EHRs as the Business and Legal Records of Healthcare Organizations. Appendix A: Issues in Electronic Health Record Management (2010 update)

Save to myBoK

Electronic health record management (EHRM) is the process by which electronic (e.g., digital) health records are created or received and preserved for legal or business purposes. EHRM requires decision making throughout the EHR's life cycle-through the processing, distribution, maintenance, storage, and retrieval of the health record to its ultimate disposition, including archiving or destruction. The scope of EHRM must include a determination of which EHRs to retain and for how long, the assignment of authorities and responsibilities, the design and administration of the process, the integrity of the data, the audit and review of the performance of those processes, how that data are protected and secured (data at rest, data in transit), and management of health information exchange.

Document and Record Management

Record Order		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Written policy identifies the reports that make up each record type (e.g., inpatient, emergency room) and the specific document order in the chart. HIM staff members ensure the chart is in the order specified in the supporting procedure before filing.	Written policies specify which reports and documents make up the legal health record as defined by the organization. The policies identify which reports are paper and which are electronic. As the need to print and assemble paper-based records diminishes, HIM management must transfer or retrain staff to work in other operational areas (e.g., assembly clerks might be trained to perform document preparation or scanning if imaging has been deployed). When the EHR is printed, a standardized chart order must be developed based on the user's needs (e.g., different EHR views may necessitate different assembly order for lawyers and patients).	Record order may continue to be important to HIM once a totally electronic format is achieved. If scanning documents continues to be part of the EHR, the processing of the documents before scanning, indexing, display, storing, and destruction will be an essential function. Format and access should be defined according to the information system chosen and the user's need for protected health information (PHI) relative to his or her job for both display and print capabilities. When the EHR must be printed, a standardized chart order based on the user's needs must be developed (e.g., different EHR views may necessitate different assembly order for lawyers and patients). Develop print groups of the record that are printed out when a paper medical record is needed.

Workflow Changes		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Written policies list the reports required to signify the record is complete and ready for purposes such as coding, release of information (ROI), and meeting the organization's legal definition. Staff members follow written procedures to review each	Consider electronic rules and alerts on ROI requirements to allow for expanded delegation of ROI operational capabilities and responsibilities. Develop policies for disclosure tracking and auditing capabilities. Determine whether ROI will remain centralized in HIM or be decentralized.	Consider work queues that are built into electronic record systems that will drive staff members' work for the day (e.g., verbal orders that are not signed, transcriptions, etc.). Consider electronic rules and alerts on ROI requirements to allow for expanded delegation of ROI operational capabilities and responsibilities.

record received in the department. Forms inventory is critical, as is forms design, for efficient capture of information.	Ensure that the organization has carefully planned EHR content and access before moving coding or transcription functions off-site (e.g., will coders require online access to clinical documentation, such as doctors' progress notes?). Forms inventory and design become even more critical at this phase because efficient processing (scanning, indexing, and online review) is predicated on effective forms management. Define when the record is complete for coding purposes (e.g., which reports will be available to coders and in which format-paper or electronic). Conduct a workflow analysis determining current manual and paper processes that will be electronic. Look for duplication, redundancies, and inefficiencies associated with the current manual process. Streamline current processes preparing for the transition (reduce duplication of efforts, redundancy of entering data, and other related inefficiencies).	Develop policies for disclosure tracking and auditing capabilities. Determine whether the ROI will remain centralized in HIM or be decentralized. Ensure the organization possesses appropriate access to EHR content before moving coding or transcription functions off-site. Define when the record is complete for coding purposes (e.g., must specific reports be available to coders before coding?). Forms management and control are essential so that manual processing is avoided and the EHR can be upheld legally without disruption of unofficial forms.

Record Completion		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Written procedures outline deficiencies to look for when reviewing the different record types (e.g., inpatient, emergency room). Each record is reviewed for presence or absence of reports requiring necessary signatures. With use of an automated deficiency system, deficiencies are entered manually into the system for tracking and notification that completion is necessary.	Written procedures outline deficiencies to look for when reviewing the different record types (e.g., inpatient, emergency room). Review and consider e-signature processing capabilities, limitations, and opportunities for electronic portions of the EHR.* Determine if the vendor can automate deficiency analysis. Establish business rules for viewing the EHR on the basis of an individual's role and the completion status of a document (e.g., should ROI staff see only complete electronic records?). Ensure EHR system capabilities to monitor and track record or document completion (e.g., notifications to individual clinicians, aggregated management screens, and reports for HIM).	Consider electronic rules and alerts to clinicians for the completion of the record. Procedures in HIM outline auditing this completion process versus analyzing the record for completion. Written procedures outline deficiencies to look for when reviewing the different record types (e.g., inpatient, emergency room). Review and consider e-signature processing capabilities, limitations, and opportunities for electronic portions of the EHR.* Determine if the vendor can automate deficiency analysis. Establish business rules for viewing the EHR on the basis of an individual's role and the completion status of a document (e.g., should ROI staff see only complete electronic records?). Ensure EHR system capabilities to monitor and track record or document completion (e.g., notifications to individual clinicians, aggregated management screens, and reports for HIM).
*Consolidated Health Informatics. "Standards Adoption Recommendation." Available online at http://www.ncvhs.hhs.gov/061011p2b.pdf		

Filing		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**

Records are filed in folders, and each is as- signed a patient-specific number. Organizational policy should define the medical record numbering system used. Policy defines where and how records are stored. Retention schedule is included in the policy. Policy outlines handling and storage of incomplete records, as well as when the record is considered complete for permanent filing.	Determine which file room operations are needed to ensure acceptable productivity and customer service levels in a hybrid file room environment (e.g., a combination of hard-copy records, scanned records, and information in a data repository). Considerations should include: • Functions and tasks • Hours of operation • After-hours access and backup • Staffing needs • Record control • Filing and indexing • Retention, purging, archiving	Review file room staffing and need to reduce or redefine staff as the record becomes fully electronic. Determine whether any of the paper record will be converted to electronic format or whether paper records will be phased out over time as a result of retention and purging policies. Establish policies and procedures to outline the management of remaining paper records to include loose sheets and any outside records.

