deploy upgrades to comply with regulatory requirements and to remain compatible with new technology. Organizations require a process to review and confirm the timing

---

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

[20] Note: References to system testing, system updates, or system upgrades in this section refer to software application updates, database upgrades, or an update to the EHR by inclusion of a new module. Regularly scheduled system updates that occur routinely on an ongoing basis are not addressed here (for example, the recurring midnight census update).

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

of system updates in advance, so that they may determine the impact on users and test updates appropriately.[†]

Once a system update or upgrade is planned, extensive testing should be organized and communicated to relevant staff. In addition, organizations should have:

- Defined procedures that allow end users to be actively involved in the update process,
- An organized and prioritized update schedule, and
- Active communication with IT and other vendors that may be impacted by system enhancements.

Each department should identify a system "super user" who is responsible for communicating between the individual department and the EHR core team. These super users can also be utilized for testing and training within the department. The organization should develop a test environment that super users can use extensively for testing and training EHRs and other applications. This test environment simulates real life situations without potential harm to live data. When a vendor releases a system update it should be deployed in a manner that allows the organization to "turn on" new applications, features, or functionality in an incremental fashion. The use of departmental or application super users allows organizations to gauge the impact of each update independently and plan for its overall affect.

Any update has the potential to affect another application. Regression and integration testing for all changes should be incorporated into the overall implementation plan. Minor changes in system functionality may not appear to require extensive testing; however their affect on another application may turn into a major change. It may be difficult to test every single element within the system, so it is important to anticipate the impact of changes and prioritize testing efforts. For example, an organization may choose to identify high risk, high volume, or problem prone areas for extensive testing efforts. Vendors can assist the organization in identifying specific areas within system upgrades that may be affected, however in the end, it is the healthcare organization that is at risk for system upgrades that are not fully tested, particularly in regards to integration testing between applications.

As more information is captured electronically, organizations will also encounter risks in aging or legacy data management. As part of system updates and upgrades, organizations must address the management of aging data, including investigation of specific system purging and archival capabilities, potential system space limitations, and routine archival intervals or back-ups.[†] Initially, many organizations may choose not to purge or archive any data. This is because when the system is new, space is readily available and system response time, when retrieving data, is initially acceptable. But as more data is stored in the system, system response time can decrease due to the large amount of data stored. Some systems may not have purging or archival capabilities that meet the statute of limitations required in individual states or defined in hospital policy, thus requiring back-

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

end processes to ensure health data is maintained for the required length of time. Adequate management of healthcare legacy data carries inherent risks to cash flow, effective operations, and record-retention requirements. These risks can be mitigated by thorough testing of applications and proactively preparing for legacy data management.

Maintaining the Legal Health Record

The legal health record (LHR) is defined as the subset of all patient-specific data created or accumulated by a healthcare provider that constitutes the organization's official business record, and is typically used when responding to formal requests for information for legal and legally permissible purposes.[21] The LHR is a subset of HIPAA's required designated record set. In the EHR, organizations have struggled to define the information in the LHR, correlate it with HIPAA privacy requirements, understand the need for a designated record set, and ensure electronic information is retained in accordance with record retention requirements.

It is the health information manager's responsibility to ensure the organization has an LHR policy and it is maintained to meet state and federal specific statute of limitations. A healthcare provider organization must develop and maintain an inventory of the documents and health information that comprise the LHR and declare the LHR in policy. As updates and additions are made to the EHR system, the organization must review the inventory of information that comprises its legal health record and update its legal health record policy to reflect changes in the inventory as necessary.[†]

The HIM professional should understand functional aspects of the EHR system, including any system limitations that would affect the legality of the health record.

A significant consideration in defining the LHR is determining when to include external information. Integrating health information from external providers or other healthcare organizations is a common practice in healthcare. HIPAA requires organizations to include any information used in clinical decision making. However, organizations often struggle to identify which pieces of external information were used in clinical decision making. LHR policies must describe how staff will correctly identify external information used in clinical care decisions and dispose of information that is not used. Policies should define limitations on redisclosure and describe requirements for clinical staff training on the use, storage, and disposal of external information.[†] For more information refer to AHIMA's practice brief on "Developing a Legal Health Record Policy[22]" and the "Legal Health Record Matrix" in the accompanying appendix.[23]

---

[21] Servais, Cheryl E. *The Legal Health Record*. Chicago, IL: AHIMA, 2008.
[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.
[22] AHIMA EHR Practice Council. "Developing a Legal Health Record Policy." *Journal of AHIMA* 78, no.9 (October 2007): 93-97. Available online in AHIMA Body of Knowledge at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035543.hcsp?dDocName=bok1_035543.
[23] "Developing a Legal Health Record Policy: Appendix A." *Journal of AHIMA* 78, no.9 (October 2007): web extra. Available online in AHIMA Body of Knowledge at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035718.hcsp?dDocName=bok1_035718.

Information Security

Paper health records were maintained in file rooms or offsite warehouses and secured via keypad entry locks and other physical measures. Information security in the electronic or hybrid environment includes additional complexities such as the need to secure not only information on hard drives but also on mobile devices. For example, organizations must address laptops, palm pilots, and discs in the information security program. It is unlikely someone could walk out of an organization with 50 patient paper records; however losing a laptop with thousands of pieces of patient data on it can happen easily. If this were to occur and the information had not been stored anywhere else it could have an impact on patient care. Organizations must clearly define information security processes in policies and procedures. The information security policy must address the security of portable devices, the removal of protected health information without encryption, define breach notification processes, and address network security. For more information refer to AHIMA's practice brief "The 10 Security Domains."[24]

Disposal of health records also poses a risk to information security. LHRs should be maintained in accordance with state and federal record retention guidelines. For example, some states require adult health records to be maintained for seven years after the date of discharge. At the end of the retention time period, health records may be disposed of, but disposal must be done in the proper manner. Disposal of health records is a key component of an organization's record retention program. It can be expensive to store health records past the retention date; in addition retrieval of these records (if they are requested) can become labor intensive. Records management software is available to coordinate records management activities throughout the information lifecycle. Organizations must define destruction methods for each type of media in the facility (for example, radiology films, paper documents, and electronic laboratory results) to ensure the end result is to permanently, irreversibly destroy or erase protected health information.[†] For example, when destroying paper records the organizations may choose to cross cut shred, pulverize, or incinerate the paper. Electronic media such as USBs and CDs may require physically damaging the media. If an organization chooses to outsource the destruction of protected health information, the organization must have a signed contract with the vendor in order to mitigate risks of a breach. The contract should, at a minimum, spell out the responsibilities of the vendor for the secured destruction of records and information. It must also include the manner of destruction, time frames for destruction, and ensure a certificate of destruction is maintained.

---

[24] AHIMA. "10 Security Domains (Updated)." *Journal of AHIMA* 81, no.2 (February 2010): 57-61. Available online in AHIMA Body of Knowledge at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_046425.hcsp?dDocName=bok1_046425 .

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

Part III: Hybrid Records Management

A hybrid record is a system with functional components that include multiple media and utilize both manual and electronic processes. The media in hybrid records most often includes both paper documents and electronic data, but they can also include scanned images, microfilm, microfiche, and CDs. Managing information integrity in a hybrid health record environment presents unique challenges that affect many functions.

With hybrid health records there is the danger that some documentation, data, or information will be in the paper record but not available online and vice versa. Any ambiguity on where information is located carries the risk it may not be found. It is not realistic to expect clinical care providers to check in two places for information and patient care may suffer if care providers cannot locate the information they need. There is also a downstream risk for end users. For example if health information management (HIM) or quality management professionals cannot locate information, it will be omitted when performing job functions such as coding or quality reporting. The organization can mitigate risks by methodically tracking the location of information across the organization and developing clear policies and procedures that address information management throughout the transition to fully electronic information.

A large number of organizations are in a hybrid state and continue to move toward an electronic health record (EHR) by implementing specific applications based on an overall implementation schedule. This transition process requires strong project management and leadership skills as well as the ability for complex decision making. Information integrity must be maintained as each new application is implemented through workflow analysis and revision of policies and procedures.

This section of the paper explores the impact of the hybrid environment on the following:

- Physician order entry
- Patient safety
- Quality reporting
- Record completion
- Coding

Physician Order Entry

In the hybrid environment there are many processes that begin electronically but end manually or vice versa. As new EHR modules are implemented, each organization must define how these processes will be handled. This is particularly important in relation to capturing physician orders. For example, a physician may write a paper order that is entered into the EHR by someone else. If an organization utilizes this type of indirect data entry, the system capabilities to support this process must be identified and a standard process for authentication of verbal orders must be determined. This is critical because multiple data integrity issues can arise. For instance, with indirect data entry of orders, the time the physician wrote the verbal order likely does not match the time the

order is entered into the EHR, which can be problematic. If an organization has a significant delay in the data entry process, patient care risks may arise.

Verbal order entry hinges on staff entering the order correctly as a verbal order and correctly identifying the provider who gave the order. If either of these two steps are done incorrectly, the system cannot function as it was designed. The following case example illustrates this point.

> Case Example #1:
> At one particular facility, verbal orders are the exception, not the norm, so the order entry system is configured to default every order as a "written" order. At this facility, this means when a nurse enters a verbal order, he must remember to change the default parameter to "verbal" order. Furthermore the workflow is designed so that verbal orders automatically trigger the system to queue the physician for signature.

Organizations should ensure system functionality is clearly understood and built into end user training. In the above example, staff must change the parameter of the order from "written" to "verbal" so the system will prompt the provider for a signature. If the nurse does not change the default, it will appear as if it is a written order and the system will not forward the order to a provider for signature. Depending on system functionality, the organization can prevent an error by developing a built in system check that "rejects" an order signed by someone who is not authorized to issues orders; thus the nurse in this example would likely receive an error message and be prompted to change the parameter. The organization can also develop a custom report that identifies any order signed by someone who does not have clinical staff privileges to issue physician orders.

As noted above, verbal order entry also hinges on correctly identifying the provider who gave the order. The following example illustrates the problem that can arise if this is not done correctly.

> Case Example #2:
> A nurse receives a verbal order from Dr. John Smith and inadvertently enters the verbal order as Dr. Joseph Smith. The EHR system assigns the signature application to the wrong physician. When Dr. Joseph Smith logs into the system he may or may not realize this is not his patient. If he signs the order, he becomes a physician of record on a patient he has never seen. If he recognizes the error, a process is needed to correct the order and assign it to the correct physician.

In this example the organization may have no way of identifying the data entry error until the physician has already signed an incorrect entry. As noted earlier, understanding the system functionality is critical. Organizations must clearly define how correcting or retracting CPOE data entry errors will be accomplished. Procedures for doing this vary depending on system functionality. Organizations should explore these errors with the vendor and explore correction opportunities. For example, correcting a progress note may be an editing function within the application, while correcting orders in the order entry

module may be more complex if system functionality is designed to consider orders permanent once a signature has been applied. If the incorrect provider identifies the error prior to signing the order; organizational policy should further define which department or staff are allowed to change the physician assignment on the order.

Patient Safety

Patient safety risks can occur in the hybrid record when information is handled by multiple people. For instance, the hybrid ordering system discussed in the previous section carries patient safety risks as illustrated in the following example:

> Case Example #3:
> A physician hand writes an order for 25 mg of Phentynol. A ward clerk enters the order into the electronic system, however inadvertently enters 250 mg of the medication instead of 25 mg.

Human error in data entry such as in this example may not occur often; however the results could be catastrophic. In the hybrid environment the system may not have the capability of built-in checks and balances to ensure this type of error in case example #3 does not occur. In addition, legibility issues continue when the original order is handwritten by the provider. The electronic order that is entered by the ward clerk is legible when it is sent to the receiving department; however the original handwritten order that is a part of the legal health record may not be.

As organizations maintain information in both paper and electronic mediums, patient safety concerns can also arise if those involved in patient care are using different sources for information. In this hybrid environment clinical providers may still rely on the paper documents as their primary source of information for making clinical decisions. This can become risky if the electronic application has been updated and the paper has not. This is illustrated in the following example.

> Case Example #4:
> Upon admission, the attending physician reviews a printed chest radiology report that indicates no abnormalities, and consequently does not include antibiotics in the admission orders. However the radiologist subsequently amends the radiology report in the EHR to reflect a positive finding of a pulmonary infiltrate. The attending physician is not using the EHR and thus is not aware of the revised radiology report causing a delay in the order for antibiotics by several hours and thus delaying the patient's recovery.

Organizations can minimize patient safety concerns by providing education and training to clinical care providers regarding the location of source information in a hybrid environment.

Quality Reporting

An EHR can be a very useful tool for gathering data for quality reporting. In a hybrid environment however, organizational reporting is at risk because information is typically pulled from paper documentation as well as electronic data fields. As EHRs are implemented, an organization can define specific fields that are built into the system to capture mandatory quality reporting indicators. These quality fields are specific to the organization and are often a customized field; thus creating potential information integrity issues if the custom fields are not completed correctly. This is illustrated in the following case example.

> Case Example #5:
> An organization wants to track the Joint Commission Stroke Performance Measurement (STK-04) electronically (so they need to record when IV thrombolytic therapy was initiated for stroke patients). In the emergency department system, they added a data field that is linked to the pharmacy module. As the thrombolytic agent is ordered in the emergency department the system asks the provider if this is a stroke patient. If the provider answers "yes" then an automatic timer begins in the system. The timer turns off when the nurse enters that the thrombolytic agent has been administered.

The process described in this example will only collect accurate information for the quality indicator if the provider correctly answers the initial question. To further complicate matters, providers often see patients in multiple healthcare facilities and quality reporting mechanisms may vary from one facility to the next.

Quality reporting varies from organization to organization as well as from system to system, both in terms of what measures are employed and how the information is captured. Integrated health care delivery systems (IHDS) with several facilities, including perhaps outlying clinics or individual physician practices, face a real challenge to standardize the mechanisms for gathering quality reporting data. If the IHDS is implementing an EHR in a staged approach, for example a module at a time or a facility at a time, some sites may be utilizing electronic data capture for quality reporting and others may still be relying on paper processes. This difficulty is compounded if facilities within the IHDS are utilizing different systems with varying capabilities and functionality. Organizations must establish the source documents and systems to be used in quality reporting to avoid pulling potentially uncorrected or out-of-date information in downstream systems.[†]

Following source identification, organizations can develop a custom defined report consisting of data extrapolated from the system, and/or they can identify patients electronically and populate a work list of electronic health records that assigned staffs review.

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

Record Completion

Health record deficiencies are defined at the organizational level to reflect compliance with regulatory requirements. For example, most organizations require each entry within a record be signed and include the date and time of the signature. All record completion and deficiency requirements must be outlined in an organization's record completion policies and procedures. Organizations must review and update all record completion and deficiency policies and procedures as new EHR applications are implemented.†

In the paper environment, the record completion process began with assembling large paper charts into folders and ensuring the record was in the correct order and contained all required documentation. Following the assembly processes, clerical staff reviewed every page to flag missing signatures and noted missing documentation. As physicians presented to the HIM department to complete deficiencies, clerical staff reanalyzed charts to ensure signatures were not missed or to pass the chart to another physician. These processes are labor intensive and consume multiple resources including staff time and supplies, such as folders, color codes, and labels. In a hybrid environment, these processes still remain except they must be done in two different mediums to assure all components of the health record are available and complete. This is complicated by the struggle to maintain an accurate matrix of what is in paper and what is in electronic format.