Locking the Record		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Written policies and procedures define when the record is complete and permanently filed (e.g., all loose reports filed, deficiencies complete, coding done).	Written policies and procedures define which part of the record is kept as paper and which is electronic. Policy also defines when both paper and electronic portions of a hybrid record are considered complete (e.g., no additional processing is required, all reports are complete). Complete records are locked and avail- able as read only. Any subsequent additions, changes, or deletions are handled as addenda to the record. Policies and procedures must define which documents are to be signed electronically and which are to be signed manually, as well as how to handle the existence of both electronic and manual signatures on the same or different versions of the document.	Written policies and procedures define when a record is considered complete (e.g., no additional processing is required, all reports are complete). Policy must indicate at what point electronic documents are locked and available as read only. Any subsequent additions, changes, or deletions are handled as addenda to the record. Software must have the ability to insert a record document in such a way that the entire record is retrievable, regardless of the discontinuity of episodes of care or late additions of documentation to a single episode of care.

Report Capabilities		
Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Data are abstracted from medical records and manually entered into abstracting software. Depending on the capabilities of the abstracting software or other information system, reports may be available from these data electronically. If no electronic reporting capability exists, reports may be prepared by using data from printed reports produced by the system.	Report-writing software may be available that will pull data from the abstracting and other systems. There also may be predefined (e.g., standard or boilerplate) reports available that are part of the electronic portion of the medical record.	Software should have the greatest possible functionality, flexibility, and integration capabilities to enable data to be pulled from any part of the electronic record (e.g., abstracting, billing, ADT). Data from all applications should be available and able to be formatted as needed for presentation or analysis. Flexibility in report functionality (such as graphing) is a major asset. Predefined (or standard) reports can be developed for routine reporting.

Version Control

Version control is required to manage different iterations of documents (such as when a document has been displayed in an unsigned state in a medical record). Once the person authenticating the document signs it, a new version of the document is displayed. However, if the signer makes changes to the content of the document in addition to signing it, a decision must be made as to whether both versions of the document need to be available.

HIM departments long have had to determine whether to retain older versions of documents in the complete medical record. (The laboratory, for example, often has multiple versions of test results from the initial preliminary result until the final result is available.)

In hybrid and fully electronic health records, it is important to have a flag or other signal indicating that previous versions of the document exist. System documentation should include a clear indication of when each version was viewable by caregivers for use in making clinical decisions. Another version control scenario to consider carefully is when amendments are made to documents through the organizationally approved process.

Every organization should determine the capacity of their medical records in each state of being (paper, hybrid, or fully electronic) to allow appropriate viewing of earlier versions of documents and develop policy that reflects the capability of the individual EHR. At the very least, caregivers should be made aware that earlier versions of documents exist, and they must be able to access them if needed.

Policy and procedure also are needed detailing how disclosures of documents with multiple versions are to be handled. This is not a new issue with EHRM and should be considered carefully and redefined during the migration from paper through a hybrid state and into a fully electronic record. Are all versions released or only the final version? Each organization must specify what will be released when copies of the record are requested. It may be acceptable to release only the final versions of documents if there have been no changes between versions except the addition of signatures or minor editorial changes. However, if clinical information that may have been critical to caregiver decision making has changed, it may be appropriate to release previous versions of documents in addition to the final version.

Another consideration is the HIPAA requirement to notify all parties who may have been sent copies of health records to be notified when there is a change. A procedure for accomplishing this notification must be integrated into organizational policies and procedures to ensure compliance.

Reconciliation for Electronic Processes

Reconciliation is the process of checking individual data elements, reports, or files against each other to resolve discrepancies in accuracy of data. Reconciliation ensures that data are complete, accurate, and consistent. Just as HIM departments perform reconciliation processes for the paper record, the need for quality oversight to reconcile data continues and often expands with the EHR.

The focus on timely reconciliation processes has accelerated with the advent of the EHR. Processing must move from five days a week to seven days a week throughout the year. As the reliance on the EHR increases, processes such as ensuring that data move across interfaces for timely posting in the record and elimination of duplicate medical record numbers become critical for effective care decisions.

HIM professionals are skilled at creating and managing processes that ensure attention to detail and have a broad understanding of the flow of information across the care continuum. Orientation to detail and a broad understanding of the effect of timely, quality information are necessary traits for successful implementation and maintenance of the EHR. HIM professionals also understand how to balance and prioritize the criticality of clinical information and business system needs.

	Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Inpatient Visits	Verify that a record exists for each discharge. Verify correct patient type registered (e.g., inpatient, short stay, observation status) to ensure accurate billing.	Same with the addition of monitoring canceled admissions.	Same

Emergency Department, Outpatient, and Clinic Visits	Verify that record exists for every registration. Verify correct registration of multiple visits in one day according to APC regulations.	Same with the addition of monitoring canceled admissions.	Same
Interface Engine	N/A	Monitor interface engine logs at least daily for failed reports. Research and correct documents that fail to cross an interface between disparate computer systems (e.g., stand-alone transcription system to an EHR). Ensure that documents are posted to the correct encounter and are in the correct location. Verify that content remains constant when moved from one system or database to another. The extent of reconciliation increases with the number of disparate computer systems.	Same
Master Patient Index and Enterprise Master Patient Index (EMPI)	Correct duplicate patient name and number entries by accurately matching patients to paper records. Ensure match to all computer systems (e.g., laboratory, radiology, pharmacy, and billing). Correct other or duplicate names in system (e.g., legal guardian names) through verification of secondary matched data elements.	Same issues as in the paper-based record.	Same issues as paper-based and hybrid records. The EHR may be able to identify automatically the components of records in other electronic systems and provide notification of changes.
In-box Maintenance	N/A	Monitor unopened mail and incomplete documentation (e.g., unsigned dictations, and unreviewed results,	Same
Autofaxing Files and Automatic Data Transfers	Monitor transcription systems for failures of sent documents. Periodically validate that fax numbers work and that remote fax machines are located in secure locations.	Expanded monitoring including voice recognition and direct charting.	Expanded to include transfer of EHR files for ROI, autofaxing to community physicians, download of EHR data to patient personal health records, and community-based health records or databases.
Work Queues	Primarily focused on HIM department systems such as coding and incomplete chart tracking.	Expanded to include scanning system.	Extended to entire EHR.