System functionality may create additional challenges. Authors may authenticate an entry into the EHR as they complete it. For example, a radiology report may be authenticated as a final step when it is created. In other instances the authentication process may be separate from the documentation process. For example, when a physician calls a nurse to give a verbal order, the nurse will enter the order into the system and the physician may sign it at a later time. In this latter instance, applying the signature itself requires the physician to log into the system, sign into the electronic signature module, enter his/her unique identifier, and then apply a signature. If the system does not have the capability to prompt, or require, physicians to sign verbal orders upon his/her next entry into the EHR, the signature deficiencies will require continuous manual checks.

Some EHRs include electronic deficiency functionality, but even so checks and balances are needed.[25] This is illustrated in the following case example of a facility with a hybrid record.

> Case example #6:
> A healthcare facility has interfaced dictated/transcribed reports into the EHR, but has not implemented electronic signatures, so the reports must still be printed and signed. The system assigns electronic deficiencies and flags the dictated reports as incomplete. Once the reports are manually signed, a staff member updates the system to remove the deficiency flag. This is a backend process, conducted after discharge in the HIM department with reporting done regularly so follow-up on deficiencies is completed within the required 30 days. In this scenario, a

[25] Wiedemann, Lou Ann. "Completing Charts in EHRs." *Journal of AHIMA* 81, no.1 (January 2010): 40-41.

consultation report dictated on January 2 is subsequently transcribed and interfaced to the EHR on January 3. The report is flagged as deficient on January 3. On February 4 the patient is still "in-house" and the consultation report shows up on the delinquent list in the HIM department because it has exceeded the 30-day requirement for deficiencies to be completed. This back-end process breaks down because the patient is not yet discharged.

As this case example illustrates, the process breaks down when there is an extended patient stay. The systems deficiency functionality is certainly useful, but it can present unique challenges and policies and procedures must be adjusted to accommodate a wide variety of workflows.

An additional challenge is EHR system functionality may vary in different modules creating additional complexity for record completion. For example, electronic signature capabilities may not be implemented for every module. So for instance, the EHR may provide physicians with the ability to electronically enter progress notes; however physicians may still need to apply a manual signature to an electronically created progress note. This creates complex processes as the electronic progress note must be printed, the signature deficiency assigned, and the paper presented to the physician for signature. Errors can occur as clerical staff struggle to understand system functionality and the capability defining which deficiency activities are electronic processes and those that remain manual.

In most EHR systems, some type of oversight is needed to ensure records are complete. The analysis process may transform to managing an error report on outstanding completion prompts that clerical staffs review and correct. For example they might identify a verbal order that has been assigned to the incorrect physician. These deficiencies must be identified and corrected.

To reduce back-end record completion processes, organizations should require all providers to document and sign electronically as new modules are implemented. If the organization allows the physician the opportunity to opt out of the electronic signature application, the HIM department becomes responsible for identifying electronic and manual deficiencies. Maintaining dual processes, one for physicians who utilize electronic signatures and one for physicians who do not, is resource intensive and error prone. Ensuring a complete record in this situation is difficult at best. As they implement EHRs, organizations must define new record completion standards and processes to clearly establish requirements for clinical care providers.[†]

Coding from Hybrid Records

In a hybrid record, data resides in multiple systems thus coding staff struggle to move quickly and efficiently between the systems and paper documentation to find information. Incorrect code assignments can result if the coding professionals cannot find all relevant

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

information. Organizations can assist coding professionals by ensuring coding policies and procedures are current and set realistic accuracy and productivity standards. For example, a policy may require that coders will review all appropriate sources of documentation, whether electronic– or paper-based. But in order for this to be done, the organization must develop, share, and maintain an information inventory indicating clinical documentation source systems and implementation dates. Coding managers may need to evaluate coding accuracy and productivity and adjust benchmarks specifically for the hybrid environment. Some organizations have chosen to provide coders with multiple computer screens and multiple active windows to assist with this challenge. Computer-assisted coding software is implemented by some organizations to automate coding workflow. This technology assists the coding process in locating documentation in multiple systems. For more information refer to AHIMA's Practice Brief "Automated Coding Workflow and CAC Practice Guidance."[26]

[26] AHIMA. "Automated Coding Workflow and CAC Practice Guidance." Journal of AHIMA 81, no.7 (July 2010): 51-56
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_047691.hcsp?dDocName=bok1_047691

Part IV: Best Practices for Information Integrity

Information integrity in the electronic health record (EHR) gives clinical care providers the ability to trust EHR information to make important care decisions. In today's competitive and rapidly changing environment, healthcare organizations need sound information integrity practices that ensure the accuracy, consistency, and reliability of the health information that is needed to support patient safety, quality initiatives, various reporting activities, and patient care across the continuum. As the need to derive meaningful uses from EHRs becomes a higher priority, sound information practices also become increasingly important.

Healthcare organization must ensure a complete health record is produced during the normal course of business and that it represents the legal business record. The following can threaten information integrity in the EHR:

- Lack of cohesive approach to forms automation
- Changes in technology that result in new practices such as electronic signatures
- The need to process amendments, corrections, and deletions
- The need to accommodate late entries or editing
- Conversion of information to printed hard copies due to limitations in print restrictions, printing from multiple systems, or the lack of printing abilities within the system

This section of the paper explores the impact of these challenges on health information management operations and provides best practices for maintaining information integrity specifically for:

- Forms management
- Electronic signatures
- Amendments, corrections, and deletions
- Late entries
- Editing
- Amending transcribed documents
- Printing

Forms Management

One benefit to transitioning from paper-based records to an EHR is the increased efficiency gained through workflow analysis to convert manual processes. Health information technology (HIT) is expected to improve the quality of care by improving the accuracy of patient identification and communication among care providers. The Joint Commission's National Patient Safety Goals state "hospitals should consider implementing a forms automation system early in the process [of EHR adoption]."[27]

[27] HIMSS EMR White Paper available online at http://www.himss.org/content/files/EHR/EMR_FormsWhitePaper.pdf

While many organizations understand the importance of this drive to forms automation, the road map for achieving the optimal solution requires careful consideration and due diligence. Whether the organization expects forms automation to meet the basic needs for a forms repository or the more ambitious goal of a fully integrated enterprise-wide solution, there are a considerable number of technology and document management solutions that can leave an organization with a daunting analysis process. Never-the-less, the development and adherence to standardized forms is critical to the success of implementing an EHR. Fortunately, the development of electronic forms can contribute greatly to the success of transitioning to the EHR.

Healthcare organizations should institute comprehensive forms management protocols during EHR implementation planning, best practices include the following:

- Conduct a comprehensive forms inventory to identify all existing paper or system generated forms that are in use in the organization
- Analyze each form to determine which will be converted to the new EHR system (considering documentation requirements, system functionality, and clinical appropriateness)
- As decisions are made about what to convert, identify guiding principles for how these determinations are made and document these principles so they can be employed throughout the system life cycle
- Ensure the EHR system captures all of the data in the forms that will be converted
- Define and use a standard format organization-wide to develop the converted forms in the new EHR; for example, consistent placement of identifiers and bar codes[†]

Electronic forms management allows organizations to create, manage, and distribute forms that previously were the result of a paper product. Paper forms management processes are extremely costly, and organizations often attempt to reduce costs by simply copying a paper original or limiting the number of approved forms. Electronic forms can eliminate those costs as well as the inefficiencies associated with producing and storing paper documents. Organizations can begin planning for electronic forms during EHR implementation planning by developing a comprehensive paper forms inventory. The subsequent development of standardized electronic forms should be informed by regulatory, state, and federal documentation requirements and by system functionality.

Identifying and managing the number of paper forms that may exist within an organization can be difficult, however it is worthwhile as organizations can be at risk if all forms are not identified and reviewed for clinical appropriateness prior to incorporating them into the EHR. A careful review and analysis of current forms should be done in order to determine which forms will be converted to the electronic format. This effort might begin by preparing a list of all electronic systems currently in use and then identifying all the forms and reports that are generated from these systems. Once that is done, ensure the data captured in existing forms and used in reports will be captured in the EHR. Consider workflow implications during this process, for example

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

determine which forms will no longer need to be multipart following implementation of the EHR. For printed formats, black ink should be required. Colored paper forms and use of Addressograph should be eliminated as early as possible in the migration (due to poor reproducibility).

Organizations must clearly define in policies and procedures how standardized forms are developed, approved, implemented, and maintained in the EHR. A checklist for forms development that reflects the organization's protocols for electronic forms is a useful tool. This checklist will assist the organization in planning the implementation of each electronic form. Whenever possible apply uniform criteria to issues such as:

- The format of forms in both online and printed states,
- Consistent placement of identifiers and bar codes (if used), and
- Standard margin size and font type.

For more details on the elements that must be explored when converting to electronic forms, review AHIMA's publication entitled "Checklist for Assessing HIM Department Readiness and Planning for the EHR."[28]

Electronic Signatures

A fully functioning EHR system should provide the ability to sign entries electronically. Historically the act of signing an entry was referred to as "authentication." However, in the new world of HIT, authentication is the security process of verifying the user's identity within the system and authorizing that the user has permissions to access the system. This IT authentication within the EHR is an important function because it defines and assigns responsibilities regarding the entries an end user can create, modify, or view.

Functionality to support electronic signatures varies in EHR systems. As such, the management of electronic signatures may be as diverse as the number of systems available in the healthcare market. Therefore, it is important to fully explore system capability regarding electronic signature functionality as well as the associated security measures. In addition, healthcare organizations must ensure that all medical staff members receive sufficient training and education on electronic signature functionality, prior to being granted access to the application.[†]

Healthcare organizations may choose to implement e-signature functionality in each independent system, which could include document management systems, transcription systems, and individual modules of the EHR. This application of e-signatures has been a source of confusion because system functionality often behaves differently. For each system, the organization should ensure the e-signature application is compliant with state

[28] AHIMA HIM Practice Transformation Work Group. "A Checklist for Assessing HIM Department Readiness and Planning for the EHR." Journal of AHIMA 76, no.6 (June 2005): 56E-H. Available in the AHIMA Body of Knowledge at: http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_027353.hcsp?dDocName=bok1_027353

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

and/or federal rules. Currently, there is no single accepted standard, law, or regulation specific to e-signatures, attestation, and authorship of patient information in an EHR, and unfortunately, sometimes these sources are contradictory.

Healthcare organizations must identify and review all applicable rules and regulations pertaining to electronic signatures to ensure their practices are compliant. E-signature policies and procedures should address issues such as multiple or dual signatures, proxy signatures, auto-attestation functionality, and batch signing.[†29] HIM professionals can consult state and federal signature requirements to ensure each entry within the health record has the proper authorship and signature. For example, if the organization is a teaching facility the hospital medical staff bylaws may require both the resident and attending faculty to sign entries. In this instance, the HIM professional should ensure each system's e-signature application is capable of this functionality before it is deployed.

Healthcare organizations must identify and review all applicable rules and regulations pertaining to electronic signatures to ensure their practices are compliant. E-signature policies and procedures should address issues such as multiple or dual signatures, proxy signatures, auto-attestation, and batch signing.

As noted earlier in this paper (in Part III on hybrid record completion) the organization must ensure each patient has a health record completed within state, federal, or organizational specific time frames. Simply implementing e-signature does not ensure each entry is dated, timed, and signed within the acceptable time limit. System functionality, such as allowing physicians to over-ride or "skip" the e-signature application, can result in record deficiencies. These deficiencies must be completed in the acceptable time frame in order to ensure a completed health record is available for each patient.

For more information and organizational guidance on electronic signatures refer to the AHIMA practice brief entitled "Electronic Signature, Attestation, and Authorship."[30]

Amendments, Corrections, and Deletions

As organization's transition to EHRs traditional information documentation practices must also transition. For instance in the paper record, amendments were typically attached to transcribed reports, and corrections and deletions were managed with a single-line strike-through on the original documentation. However, these practices do not work the same way in an electronic environment. Healthcare organizations must define policies for making amendments, corrections, deletions, and/or retractions to

[29] "Electronic Signature, Attestation, and Authorship. Appendix B: Laws, Regulations, and Electronic Signature Acts." *Journal of AHIMA* 80, no.11 (November–December 2009).
[30] AHIMA e-HIM Workgroup: Best Practices for Electronic Signature and Attestation. "Electronic Signature, Attestation, and Authorship (Updated)." *Journal of AHIMA* 80, no.11 (November-December 2009): expanded online edition. Available in AHIMA Body of Knowledge (BoK) at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045551.hcsp?dDocName=bok1_045551 .

documentation that has already been final signed in the EHR and procedures may need to be defined for each EHR application. Policy should require that, once a document has been final signed, it must remain locked from further revisions and a new entry must be made, with a separate signature, date, and time added to the electronic record. Other issues to address in organizational policy and procedures include:

- Location of an amendment within the original document (for example, at the top or bottom of the entry)
- System processes for changing information that has been authenticated by the author
- How to distinguish between the original and edited text (for example, different color or font)
- Acceptable usages of deletions or retractions

As noted earlier in the EHR management and use section of this paper, information integrity can be compromised when retrospective changes are made to documentation. (Refer to Table 1, Options for managing corrected information across interfaces.) Thus this process must be managed carefully to ensure integrated systems remain synchronized. System functionality that explicitly identifies edited text, namely some sort of versioning, will facilitate this process. For more information on managing these functionalities within the EHR refer to AHIMA's Amendment, Corrections and Deletions Toolkit.[31]

Late Entries

Documentation that is entered after the point of care may be considered a "late entry." However, generally this concept of late entries applies to time sensitive documentation that can get out of sequence. For example, a progress note entered the day after a physician treats the patient, or a nursing note that is entered at the end of the shift are late entries. Dictated reports or summaries, such as a history and physical or a discharge summary, may be attached to the electronic record after the exam or discharge date in this example, but would not be considered a late entry.

Late entries in the EHR environment are problematic because care is rendered prior to the addition of the late entry to the health record. An assumed benefit of the EHR is that it speeds communication between clinical care providers, meaning as soon as documentation is entered into the record it is available to others. However, late entries may not be available when needed. This could adversely affect patient care and have serious liability ramifications for the organization. The following case scenario illustrates the problem:

> Case Example #7:
> A nurse fails to document a patient's allergy to Penicillin during the admission assessment. Following admission, a chest x-ray reveals pneumonia so the

[31]Amendments, Corrections, and Deletions in the Electronic Health Record: an American Health Information Management Association Toolkit available in AHIMA Body of Knowledge at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_044678.hcsp?dDocName=bok1_044678.

attending physician uses the CPOE system to order Penicillin. The EHR does not alert the physician to the Penicillin allergy because the nurse has not yet entered that allergy at the time the doctor is entering the order. The order is filled and the patient receives an initial dose of Penicillin. Subsequently, the nurse enters the allergy information at the end of her shift.