Downtime Processes	None except for HIM functions.	Ensure online data are captured after downtime through direct entry or scanning.	In addition to more detailed and lengthy postdowntime data capture, ensure that data flow to a data warehouse or other repository in a timely manner and in the correct sequence. Track legal EHR variations from the policy on individual records for all downtimes, as well as historically for lengthy downtimes.
Patient/Legal Guardian Amendments Living Wills and Durable Powers of Attorney for Healthcare Decision Making	Ensure documentation is filed in paper record.	Ensure documentation is scanned into EHR or post a flag that indicates such documents exist and how to access them.	Ensure documentation is either scanned into the EHR or ensure the amendment made online adheres to the agreed on amendment process.

Managing Other Types of Digital Records and Data

HIM expanded into EHRM in conjunction with the advancement of digital technologies. No longer are health records made up of analog (i.e., paper-based) discharge summaries, progress notes, physicians' orders, and flow sheets. Digital electronic reports from the laboratory and pharmacy, digital nurses' notes, e-mail and voice messages containing PHI, digital X-rays, digital photographs from the emergency department, digital material received from other facilities, video files of cardiac catheterizations, and audio recordings of heartbeats are all part of the clinical data gathered about patients. Consequently, all electronic information that is generated about patients in healthcare organizations-regardless of the record type and storage medium-may be classified as part of the EHR. Therefore, all the different, electronic types of records, such as e-mail and voice-mail records, and all the different data types, such as discrete, structured data and unstructured free text, diagnostic image, document image, vector graphic, audio, and video data that are part of the EHR must be well understood and well managed.

Other Types of Digital Records

E-mail

E-mail has become a record-generating and communication system vital to the business processes within healthcare organizations. It has replaced most healthcare organizations' traditional analog communication processes, and it is being used increasingly for a number of nontraditional e-mail activities, such as sending secured, digital reference laboratory results and attaching secured, digital discharge summaries to the physician's office. Therefore, it is essential to manage e-mail with the same thought and attention that have gone into managing other types of patient records.

E-mail is another type of business record and is subject to the same course of evidentiary discovery as any other healthcare organizational business record, such as the patient medical record, patient financial record, or employee record. In addition, e-mail messages have a life cycle just like any other record. E-mail messages are created, indexed, searched, retrieved, routed, stored, and purged. More importantly, e-mail is now one of healthcare organizations' largest and most vital information assets. Therefore, like any other business records, e-mail records and the information contained in the e-mail require EHRM.

The first step in e-mail management should be to retain e-mails within an overall electronic document management strategy. For example, most often, the information contained in e-mails is interconnected (e.g., regarding Mary Smith's diagnosis, the privacy official's recent meeting minutes, etc.). To ensure that all the e-mails relating to Mary Smith or the organization's privacy meetings can be located, it makes sense that the strategy includes identifying the existing enterprise-wide repositories that securely store e-mail records and attachments that merit evidentiary handling.

Next, to reduce the legal risks of e-mail records, healthcare organizations should develop or acquire an e-mail management system. This system should include a centralized archive. In addition, the system must be easy to use, providing intuitive methods for identifying e-mail classification (such as patients) and retention rules. The system also must provide fast and efficient access to the archive, including tried-and-true search capabilities. Finally, the system must work with today's popular e-mail systems, such as Microsoft Exchange, and be seamlessly integrated into the EHR.

For example, the system should enforce e-mail archiving policies. When an individual closes an e-mail and is ready to discard or save it, a prompt should appears with a yes or no choice asking if the user would like to make this a part of any of the healthcare organization's business records, such as the classification of patient medical records. If the healthcare organization declares ahead of time that the e-mail must always be retained to comply with a regulatory, legal, or business need, such as an e-mail correspondence between a provider and a patient, then this opt-in or opt-out e-mail capture function can be eliminated. In addition, this function can be managed in the background by using Web technology so that, for example, each new patient added to the master patient index triggers a domain name with all inbound and outbound mail captured for "patientname.com."

Retention rules should be triggered automatically by actions, which include automatically deleting or encrypting a "patient class" of e-mail after a defined number of days, months, or years so it cannot be accessed. (Note: Never archive encrypted e-mail records for fear of losing the algorithms or keys.) This process can include issuing an e-mail notification to all authorized users when, for example, e-mail records one through 100 for "patientname.com" are approaching the organization's retention mark or issuing an e-mail notification when user mailboxes contain more than, for example, 100 MB of messages.

Despite good intentions, such systems quickly become overwhelmed by metadata and attachments. In terms of a storage crisis, attachments present a significant risk. Perhaps a problem of greater importance is the proliferation of e-mail copies (i.e., carbon copies and blind copies). Copies produce a negative effect on healthcare organizations' abilities to discard all e-mail record copies at the end of retention periods. Therefore, creating the appropriate rules, policies, and processes must precede system deployment.

Like other business records, e-mail records present a huge opportunity to reduce the risks of enormous legal costs in evidentiary proceedings. On the other hand, their anticipated explosive growth and growing significance in the legal process present formidable challenges. The opportunity for HIM professionals to manage the organization's patient e-mail records just like other records will allow HIM professionals to oversee the aspects of many enterprise-wide information repositories and focus on both the digital and analog patient record repositories inside and outside their existing domains.

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
E-mail messages, such as those containing PHI, could be printed to paper and filed in the appropriate folder.	E-mail messages, such as those containing PHI, are printed to paper and filed in appropriate folders.	E-mail messages, such as those containing PHI, are integrated seamlessly into the EHR, where they are indexed and can be searched, retrieved, routed, stored, and purged or destroyed. E-mail messages containing PHI are encrypted in transit and at rest.

Voice Mail and Phone Messages

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Analog voice-mail messages, such as those containing PHI, may be transcribed into a paper-based written note for the medical record. Analog telephone messages or notes may be documented as progress notes or orders that are later appropriately verified by the physician.	Analog or digital voice-mail messages, such as those containing PHI, may be transcribed into a paper-based written note and filed in appropriate folders.	Digital voice-mail messages containing PHI and telephone conversations with patients or providers (e.g., changes in condition, medication, treatment) should be documented or imported into the EHR where they are indexed and can be searched, retrieved, routed, stored, and purged or destroyed. Complete documentation of patient and provider identification, date, and time of the actual conversation or message, as

		well as the date and time of the entry into the EHR.