This case scenario could result in harm to the patient and potentially serious legal liability to the healthcare organization. Time sensitive, sequential documentation should be captured as close to the point of care as possible.

The healthcare organization's policy must define the acceptable period of time allowed for end users to document in the record (in hours or days). Furthermore, policies and procedures should address how a late entry is made within the EHR. Late entries must be clearly labeled and must contain current date, time, and authorized signature. Backdating the signature, date, or time must not be allowed.[†] Furthermore, organizations should outline in policy who is authorized to make late entries in the EHR and identify situations in which late entries are not allowed.

Editing

Editing entries in the EHR is the act of changing documentation prior to applying a final signature. This functionality is typically available in every application within the EHR, including progress notes, physician orders, nursing assessment, respiratory therapy care notes, or x-ray reports. For version control purposes, organizations should have a clear understanding of how the editing process works in their system. Organizations must address documentation issues that occur when information within the system has been altered and identify if information edits are included in system version control.

As organizations understand the edit functionality further, end user training, education, and requirements can be developed. Because edit functionality can assist organizations in promoting the need to document at the point of care, organizations should clearly define that each end user is responsible for editing their own entries. In addition, organizational policy must clearly establish that once the end user has applied a final signature to a document in the EHR no further editing of that documentation is allowed. Once a final signature is applied, any changes are an amendment to the record.[†]

As noted in Part I of this paper, multiple interfaces within the EHR add complexity to managing editing and version control. For example, consider a case where transcribed x-ray reports are typed in a transcription system which is then interfaced with the EHR. If the radiologist identifies an error in a report prior to the application of his electronic signature, which system is the edit corrected in? The organization must clearly define the source system for each documentation application so end users know the appropriate

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.
[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

system in which to enter corrections. The organization should also define how edits may affect report distribution, in order to mitigate the risk of disclosing inaccurate information.†

Amending Transcribed Reports

Transcribed reports have historically been a part of the health record. The manual transcription process typically involves the following sequential steps:

1. Clinical care providers dictate reports, often lengthy such as an operative note for example, into a dictation system.
2. Transcriptionists listen to the dictation and create the free text report or document.
3. The report is filed in the corresponding patient's health record and copies are distributed to the dictator and perhaps other care providers as directed.
4. The provider who dictated the report reviews and signs it (either electronically or on paper).

Some organizations continue to utilize transcription software as a step in the transition to a full EHR. The decision to continue the use of transcribed documents in an EHR is up to each organization. Organizations may currently have policies and procedures in place to address amendments or corrections to transcribed printed reports. These policies and procedures will need to be adjusted to accommodate electronic signatures. In addition, as the EHR implementation allows physicians to enter more and more information directly and dictation decreases, the workflow and processes will likely need to be further adjusted.

Organizations with a health record that contains both direct data entry and transcribed reports may encounter additional information integrity risks. End users may have different connotations for the terms *amendments*, *corrections*, or *deletions* and they may associate these terms with different processes for correcting information entered directly verses transcribed reports. Therefore, organizations must have clearly defined policies and procedures for these practices to ensure the integrity of the information remains intact. Best practices in amending transcribed reports include standardizing the location of additional documentation in each report type, clearly identifying new documentation, and requiring a separate signature, date, and time for corrected portions of the documentation.†As noted in the Editing section, once a transcribed report has been signed by the provider, it should be locked from any further editing.

The report distribution process for transcribed documents also poses an information integrity risk. Once a document has been transcribed, many systems have the functionality to fax or automatically send the draft report to authorized individuals and this is commonly done to share information for follow-up care. There can be significant ramifications however if a shared draft is later revised significantly and is not communicated. At best, a receiving provider may be confused if different versions of a document are sent with no indication of which is the corrected version. To mitigate risk

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

in report distribution, organizations should define how amended transcribed reports will be redistributed to requestors or if the practice of distributing transcribed reports prior to final signature will be allowed. For more information on amendments, corrections, and deletions of transcribed reports within the EHR and their distribution, refer to AHIMA's Amendments, Corrections, and Deletions in Transcribed Reports Toolkit.[32]

Printing

Paper records are more than just out of date, they are tremendously expensive. Although there are many organizations and providers within the healthcare industry with paper records, recent industry activities such as the American Recovery and Reinvestment Act (ARRA) of 2009, have placed a high priority on converting paper records to electronic. According to the Office of the National Coordinator for Health Information Technology, the healthcare industry could save an estimated $300 billion each year by eliminating paper.[33] Healthcare costs and the need to increase the quality of healthcare will continue to drive EHR adoption. Information integrity issues that arise as a result of printing EHR information will continue to shape and influence organizational policies and procedures.

With the use of an EHR, where information begins electronically and is maintained that way, the use and storage of paper should decrease. However, many organizations do not experience this; paper can actually increase depending on how much printing is done. One reason for this is because it is often difficult for end users to give up the hard copies of patient information. However, continued use of paper after EHR implementation poses significant risks to information integrity. Organizations should limit printing from the EHR as much as possible and clearly define policies for print restrictions for EHR users.[†] Such policies must meet all federal and state requirements (for example, HIPAA) and should coincide with protected health information (PHI) user group accessibility, level of privileges, and system audit trail capabilities.

The organization should work with system vendors to ensure system print functionality is reviewed and discussed prior to EHR implementation. Early in the implementation process, the organizations should conduct an analysis of paper workflows to determine how best to convert to electronic processes and begin to discuss print restriction policies to support information integrity.[†]

During the transition to a new system, EHR module, or application, some organizations choose to operate both electronic and paper processes to ensure information is flowing in an appropriate manner. When this is done, paper increases, so electronic efficiencies are not realized, and if this continues, information integrity is at risk. Organizations considering this approach must institute controls to ensure printing is discontinued once it is verified that the new system is working properly. For example, if the organization is

---

[32] Electronic Signature, Attestation, and Authorship. Appendix E: Amendments, Corrections, and Deletions in Transcribed Reports Toolkit available online in AHIMA Body of Knowledge at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045548.pdf.

[33] "Electronic Health Records: What's taking so long?" www.time.com, March, 2009.

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

implementing computerized physician order entry (CPOE), physicians will begin to enter orders in the electronic module. In order to verify CPOE system interfaces, staff may temporarily print the electronic order and double check this printed order to confirm the order crossed the interface correctly and was processed by the relevant ancillary department. Once verified, the printed order is destroyed. The extra steps in this example are an implementation mechanism and thus should be time constrained (for example, limited to one week) and printed orders should be included in the legal health record, as evidence of the double check mechanism.

Organizations encounter further challenges associated with printing electronic information once the initial EHR implementation period has passed. An assumed benefit with EHR implementation may be to decrease the size of paper records and the overall consumption of paper, toner, and record folders. Without clear print restrictions and access policies an organization may find these benefits are not realized. In addition, as end users continue to use or obtain clinical information from printed documents, rather than the electronic system, many benefits associated with the EHR system may not be realized. For example, if physicians routinely print information for review, rather than interacting directly with the EHR, they will not see system alerts and prompts. For instance, the EHR may show an alert prompting the physician to change the patient's medication if the CPOE module is integrated with laboratory data. But if the physician continues to review lab results in printed format, he/she would miss both the alert for an abnormal laboratory result and the medication alert.

The management of information printed from the EHR directly affects the integrity of the health record. How print information has been used will determine how it is later managed. Information that is printed from the EHR and has not been written on must be properly destroyed.[†] The organization should ensure it will be discarded in accordance with hospital policy and in compliance with HIPAA guidelines (for example, shredded immediately).

Printed information that has been written on by a clinical provider may need to become part of the legal health record. For example, if a physician prints a laboratory report, and then writes his/her conclusions or decisions on the hard copy report, policies and procedures must address what to do with this annotated print-out. The organization must establish a procedure for how to include this type of additional documentation in the EHR so other clinical providers have the information when making further patient care decisions.

Lack of such protocol can lead to a "nightmare because you don't know whether someone printed out [a piece of the record] and wrote on it, and if they did, where it is," says industry expert Margret Amatayakul, RHIA, CHPS, CPHIT, CPEHR, FHIMSS.[34]

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

[34] Rollins, Gina. "Printing Electronic Records: Managing the Hassle and the Risk." *Journal of AHIMA* 78, no.5 (May 2007): 36-40.

Organizations that allow printing from the EHR must clearly define in policy and procedure how staff will treat print outs that are written on, and they must further identify how that information will be included in the health record (for example, as an amendment or as a new note).[†] Furthermore, they must set system parameters to ensure printed information includes a header or footer identifying the user, print location, date, and time that the information was printed.[†]

Depending on system functionality, the EHR may or may not meet the requirements to serve as the legal health record. Often the health record consists of a hybrid with both electronic and paper information. At some point (typically after discharge for acute care patients) the information from various applications and in various media is brought together to form the legal health record. When an organization is managing the health record in both paper and electronic media, the organization must define how these electronic and paper media come together to create a centralized, complete health record.

Today, organizations with a hybrid record may still find it necessary to print the electronic portions and capture the legal health record in paper form. If printing is intended, an organization must ensure there is sufficient system functionality to allow it. For example, there may be limitations in the number of licenses for printing, formatting issues when converting an electronic document to paper for printing, and the inability to print all modules with a single key stroke. Furthermore, organizations who determine that the legal health record will be a paper record generated at discharge, must define how and when printing will occur. For example, system report queries can be developed internally to identify patients who have a discharge status at midnight. Once an account is identified as discharged, the system can be set up to automatically print all electronically generated information to a specific printer. In this instance, policies and procedures must be defined to standardize how the information will be printed and merged, including who is responsible for ensuring information integrity.

When an EHR is comprised of multiple interfaced systems, printing independently from each system is inherently risky, prone to human error, and should only occur with strict organizational policy and procedures in place to monitor the practice. One reason for this risk is because systems have varying implementation dates, which means that determining when information was generated in paper verses electronic will vary in each system. The following example illustrates this difficulty:

> Case Example #8:
> On January 1, a laboratory system is implemented via system A. On March 1, a radiology module is implemented via system B and on June 1, a nursing education module is implemented via system C. The source information for the legal health record of an inpatient stay with dates of service from February 26 through March 3 includes the following:
>
> - Laboratory information for the whole stay printed from system A
> - Radiology information in paper from February 26 through February 28
> - Radiology information printed from system B for any radiology test in March

- Nursing education information in paper

As this example illustrates, the source of information may be different for each patient, based on the system conversion dates and the patient's dates of service.[35] As described further in the next section on information sharing, the organization must establish a thorough information inventory that identifies the source system and date of conversion for every system, application, and module that generates patient health information. It must document all subsequent additions or changes, including the date an information source transitioned from paper to electronic.[†] Printing information from one of these systems, if it is not the source system for that information, can lead to inconsistent versions of information risking patient safety.

Organizations should keep in mind that for the most part, EHR systems were not designed to be a paper-based product. They were designed to be created, viewed, and maintained electronically. The decision to print this information could turn into a costly endeavor. Electronic documentation can look wonderful and concise on the screen, however the printed format may be almost unrecognizable. In addition, printing from an electronic system can increase chart size. A paper-based emergency department record that historically was 25 pages long can turn into a 150 page document when printed from an EHR. This can have long term consequences such as increased costs associated with copiers, toners, folders, color coding, and record storage fees.

An alternative to printing the electronic portion is to scan the paper portion and eliminate the paper, thus creating a complete electronic record. A document management system can be used to accomplish this and create a digital legal health record that consists of scanned paper documents with electronic interfaced data. Regardless of which approach is taken, in defining the legal health record the organization must define what information created electronically will remain electronic and what will be printed, if anything.

[35] Nunn, Sandra. "Managing Source System Content in the EHR." *Journal of AHIMA* 79, no.3 (March 2008): 60–61.
[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

Part V: Sharing Health Information

The exchange of health information is an essential function in every healthcare provider organization. Maintaining the privacy and security of information during this process is critical. The information contained in the electronic health record (EHR) should be complete and timely to support the continuum of care.

In addition to traditional practices such copying paper records for release of information (ROI) the health information exchange (HIE) landscape has changed dramatically. Both technology advances and the call for increased EHR adoptions will further efforts in information exchange in the coming years. "A fully longitudinal health record that follows the patient throughout the healthcare continuum will provide clinicians an opportunity to improve patient care."[36] The integrity of the information that is shared is no less critical. For more information refer to AHIMA's Practice Briefs on "Understanding the HIE Landscape, Reconciling and Managing EMPIs,[37] and Managing the Integrity of Patient Identity in Health Information Exchange."[38]
The ROI function in the paper environment is a time consuming manual process that includes logging of requests, physically locating a paper record, copying the record a page at a time on a copy machine, manually completing the request in the ROI application, and mailing the copies. From start to finish in a paper record environment this process can take several days. In the EHR, information integrity becomes a primary concern as disparate systems are utilized for disclosing health information. Although the information may originate from disparate systems, organizations may want to consider benefits to centralizing the ROI function when patient information is electronic. This allows the organization to be responsive and adhere to new requirements such as controlling access, maintaining an accounting of disclosures, and complying with request for restrictions.

This section of the paper addresses issues and challenges in maintaining a legal health record and managing the multiple locations of information within the organization as well as the process of releasing information itself. For more information on managing ROI functions, review the AHIMA practice brief entitled Management Practices for the Release of Information.[39]

---

[36] AHIMA. "Understanding the HIE Landscape." *Journal of AHIMA* 81, no.9 (September 2010): 60-65.
[37] AHIMA. "Reconciling and Managing EMPIs (Updated)." *Journal of AHIMA* 81, no.4 (April 2010): 52-57. Available in the AHIMA Body of Knowledge at:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_046942.hcsp?dDocName=bok1_046942
[38] AHIMA. "Managing the Integrity of Patient Identity in Health Information Exchange " *Journal of AHIMA* 80, no.7 (July 2009): 62-69. Available in the AHIMA Body of Knowledge at:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_044000.hcsp?dDocName=bok1_044000
[39]Bock, Linda J.; Demster, Barbara; Dinh, Angela K.; Gorton, Elisa R.; Lantis, James R., Jr. "Management Practices for the Release of Information" *Journal of AHIMA* 79, no.11 (November–December 2008): 77-80. Available in the AHIMA Body of Knowledge at:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_040788.hcsp?dDocName=bok1_040788

Sharing Transcribed Reports

Workflow analysis is critical as the organization transitions to an EHR. At each step during the transition, system functionality may provide opportunities to improve processes. For example, as transcription functionality is implemented it may provide the organization an opportunity to discontinue printing hard copies of reports mailed to dictating or referring physicians. In the paper world, this process is very time consuming as dictators routinely receive a copy of all of their reports and they commonly request additional copies for referring physicians. Improvement in this workflow is significant if the organization takes advantage of transcription system functionality that allows a transcriptionist to automatically fax transcribed reports to physicians. Costs for staff handling of reports, paper, envelopes, and postage can be eliminated.

Additional improvements in this workflow may be realized if the transcription module is interfaced with the EHR. As reports are transcribed they may be electronically transmitted to the EHR. This allows physicians to view transcribed reports online so they would no longer need printed or faxed copies. These workflow improvement opportunities are dependent on system functionality. This is another example why it is important for healthcare organizations to fully understand EHR system functionality and ensure it is used to achieve optimal performance.