Material Received from Other Facilities (e.g., hard copy, diagnostic images, cine films, compact discs)

Paper Systems	Hybrid or Transitional Systems	Fully Electronic Systems
Hard-copy material is incorporated into the paper-based medical record according to written organizational policy. Diagnostic images, cine film, and CDs are reviewed by healthcare providers and may be returned to the originators after copies are made if they are deemed necessary. If copies are made, they should be filed in an easily identifiable and accessible storage repository, such as in an analog film library or in CD jackets that can be attached to the paper chart.	Hard-copy material may be scanned into the document image-enabled EHR according to written policies and procedures. Depending on the status of the EHR, digital diagnostic images and cine film, including those stored on CDs, may become part of the EHR. Analog diagnostic images, cine film, and CDs may be stored in the appropriate storage repository of the appropriate facility department.	Hard-copy materials are scanned into the document image-enabled EHR following written policies and procedures. Digital diagnostic images and cine film, including those stored on CDs, become part of the EHR.

Other Types of Data

Free Text

Free text is one type of unstructured data found in EHRs. Free-text data are narrative. The data are generated by word- or text-processing systems, and their fields are not predefined, limited, discrete, or structured. Instead, their fields are unlimited and unstructured. When a healthcare professional needs to search unstructured free text, it is not a simple task for the information system's search engine to find, retrieve, and allow the user to manipulate one or more of the data fields or elements embedded in the text. Typically, EHR free text is found in healthcare information systems' comments fields and in the documents generated by healthcare transcription systems.

Many EHR users like to generate free text by typing unstructured, narrative information into EHR comment or related fields and documents instead of pointing and clicking structured data into EHRs because they are used to typing information into e-mail messages and other electronic documents to express their findings and recommendations (similar to the way they handwrite findings and recommendations into analog [e.g., paper] documents). When users are required to point and click pieces of information or phrases into electronic fields and documents in EHR systems, they often complain that the point-and-click data input method takes more time than typing, that the composed sentences based on pointing and clicking appear rudimentary, or that the structured data elements for pointing and clicking cannot be located easily on the screens.

Some EHR users like to generate unstructured free text by dictating narrative information into digital-dictation or speech-recognition systems. Once the information is transcribed by word-processing systems or translated to text by speech-recognition systems, familiar easy-to-read and easy-to-understand documents are presented to the user. Such documents include but are not limited to radiology and pathology result reports, operative reports, and clinical notes and evaluations. (Note: Speech-recognition system engines take the unstructured, free text–based voice data and codify the data, often with the help of templates. Hence, the format of the output text data from these systems becomes structured, with predefined and limited fields.)

Free text is important in the management of EHRs.

1. Because free text is unstructured and not easy for electronic search, retrieval, and manipulation functions, many information systems of structured data (e.g., healthcare information systems, clinical information systems) do not allow for free-text data entry or carefully limit such options on their screens.
2. To speed up the documentation process and avoid duplication of effort, many EHR users copy and paste free-text data into their SOAP notes, progress notes, and narrative reports. Just as with paper-based records, EHR users must be held responsible for their record entries that are not complete, accurate, timely, and authenticated. Therefore, healthcare organizations should develop policies and procedures related to copying and pasting free-text documentation into EHR systems.

The copying and pasting action poses several risks, including but not limited to:

- Copying and pasting the note to the wrong encounter or the wrong patient
- Copying and pasting abnormal laboratory or X-ray results into notes without addressing the abnormalities in the note, which could be used as evidence of carelessness or negligence
- Lacking the identification of the original author and date

In addition, the action of copying and pasting free-text data into the EHR can lead to documentation excesses. Such excesses can be unnecessary duplication of information that not only lengthen the notes and reports but make the notes and reports more difficult for other caregivers to read. In addition, such excesses take up space in computer memory that is potentially limited and slow computer retrieval times.

3. Digital dictation, transcription (word-processing), and speech-recognition systems must be integrated carefully into EHR systems, the systems responsible for meeting all legal (local, state, federal) requirements in the areas of document authentication and retention. Therefore, standards, such as those recommended by Health Level Seven (HL7), version 2.3 and higher, must be deployed for document message transfer between these systems and the EHR. Key features include the electronic capture and integration of text reports into the EHR and the electronic scanning and correcting of each report for omissions and inaccuracies of patient and provider identification data. In addition, key EHRM tasks must include collecting appropriate signatures; allowing for the review and retrieval of the text reports; and archiving the text reports in a way that allows for economical, long-term storage and eventual destruction.

Paper Systems	Hybrid or Transitional Systems	Fully Electronic Systems
Handwritten findings and recommendations in analog, paper-based documents and forms.	Some handwritten findings and recommendations in analog, paper-based documents and forms. Some typing into electronic systems' comments fields. Some dictating into digital dictation systems for subsequent transcription.	Pointing and clicking findings and recommendations into electronic information systems. Dictating into speech-recognition systems with natural language processing capabilities.

Digital Images, Photos, Video, Audio, and Graphic Files

In the development of a recommendation, the fundamental requirements considered for representing multimedia objects in patient EHRs include that the objects stored in the patient records are uniquely identifiable persistent entities and that the objects contain patient study, study component, examination, equipment, unique identification, and other information (e.g., date, creator, body part) as attributes and metadata in addition to the objects themselves. The following items are recommended for future consideration and research support to address issues related to multimedia patient information:

1. Standards committee collaborations-As the standards continue to develop, it is recommended that the Digital Imaging and Communications in Medicine (DICOM) and HL7 standards developing organizations (and others as appropriate) work together to harmonize their standards for healthcare applications.
2. Time to incorporate industry standards-Consideration should be given to providing support for reducing the time between implementation of industry standards and incorporation into federal standards.
3. Long-term storage and retrieval of information-Consideration should be given to accounting for problems associated with the migration of information among media bases-problems that are partly due to rapidly changing information technologies.
4. Unique identifiers-Assignment of unique identifiers should be supported in the Integrating the Healthcare Enterprise initiative to provide harmony with DICOM, HL7, and other standards.
5. Computer system firewalls-For biomedical information exchange between agencies, issues of computer system security and firewalls are often a larger hindrance to effortless communication than are the use of different data standards within agencies. Additional research is needed to develop secure data systems that remain open to exchange of large data sets from the outside.