Release of Information in the EHR

Even in a fully functioning EHR environment, the release of information process requires oversight and careful management to ensure:

- HIPAA privacy rules regarding minimum necessary are met,
- Authorizations are valid, and
- Correct information is replicated (either on CD or on paper) from the source system(s).

When a written request for information is received, it must be reviewed to ensure it is appropriate before EHR information is released. For example, a staff member who is knowledgeable of confidentiality, privacy, and security requirements must verify the requestor has the authority to make the request. And it is important to verifying the correct identity of the patient information to be shared. Finding the balance between information integrity, privacy, legal compliance, and facilitating quality patient care through information sharing can be a challenge. Hybrid records make this even more challenging.

Health information is shared outside of the provider facility for a variety of activities including continuing care, submitting claims for payments, applying for health or life insurance benefits, and litigation. Depending on the purpose for the request, errors in the release of information process may delay care, delay benefits, or increase liability for example. Risk of error in the release of information process can increase as information is moved from a paper based system to an EHR where portions of the health record may be located in separate systems and may have varying implementation schedules. As noted

earlier in the best practices for printing section of this paper, printing or copying from multiple information sources is inherently error prone and risky[40] and the need for a thorough information inventory was explained. As EHR modules are implemented, the organization must track and document all changes to maintain the information inventory, including the date of any transition of an information source from paper to electronic. The following case example was reviewed earlier (see case example #7) to underscore the need for an information inventory. Here, the same example illustrates the challenge for accurate release of information.

> Case Example #9:
> A healthcare organization with the following implementation schedule determined that printing of hard copy reports will discontinue on the implementation date, as each application is implemented. On January 1, a laboratory system is implemented (EHR module A). On March 1, a radiology module is implemented (module B) and on June 1, a nursing education module is implemented (module C).

In this case example, to accurately fulfill a request for information regarding an inpatient stay from February 26 through March 3 a staff member would need to do the following:

- Print any existing laboratory information from EHR module A
- Photocopy any paper radiology reports for dates of service in February
- Print any radiology reports for the dates of service from March 1 through March 3 from module B
- Photocopy paper nursing education information
- And such

In this example, there would be no need to check EHR module C for information on this patient because the patient was discharged before that module was implemented. As this case example illustrates, it is critical that staff who fulfill information requests be made familiar with all necessary EHR modules and be trained on how to locate the correct source of information within them.[†] For example, within the lab module there might be different steps involved to locate different types of laboratory reports.

Patient Portals

Patient portals or kiosks allow patients to request information without physically going to a department within the healthcare facility; thus automating the request process. Depending on system functionality, organizations can define required fields (such as the date of service, what specific information is needed, and the length of authorization) in the automated request application. This information integrity mechanism, similar to

---

[40] Note: At the time this toolkit was developed, the ARRA requirements for electronic access to health information were not yet established and thus are not addressed here. Access to electronic health information under ARRA is expected to require organizations with an EHR to produce requests for information in electronic format, for example, encrypted disc. Additional risks could be identified based on ARRA's requirement. For the latest information on ARRA visit AHIMA's ARRA resource page.

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

required structured data entry fields discussed earlier, helps ensure an authorization is complete and includes all required elements.

A key step prior to implementing patient portals is to address a mechanism for signature verification. This process can be cumbersome if staff must verify an electronic signature via a patient portal with a manual signature that was obtained previously. To mitigate this issue, organizations should clearly define what constitutes an acceptable signature prior to implementation. Further benefits to the ROI process can be seen when the organization transitions to a fully integrated EHR that allows information to be shared in electronic media, such as a DVD, instead of presenting paper documents to the requestor.

Designated Record Set

The designated record set (DRS) is a group of records maintained by or for a covered entity that is the medical and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; information used in whole or in part by or for the HIPAA covered entity to make decisions about individuals.[41] The DRS is not the same as the legal health record, discussed earlier in the EHR management and use section of this paper. Both identify a specific set of information that must be disclosed upon request. However, organizations use the DRS when responding to most ROI requests, or disclosures. These would include disclosures to patients, families, clinicians, or third party payers for example. In contrast, the legal health record (LHR) is used primarily in response to legal requests, such as subpoenas. The LHR is a subset of HIPAA's required DRS. To better understand the distinction between the two, read AHIMA's practice brief "Defining and Disclosing the Designated Record Set and the Legal Health Record."[42]

Understanding the difference between the DRS and the LHR can be confusing. The designated record set is used to clarify the access and amendment rights by individuals under the HIPAA standards and would include records such as superbills, remittance advices, and case management notes. The LHR serves to identify what information constitutes the official business record of an organization for evidentiary purposes, typically used when responding to formal requests for information for legal purposes and would include records such as history and physicals, physician orders and nursing notes. Without a clear distinction between the DRS and LHR, an organization risks producing records for legal purposes that are not complete or do not meet the intent of a subpoena for example. Healthcare organizations must explicitly define both the DRS and the LHR, and understand the distinct purpose of each. In addition, the organization should provide staff with training on the differences between the two sets and define the instances in which each should be released.[†]

---

[41] Servais, Cheryl E. *The Legal Health Record*. Chicago, IL: AHIMA, 2008.
[42] Dougherty, Michelle; Washington, Lydia. "Defining and Disclosing the Designated Record Set and the Legal Health Record." *Journal of AHIMA* 79, no.4 (April 2008): 65–68. Available in the AHIMA Body of Knowledge at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_037468.hcsp?dDocName=bok1_037468
[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

E-Discovery

For most requests for information, either the DRS or LHR is disclosed. However, under E-Discovery all information requested by the court must be provided. E-Discovery refers to any process in which electronic data and metadata are sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. Once, it was believed that E-Discovery was not applicable in healthcare, however case law has since indicated that it does apply to healthcare organizations and practitioners. E-Discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government-sanctioned hacking, also called forensic investigation, of both electronic information and metadata for the purpose of obtaining critical evidence is also a type of E-Discovery.

The nature of digital data and EHR systems makes them extremely well-suited to forensic investigation. Digital data can be electronically searched with ease, whereas paper documents must be scrutinized manually. Furthermore, digital data are difficult or impossible to completely destroy, particularly in a network. This is because the data appears on multiple hard drives and because digital files, even if deleted, can be restored. In fact, the only reliable way to destroy a computer file is to physically destroy every hard drive where the file has been stored. E-Discovery is an evolving field that goes far beyond mere technology. It gives rise to multiple legal, constitutional, political, and personal privacy and security issues, many of which have yet to be resolved.[43]

The role of the records custodian is a pivotal role in litigation and the HIM professional must be able to testify that the health record, whether generated in a hybrid or electronic environment, was created during the normal course of business.[44] As such, the HIM professional must have an understanding of the organization's EHR, including the functional capabilities and efforts related to preserving the integrity of the health record. Organizations have a duty to preserve information. Thus they must comply with E-Discovery processes, including implementing a legal hold and retention of information. The organization must be able to comply with E-discovery, regardless of the number of integrated EHR systems, modules, or applications.

Organizations will be at risk during E-Discovery if appropriate policies and procedures are not in place to support and maintain an E-Discovery management plan. The Federal Rules of Civil Procedure contain explicit instructions and requirements for producing electronically stored information (ESI). These rules apply to federal civil cases, including healthcare litigation.[45] Organizations are at risk of receiving punitive damages, increased legal fees, and unfavorable court rulings if these requirements are not met. For more

[43] Definition available online at http://searchfinancialsecurity.techtarget.com/sDefinition/0,,sid185_gci1150017,00.html
[44] Washington, Lydia. "From Custodian to Steward: Evolving Roles in the E-HIM Transition." *Journal of AHIMA* 81, no.5 (May 2010): 42-43.
[45] Federal Rules of Civil Procedure (2009): http://www.law.cornell.edu/rules/frcp/

information on E-Discovery, refer to AHIMA's practice brief entitled "The New Electronic Discovery Civil Rule."[46]

The records management program will provide the organization with the foundation for an effective E-Discovery management program.[47] Traditional records management life cycle activities include the creation, distribution, storage, retention, and preservation of information in a manner that allows for information to be retrieved, searched, and produced. Organizations should develop policies to preserve ESI in a collaborative approach that includes representation from Legal Services, IT, HIM, Risk Management, and Senior Leadership. During this process IT should provide education regarding the fundamental system functionality employed for data storage and retrieval, HIM should provide education on record retention requirements and LHR definitions, and Risk Management should provide basic organizational strategies for litigation response coordination. The organization must develop an E-Discovery management plan that includes a legal hold policy, a litigation communication plan, the functional ability to "lock" the EHR and discontinue destruction of information, assurance that the duty to preserve is met, and a clear definition of the LHR.[†]

Closing

Quality patient care depends in part on the availability and quality of patient information. Information in the health record should clearly and concisely relay the full story of the care a person receives. Sound information management practices are required to achieve this. An effective EHR implementation should provide a positive impact on the quality of care, patient safety initiatives, and further organizational efficiencies. Once an EHR is implemented, how information is captured, how interfaces are managed, and many other practices will determine whether healthcare providers can in fact trust the information contained in the EHR to help them deliver quality care. This paper provides best practices to ensure information integrity in the course of using and managing an EHR system, whether fully electronic or in a hybrid state, and covers practices for multiple processes from capturing information all the way through the continuum to sharing information.

Information integrity in the EHR gives clinical care providers the ability to trust EHR information to make important care decisions. In today's competitive and rapidly changing environment, healthcare organizations need sound information integrity practices that ensure the accuracy, consistency, and reliability of the health information that is needed to support patient safety, quality initiatives, various reporting activities, and patient care across the continuum. As the need to derive meaningful use from EHRs becomes a higher priority, sound information practices also become increasingly important. It is hoped the best practices presented here, will be used to attain this goal.

---

[46] AHIMA e-HIM Work Group on e-Discovery. "New Electronic Discovery Civil Rule." *Journal of AHIMA* 77, no.8 (September 2006): 68A-H. Available online AHIMA Body of Knowledge (BoK) at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031860.hcsp?dDocName=bok1_031860 .

[47] Reich, Kimberly Baldwin-Stried. "Developing a Litigation Response Plan." *Journal of AHIMA* 78, no.9 (October 2007): 76–78,86.

[†] Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium at http://compendium.ahima.org.

Additional Resources

AHIMA E-Discovery Task Force. "Litigation Response Planning and Policies for E-Discovery." *Journal of AHIMA* 79, no.2 (February 2008): 69–75

AHIMA e-HIM Work Group on E-Discovery. “The New Electronic Discovery Civil Rule.” *Journal of AHIMA* 77, no. 8 (September 2006): 68A–H.

AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." *Journal of AHIMA* 76, no.8 (September 2005): 64A–G.

AHIMA e-HIM® Work Group on EHR Data Content. “Data Standard Time: Data Content Standardization and the HIM Role.” *Journal of AHIMA* 77, no. 2 (February 2006): 26–32.

AHIMA e-HIM Work Group on Health Information in a Hybrid Environment. “The Complete Medical Record in a Hybrid EHR Environment. Part II: Managing Access and Disclosure. AHIMA Practice Brief. (October 2003).

AHIMA HIM Practice Transformation Work Group. "A Checklist for Assessing HIM Department Readiness and Planning for the EHR." *Journal of AHIMA* 76, no.6 (June 2005): 56E-H.

AHIMA Work Group on Electronic Health Records Management. “The Strategic Importance of Electronic Health Records Management.” *Journal of AHIMA* 75, no. 9 (October 2004): 80A–B.

AHIMA. “Quality Healthcare Data and Information.” Position statement. October 2006. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Amatayakul, Margret “Are you using an EHR really? Electronic health records can support patient care cost-effectively but only if they're used as intended.” *Healthcare Financial Management* (Nov. 2005).

Brandwein, Aaron. “Defining the Legal Medical Record in a Hybrid World While Staying Sane, Too” *Advance for HIM Professionals*. (Aug. 2008)

Centers for Medicare and Medicaid Services. “Conditions of Participation for Hospitals.” Available online at www.cms.hhs.gov/manuals/107_som/som107ap_a_hospitals.pdf.

Committee on Data Standards for Patient Safety. *Key Capabilities of an Electronic Health Record System: Letter Report*. Board on Healthcare Services and Institute of Medicine. Available online at http://newton.nap.edu/catalog/10781.html.

Connecting for Health. “Background Issues on Data Quality.” April 2006. Available online at www.connectingforhealth.org/commonframework/docs/T5_Background_Issues_Data.pdf.

"Developing a Legal Health Record Policy: Appendix A." *Journal of AHIMA* 78, no. 9 (October 2007): web extra

Dimick, Chris. "Charting the Legal Health Record." *Journal of AHIMA* 78, no.5 (May 2007): 30.

Dimick, Chris. "Record Limbo: Hybrid Systems Add Burden and Risk to Data Reporting" *Journal of AHIMA* 79, no.11 (November–December 2008): 28–32.

Dougherty, Michelle; Washington, Lydia. "Defining and Disclosing the Designated Record Set and the Legal Health Record." *Journal of AHIMA* 79, no.4 (April 2008): 65–68.

Fernandes, Lorraine, and Michelle O’Connor. “The Future of Patient Identification.” *Journal of AHIMA* 77, no. 1 (January 2006): 36–40.

Health Level Seven. “The Legal Aspects of the Electronic Health Record.” Unpublished work product of the HL7 work group on legal aspects of the EHR. May 2005.

Heubusch, Kevin. "Coding’s Biggest Challenges Today."*Journal of AHIMA* 79, no.7 (July 2008): 24–28.

HIMSS. “HIMSS Electronic Health Record Definitional Model, Version 1.1.” Available online at www.himss.org/content/files/ehrattributes070703.pdf.

“Hybrid Medical Records: Reality and Risks for Today.” By Aaron Brandwein, VP HealthPort EDMS and Jason Barnhouse, VP Document Management. 18th Annual HIMSS Leadership Survey, 2007.

Kohn, Linda T., et al., eds. *To Err is Human: Building a Safer Health System*. Institute of Medicine. Available online at http://newton.nap.edu/catalog/9728.html.

Reino, Linda; Hyde, Cynthia. "From Paper to Electronic, and In Between: the Challenges Hospitals Face with the Hybrid Record." AHIMA's 78th National Convention and Exhibit Proceedings, October 2006.

Rollins, Gina. "Following the Digital Trail: Weak Auditing Functions Spell Trouble for an Electronic Record." *Journal of AHIMA* 77, no.3 (March 2006): 38–41.
Rollins, Gina. "Printing Electronic Records: Managing the Hassle and the Risk." *Journal of AHIMA* 78, no.5 (May 2007): 36–40.

“Standards for Privacy of Individually Identifiable Health Information; Final Rule.” 45 CFR Part 164.501. *Federal Register* 65, no. 250 (2003). Available online at www.hhs.gov/ocr/hipaa.

Trites, Patricia. "Metadata You Need: Determining What Must Be Collected and Retained." *Journal of AHIMA* 79, no.7 (July 2008): 52–53, 60.

Wiedemann, Lou Ann. "Completing Charts in EHRs." *Journal of AHIMA* 81, no.1 (January 2010): 40–41.

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.