Access Control and Nonrepudiation

With the implementation of an EHR comes the opportunity to improve access to patient health information. Used by the right people under the right circumstances, this improved access will lead to better communication among care providers; more information about the patient's history, current conditions, and treatments; and more organized delivery of healthcare.

However, if the information becomes accessible to the wrong people or under the wrong circumstances, patient confidentiality will be breached and patient trust in the healthcare system will erode.

Precautions must be taken to reduce the risk of breaches of confidentiality of patient information.

Access Control

Access control is the process that determines who is authorized to access patient information in the health record. In paper-based records, access is controlled through physical security safeguards, chart tracking, and outguide systems.

HIPAA privacy and security standards support the idea of providing access by determining the needs of groups of users. Facilities must identify such groups and then determine to what information the group needs access and under what circumstances, which includes determining the subsets of the information an individual is authorized to access and the functions the individual will be able to perform using the information.

For example, one group could be identified as “physician of record.” This group would include any physician who had been listed as the primary, admitting, attending, dictating, consulting, or ordering physician in the EHR system. This group would be allowed to view all information included in the record of the patient, but they might not be allowed to fax or print the information. On the other hand, an ROI group would be allowed access to all patient information for viewing, printing, and faxing.

Authorization for access to information also can be granted on the basis of other criteria besides membership in a group. Items such as terminal address, day of week, or time of day can be considered. For example, if a department operates from 8 a.m. to 5 p.m., the system could be set up so that no terminals in the department would be able to access patient information outside those hours.

Access should be terminated automatically after a certain period of inactivity. Groups also can set the length of system inactivity. The access for nurses on a nursing unit could time out after 10 minutes of inactivity; access for coders should be set for a longer time, since coders often must review numerous documents before determining a code.

Sophisticated EHR systems can limit access according to document type or field in the patient record.

Access to information for emergency situations should be considered during the process of defining access, sometimes referred to as “break-the-glass” access. Clinicians requiring access to PHI during an emergency should be allowed easy access to it. However, every incidence of such access should be monitored carefully by using audit trails within a reasonable time after the access.

When authorization is granted, the individual must be made known to the system. The term for this is “authentication” and can be accomplished by using a “what you know, who you are, or what you have” model.

Giving the individual a user name and password generally addresses “what you know.” The user name is kept in a file that identifies the information that the individual can access and the functions that the individual can perform. This model is termed “single-factor identification,” since it requires only that the user know both the password and user name.

“Who you are” refers to some form of biometric identification including fingerprints, retinal scans, and voice recognition. These more sophisticated forms of authentication require additional devices be connected to each access device (e.g., PC, laptop, PDA) to record the imprint.

“What you have” relates to a smart card or other item the user carries that can be used to identify the user.

At least two of the above factors should be joined to produce strong authentication to clinical systems. Users generally are accustomed to a two-factor model, since most bank cards require the purchaser to have a card and use a personal identification number or password to complete a transaction.

Organizations will have to find ways to accommodate providers by using multiple systems that require the use of unique passwords for each system. The concept of single sign-on, which allows a provider to be authenticated to use the EHR one time, rather than having to log in to every application he or she is authorized to access, is very much a topic of discussion but is not a reality in most organizations today.

Nonrepudiation

Many of the users authorized to access patient information also will be authorized to enter information, such as e-mail, notations, and transcribed reports. An individual authorized to provide this type of documentation to a patient record also should be authorized to use some type of electronic signature or other method of attestation. Rules connected to the application of the electronic signature can cause the notation or document to be "locked," which reduces the likelihood that an individual, including the original author, will be able at a later date to make changes to the information originally recorded. In addition, date and time stamps should be associated with the signature so one can prove when a document was finalized. The use of nonrepudiation reduces the likelihood that an author can deny having made the entry or the timing of that entry.

Amendments, Corrections, and Deletions

A key component of records management is the handling of addendums, amendments, corrections, and deletions. These are not new concepts or requirements within HIM. When a healthcare provider determines that patient care documentation is inaccurate or incomplete, he or she must follow established policy to ensure the integrity of the record.

From an EHR standpoint, there are guidelines that provide the required direction for creating and managing electronic documents in the health record. Refer to American Society for Testing and Materials and HL7 guidelines for the technical requirements that should be followed. Organizations must establish policy on addendums, amendments, corrections, and deletions within their medical record documentation policies so that the integrity of the record remains intact and in compliance with documentation standards. Policy should delineate the time frames within which the corrections and deletions will be made, and also, in conjunction with HIPAA compliance policy, outline what is necessary to make changes to the record.

The policy and procedure includes information about where the additional information is located within the body of the original report and the requirement that the addendum, amendment, or correction include a separate signature, date, and timed entry. The procedure indicates who is responsible for entering addendums, amendments, and corrections into the EHR.

These changes should be made in the source system where the documentation was originally created, as well as in any long-term medical record or data repository system. Under legal advisement, the organization should have processes in place for forwarding the changes to any other place where the information has been sent to ensure that providers have the most up-to-date information.

The policy should require that the total elimination of information should never occur. If the organization allows information to be deleted, it requires clear policies and procedures to ensure the integrity of the health record, and it should monitor and audit this functionality. Organizations that allow this functionality should review carefully clinical actions taken on the basis of initial documentation.

The electronic processes by which the corrections, deletions, and amendments are made probably will vary from developer to developer. Not all will handle the issue in the same way, even given the American Society for Testing and Materials and HL7 guidelines. There are some process characteristics, however, that should be present in all systems for correcting and deleting data.

For an individual datum or free-text response, the correction and deletion process should be made in the originating system, as well as in the long-term, archived medical record system or data repository. Documentation should be maintained of the correction or deletion, identifying date of correction, data dictionary code of the datum corrected, incorrect value of the datum, and user code of the individual certifying the datum to be incorrect.

For text reports, there should be an option to mark the report "corrected final" in addition to "preliminary" or "final." It may be possible to attach only an addendum to the report. Again, the document ID of the original document should be maintained with reference to the document ID of the corrected document along with date of correction and user code of the individual certifying the datum to be incorrect.

	Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Corrections/ Amendments	Draw a line through the original entry in such a way that the original entry remains legible. Do not alter the original record in any way.	Use both the paper and electronic processes, depending on how your documentation is created.	Corrections must be made in the source system (where the document was originally created), as well as in the long-term medical record or data repository system.

	Print the word “error” at the top of the entry, sign with name, discipline, date, and time. Indicate the reason for the correction (e.g., incorrect patient). Note the change or addition in proper chronological order.		The type of correction should be noted (error, delete, etc.) at the top of the entry, signed with name, discipline, date, and time. Maintain the original incorrect entry or document and add the corrected entry or companion document to it.
Addendas	New documentation used to add information to an original entry. Addenda should be timely and bear the current date and reason for the additional information being added to the health record.	Use both the paper and electronic processes, depending on how the documentation is created.	Corrections must be made in the source system (where the document was originally created), as well as in the long-term medical record or data repository system. The type of correction should be noted (addendum) at the top of the entry, signed with name, discipline, date, and time.
Deletions/ Retractions	Nothing is removed from a paper record. Follow the steps as noted above.	Use both the paper and electronic processes, depending on how the documentation is created.	The computer should be able to hide an original datum or document from view and replace it with a corrected datum or document. However, the original information must be retained and made available if necessary.

Purge and Destruction

Every healthcare facility must have an approved retention schedule that must apply to all paper records and EHRs. It also must include the retention schedule of the metadata (description of data and its underlying applications and programs) and audit trails. A file management system must be capable of notifying the user with a retention trigger (such as 10 years from filing date, at completion of the case, or expiration plus three years).

Selective Destruction
In an entirely EHR world, it becomes possible to use a process of selective destruction in which some types of documentation can be retained while other documentation can be destroyed. If selective destruction is the organizational choice, the policy for record retention and destruction of EHRs should outline the protocol for selective destruction on the basis of the types of documentation found in the record. Once the statute of limitations has expired on an episode of care, it then is possible for documentation to be destroyed. In the electronic record, every type of documentation can be evaluated individually for retention, with the recognition that not all documents have the same need for retention. For example, once the statute of limitations has expired, is it really necessary to keep all the nursing graphic documentation? Perhaps the progress notes of attending physicians would be retained, but notes of medical students and first-year interns would not. A facility could decide to retain the discharge summary, operative report(s), pathology report(s), and diagnostic data but nothing else. Once decisions are made according to the protocol, electronic files can be destroyed according to facility data security policy.

Destruction of Paper and EHR Media
As governed by state and federal guidelines, PHI stored in paper, electronic, or other formats must be destroyed at the end of its retention period by using an acceptable method of destruction. Acceptable measures of destruction include shredding, incineration, and pulverization. A destruction log must be maintained to identify the destroyed records. At minimum, the destruction log must capture the information listed below: a. Date of destruction b. Name(s) of the individuals responsible for destroying the records

c. Witness (name(s) of the person witnessing the destruction)
d. Method of destruction
e. Patient information including full name, medical record number, date of admission, date of discharge

If the records are destroyed by a third-party destruction company, a certificate of destruction should be obtained attesting to destruction of the records. The destruction log must be maintained permanently.

Disposal/Destruction Protocols for Electronic Patient Health Information

Computer Data and Media

Workstations, laptops, and servers use hard drives to store a wide variety of information. Patient health information may be stored on a number of areas on a computer hard drive. Simply deleting these files or folders containing this information does not necessarily erase the data.

1. To ensure that any patient's health information has been removed, utility software that overwrites the entire disk drive must be used, which could be accomplished by overwriting the data with a series of characters. Total data destruction does not occur until the backup tapes have been overwritten. Magnetic neutralization will leave the domain in random patterns with no preference to orientation, rendering previous data unrecoverable.
2. If the computer is being redeployed internally or disposed of owing to obsolescence, the aforementioned utility must be run against the computer's hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.
3. If the computer is being disposed of owing to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of a magnetic bulk eraser. This requirement applies to PC workstations, laptops, and servers.

Federal guidelines for data disposal and sanitization can be found in the National Institute of Standards and Technology's Special Publication 800–88, *Guidelines for Media Sanitization,* at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

CDs and Diskettes

CDs containing patient health information must be shredded or pulverized before disposal. If a service is used for disposal, the vendor should provide a certificate indicating the following:

1. Computers and media that were decommissioned have been disposed of in accordance with environmental regulations, since computers and media may contain hazardous materials.
2. Data stored on the decommissioned computer or media were destroyed according to the previously stated method(s) before disposal.

Methods of destruction and disposal should be reassessed periodically on the basis of current technology, accepted practices, and the availability of timely and cost-effective destruction and disposal services.

User Interfaces and Web Portals

Patient and Provider Entry to the EHR

Web portals began in the consumer market with the large, public online Internet service provider Web sites, such as AOL. Portals offered end users fast, centralized access to Internet services and information found on the portal sites. In an effort to ensure that visitors would return to sites, the large public directory and search engine sites such as Yahoo began to offer customized and personalized interaction with the Web. Customized interaction allows visitors to create customized, relevant views of the site at the role and individual levels. Personalized interaction provides Web site sponsors a means to filter information to meet the unique needs of users on the basis of their roles and preferences.

At about the same time, private organizations such as healthcare organizations began to deploy intranets to address internal business needs within secure environments. The intranets became analogous to internal, private "Internets" by restricting access to authorized users. Soon, portals were recognized as a way to provide easy access to private organizations' internal information, offering a central aggregation point or gateway to the data via a Web browser. And the portals became analogous

to internal, private “Webs” by restricting access to authorized users. Portals quickly evolved into an effective medium for providing secure access to an organization’s applications and systems used by diverse, disconnected participants in various locations.

Like the predecessor clinical workstations in healthcare organizations, clinical and clinician portals began as a way for clinicians to access easily via a Web browser an organization’s multiple sources of structured and unstructured data from any network-addressable device and develop loyalty to the healthcare organization. They quickly evolved into an effective medium for providing access to multiple applications, both internal and external.

Therefore, clinical and clinician portals became “private Webs,” restricting user access to the data and applications contained within the portal. This capability was crucial to protect the integrity of decisions made by healthcare providers and to ensure confidentiality of patient information.

More important, the portals began to provide more functionality. For example, they included customization capabilities and simplified automated methods of creating taxonomies or categories of data. Similar to how consumer portals such as Yahoo organize files and data into such categories as food, fashion, and travel, clinical and clinician portals might classify files and data according to test results, dictations, and patients.

In addition, portals grew to offer other enabling technologies, such as single sign-on, personalization, document and Web content management, proactive delivery of data, and metadata management. Therefore, in healthcare organizations with EHR implementations, the portals allowed physicians to access the EHR easily.

Quickly, it became clear that clinical and clinician portals could provide a way of addressing some of the cost issues of implementing EHR capabilities across the enterprise, including which EHR information and transactions could benefit patients. Consequently, savvy chief information officers and marketing executives determined that extending the reach of the portal to the patient could enhance the healthcare organization’s image and relationship with its customers, as well as develop community loyalty.

Soon portals developed into an efficient way to organize all the information (structured, such as relational data, and unstructured, such as e-mail, Web pages, and text documents) that clinicians and patients needed to access routinely. Consequently, today, clinician and patient Web portals are viewed as the single point of personalized access (i.e., an entryway) through which to find, organize, and deliver *all* the content contained in the EHR.

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Not applicable	Some integration of an organization’s multiple sources of structured and unstructured data, as well as back-end applications, allow clinicians with proper authorization to access pieces of the EHR easily. No access by patients.	Complete integration of an organization’s multiple sources of structured and unstructured content, allowing clinicians and patients with proper authorization to access the EHR easily.

Managing Patient Identification

Managing patient, resident, and client identification can be a major challenge for facilities in the EHR environment. The issues are not new, and HIM professionals are more aware of the issues because electronic systems can make the incongruities more visible. With today’s emphasis on patient safety, accurate and consistent patient identification becomes all the more important. No facility wants its medical and nursing staff placed in the position of administering an appropriately grouped and cross-matched blood transfusion to an improperly identified patient.

A master patient index may index patients, persons, healthcare plan members, guarantors, subscribers, physicians, healthcare practitioners, payers, employees, employers, and others. If it is shared by two or more care centers it may be called an enterprise master patient index (EMPI), enterprise patient index, corporate person index, or multifacility index.

The most common incongruities found in EMPI management are duplicates and overlays. Duplicates are identified as one patient having two or more medical record numbers or other identifiers in the same facility or division of an enterprise (across some large enterprises, however, patients purposely have a different medical record number in multiple facilities tied together by an enterprise-wide corporate identifier). Overlays are identified as two different patients’ records being indexed to one medical record number.

In some facilities, because of the nature of the services provided, patients are indexed purposely to an alias and a medical record number or other identifier in the EMPI to facilitate care. Thus, in some Level I trauma centers, trauma services alias and medical record numbers (e.g., ZEBRA, TR080 #01582444) are assigned to facilitate prehospital care when the patient cannot be identified accurately in the field. Similarly, facilities offering psychiatric emergency services or routine psychiatric services purposely may duplicate an alias and medical record number for a patient so care can commence when patients may not be able to identify themselves accurately because of their psychiatric conditions (e.g., MARIGOLD, PES041 #01582678). Later, when the patient's condition has stabilized, the patient can be identified accurately after research in the EMPI or other resources and the alias name and medical record number merged to the correct number by EMPI staff. Use of these aliases and medical record identifiers also obviates the use of John or Jane Doe aliases, which are difficult to manage because of the huge volume of patients that eventually can be attached to them, with thousands and thousands of encounter dates and account numbers.

Management of the EMPI should be an active daily component of the EHRM environment. EMPI staff should be available to admissions and registration staff to help resolve misidentification errors caused by spelling of names and recording of birth dates. As duplicates are identified by clinical staff or other means, EMPI staff should be assigned to investigate the alleged duplicate carefully, matching biometrics, signatures, and diagnoses identified in a first medical record with those of a second. Merging to one of the numbers should be undertaken only after thorough analysis of both the electronic results and text documents available online and the paper-based documents and reports available only in nonelectronic formats. Similar processes should be used to verify existing index entries for patients assigned trauma or psychiatric care aliases and identifiers.

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Usually housed in index card files, one 3x5" card is assigned per patient name. Merging is noted on the card and in the main file, forwarding the user to a later or earlier number. Physical paper records are moved from one numbered cover to another. Prepare appropriately named, identified, and bar-coded folders as necessary.	Unusual to see with respect to this function. Day to day same functioning as paper-based systems. Electronic records may have to be moved within electronic source and archival systems.	EMPI is a major database component of all vended health information systems. Lookup functionality should include a probabilistic algorithm to help admissions and registration staff choose the correct client. Identified duplicates are merged with the catalogue kept of all medical record numbers, aliases, or other identifiers stopped, including the dates when they were stopped. Account numbers, diagnostic results, and documents must be integrated into the correct chronology of the patient's record of services and attached to the persisting name and medical record number. When results or documents are viewed subsequently, the system should tell the viewer the date and time that the results or document came into the current record. Audit trails should document all details of the merge and the relocation of results and documents, as well as the ID of the staff member performing the merging of the accounts.

Overlays may be an even greater challenge to the management of the EMPI. Often involving direct knowledge of one individual and his or her life by another, two individuals indexed to the same medical record number may be very difficult to resolve. For example, the two individuals may once have been roommates or foster children in the same household and thus know a significant amount of life history about each other. One may possess documents or insurance ID cards from the other, making it easier to assume his or her identity and obtain healthcare services. A mental health patient may invent aliases at presentation for services to prevent nursing staff from learning too much personal information. In these cases, each inpatient admission or presentation for outpatient services must be analyzed for biometrics, signatures, diagnoses, and other minute facts to substantiate the pulling apart of the individual records, if warranted.

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Since all visits are mixed together on one 3x5" card, after analysis, the resulting two cards will have to be rekeyed to include *only* those encounter dates and the medical record number belonging to each patient. Preparation of appropriately identified medical record covers for each medical record number and volume must	Day to day, the same functioning as paper-based systems. Electronic records may have to be moved within electronic source and archival systems to produce two records, with each patient having	Functionality must be present in the system to allow two records to be pulled apart, encounter by encounter. All text documents, assessments, and diagnostic results associated with an encounter should move automatically with the encounter rather than having to be moved individually. When results or documents are viewed subsequently, the system should tell the viewer the date and time that the results or document came into the current record. The attachments to the encounters should be audited to ensure the results, assessments, etc., belong to the target patient. Patient account history must be validated so that

be prepared with appropriate names, identifiers, and bar codes.	one medical record number.	proper payments are applied to the correct patient or moved to the correct account or encounter, if necessary. Audit trails should document all details of the relocation of results and documents, as well as the ID of the staff member performing the moving of the documents.

Ongoing periodic identification of duplicates should be undertaken by using probabilistic algorithms to identify sets of individuals likely to be the same person. This process should include examination of such factors as name variants, address variants, Social Security numbers, and telephone numbers with weights contributing to the overall probability that the individuals are the same. This report should be produced routinely, such as weekly, biweekly, or monthly, and checked routinely by EMPI staff to clear the EMPI of duplicates. However, just because an individual is identified *possibly* to be the same as another on the duplicate patient report does not mean the record is a duplicate. Each candidate set should be examined in the same method undertaken for possible duplicates identified by other means as discussed above. As the organization moves to a completely electronic system, electronic results, documents, assessments, and demographics must be examined for evidence that the nominated sets are really the same person.

Paper Systems	**Hybrid or Transitional Systems**	**Fully Electronic Systems**
Not applicable because total analysis of index cards for possible duplicates is almost impossible on any periodic basis.	As EMPI moves to an electronic format, sets for examination as possible duplicates should be identified probabilistically. The physical record must be examined carefully to ensure that the identity of the nominated sets is the same.	Probabilistic identification of sets for examination as possible duplicates should be expected. The various electronic results, documents, assessments, and demographics of the nominated set must be examined carefully before merging.

Resources

All AHIMA resources are available online in the AHIMA Body of Knowledge at www.ahima.org.

AHIMA. "10 Security Domains (Updated)." *Journal of AHIMA* 81, no. 2 (Feb.2010): 57–61.

AHIMA. "Electronic Document Management as a Component of the Electronic Health Record." 2003.

AHIMA. "E-mail as a Provider-Patient Electronic Communication Medium and Its Impact on the Electronic Health Record." 2003.

AHIMA. "The Complete Medical Record in a Hybrid Electronic Health Record Environment: Part I: Managing the Transition." 2003.

AHIMA. "The Complete Medical Record in a Hybrid Electronic Health Record Environment: Part II: Managing Access and Disclosure." 2003.

AHIMA. "The Complete Medical Record in a Hybrid Electronic Health Record Environment: Part III: Authorship of and Printing the Health Record." 2003.

AHIMA MPI Task Force. "Building an Enterprise Master Person Index." *Journal of AHIMA* 75, no.1 (Jan. 2004): 56A–D.

American Society for Testing and Materials. "ASTM E1384-07 Standard Practice for Content and Structure of the Electronic Health Record (EHR)." Available online at www.astm.org/Standards/E1384.htm.

Comprehensive Guide to Electronic Health Records. New York, NY: Faulkner & Gray, 1999.

E-HIM Work Group on Implementing Electronic Signatures. "Implementing Electronic Signatures." Updated October 2003.

Health Level Seven. "Policy 14.00.01 Draft Standard for Trial Use." In *Policy and Procedure Manual*. Ann Arbor, MI: HL7, 2003.

Murphy, Gretchen, Mary Alice Hanken, and Kathleen Waters. *Electronic Health Records: Changing the Vision*. Philadelphia, PA: W.B. Saunders Company, 1999.

National Institute of Standards and Technology. “Guide to Storage Encryption Technologies for End User Devices.”, NIST Special Publication 800–111. Available online at http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

National Institute of Standards and Technology. “Guidelines for Media Sanitization.”, NIST Special Publication 800–88. Available online at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

Welch, JJ. “Correcting and Amending Entries in a Computerized Patient Record Admissibility of Medical Records.” *Journal of AHIMA* 70, no. 8 (Sept. 1999): 76A–76C.

Prepared by

Beth Acker, RHIA
Cecilia Backman, MBA, RHIA, CPHQ
Sara Briseno, RHIT
Camille Cunningham-West, RHIA
Cathy Flite, MEd, RHIA
Deborah Kohn, MPH, RHIA, FACHE, PHIMS
Beth Liette, RHIA
Cindy Loranger
Nicole Miller, RHIA
Diana Warner, MS, RHIA, CHPS

Acknowledgments

Mary Ellen Mahoney, MS, RHIA
Donna J. Rugg, RHIT, CCS
Allison F. Viola, MBA, RHIA
Lydia Washington, MS, RHIA, CPHIMS
Lou Ann Wiedemann, MS, RHIA, CPEHR

Prepared by (original)

Beth Acker, RHIA
Debra Adams, RN, RHIA, CCS, CIC
Camille Cunningham-West, RHIA
Michelle Dougherty, RHIA, CHP
Chris Elliott, MS, RHIA
Cathy Flite, M.Ed., RHIA
Maryanne Fox, RHIA
Ronna Gross, RHIA
Susan P. Hanson, MBA, RHIA, FAHIMA
Deborah Kohn, MPH, RHIA, FACHE, CPHIMS
Tricia Langenfelder, RHIA
Beth Liette, RHIA
Mary Ellen Mahoney, MS, RHIA
Carol Ann Quinsey, RHIA, CHPS
Donna J. Rugg, RHIT, CCS
Cheryl Servais, MPH, RHIA
Mary Staub, RHIA, CHP
Anne Tegen, MHA, RHIA, HRM
Lydia Washington, MS, RHIA, CPHIMS
Kathy Wrazidlo, RHIA

Acknowledgments (original)

Darice Grzybowski, MA, RHIA, FAHIMA
Kelly McLendon, RHIA

Back to practice brief

Article citation:
AHIMA. "EHRs as the Business and Legal Records of Healthcare Organizations. Appendix A: Issues in Electronic Health Record Management (2010 update)." (Updated November 2010).