The Legal Health Record
in the Age of e-Discovery

A White Paper of the
Electronic Health Record Adoption Task Force

November, 2008

©2008 by the Healthcare Information and Management Systems Society (HIMSS)
The Legal Health Record in the Age of e-Discovery

Introduction

The expected benefits of improved quality, lower costs, and greater efficiency are the major drivers behind the growing adoption of electronic health records (EHRs). As healthcare organizations replace their paper records with electronic versions, they must be mindful to ensure that the electronic versions have the legal standing equal to that of their paper predecessors. The HIPAA security rule\(^1\) and the 2006 Supreme Court amendments to the Federal Rules for Civil Procedure (FRCP)\(^2\) make the task of achieving full legal status for electronic health records significantly more difficult in comparison to paper records. The administrative, technical, and physical requirements of the HIPAA security rule have received a great deal of attention within the healthcare community and are well understood within healthcare organizations. However, the amendments to the FRCP that took effect in December, 2006 are less well known,\(^3\) especially in information technology departments where the management and storage of electronic data occur. The amendments provide guidelines for electronic evidence discovery—requesting and accessing electronic information during civil lawsuits in federal courts. Taken as a group they are usually referred to as “e-discovery amendments.”

Understanding the impact of the FRCP changes requires an understanding of how the definition of the “legal health record” (LHR) was formulated. In a paper published by the American Health Information Management Association in 2001, the following definition was given for the paper-based LHR.\(^4\)

“The legal business record generated at or for a healthcare organization. This record would be released upon request.”

Notably, the concept of "release of information" or disclosure is an essential component of this definition. The definition published by AHIMA in Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes,\(^5\) published in 2005, retains this key concept of disclosure while adding to the definition, concepts, and terminology suitable for electronic systems. In addition, the updated guidelines contain a list of documents that healthcare organizations may reasonably include as part of their legal record and those documents that are generally excluded such as logs, EHR audit trails, and event histories. Disclosure continues to be a key aspect of the LHR. However, e-discovery allows for access to organizational records and data during civil litigation that exceeds what healthcare organizations traditionally would define as their LHR. In fact, the very information that was specifically excluded such as logs and audits trails are now declared to be fair game for disclosure as part of e-discovery evidence requests. The reality is that all electronic data are subject to being disclosed if deemed pertinent, not just that information listed by the organization as constituting its legal record. These changes have far-reaching implications for how organizations define, manage, and store their records.
Traditionally, the major type of litigation experienced by healthcare organizations stemmed from malpractice actions. However, one new area of potential liability for healthcare organizations has appeared in the form of private Health Insurance Portability and Accountability Act (HIPAA)-related lawsuits. Since HIPAA went into effect in 2003, federal courts have held the position that private citizens had no rights to sue under HIPAA statutes. This changed starting in 2006 with Sorensen v. Barbuto, 143 P.3d 295 (Utah Ct. App. 2006), in which federal courts allowed private citizens to sue using HIPAA as a "standard of care." At least two additional lawsuits since that time reinforced this ruling, allowing for private HIPAA lawsuits in state courts. When one considers these rulings along with the frequency of data breaches reported for healthcare organizations in the media, and the increasing number of states that have instituted data breach notification laws, it is clear that the legal records of healthcare organizations, both clinical and business, will be subjected to more intense legal scrutiny.

Litigation is both civil and federal at this time. Thirteen state courts are currently allowing for e-discovery. When requested, organizations have only 120 days to respond to an e-discovery request. Organizations must be prepared for this discovery and know where key data is held within their systems before a request is made. A major challenge to healthcare organizations will be ensuring that their electronic records hold up in court and that preventable deficiencies in their quality and completeness are not the cause of unfavorable litigation outcomes.

**E-Discovery, a Closer Look**

The move to the current e-discovery rules began in 1996 with the Advisory Committee on Civil Rules. The work of that committee coupled with the work of the Sedona Conference, a legal think-tank dedicated to issues in complex litigation, led to the final amendments to the FRCP which became effective in 2006.

*The Sedona Conference Glossary: E-Discovery & Digital Information Management, Second Edition,* published in 2007 defines *discovery* and *e-discovery* as:

- **Discovery.** Discovery is the process of identifying, locating, securing and producing information and materials for the purpose of obtaining evidence for utilization in the legal process. The term is also used to describe the process of reviewing all materials that may be potentially relevant to the issues at hand and/or that may need to be disclosed to other parties, and of evaluating evidence to prove or disprove facts, theories or allegations. There are several ways to conduct discovery, the most common of which are interrogatories, requests for production of documents and depositions.

- **Electronic Discovery ("E-Discovery").** The process of collecting, preparing, reviewing, and producing electronically stored information ("ESI") in the context of the legal process.
A major focus of these amendments and e-discovery activity is ESI. This is an all-encompassing term which covers information stored in any electronic medium. Thus, e-mail, voice mail, instant messages, video, audio, photographs, databases, and all application data files including their metadata (logs, audit trails, version information, etc.) are now considered discoverable during litigation. This places a much greater burden on healthcare organizations as they manage their ever growing electronic information stores.

**Amendments to the Federal Rules for Civil Procedure**

**Rule 16 – Pretrial Conference, Scheduling and Management.** Addresses matters related to the conference between the defendant and plaintive representatives that occurs before trial. It introduces the concept of electronically stored information and also sets a time-frame for parties to discuss and finalize the terms for evidence production and preservation. Information identified during the pretrial conference as being pertinent to an ensuing trial will be placed on “hold” status. Rule 16 will impact organizations most that have poorly defined data stores and ineffective mechanisms for retrieving information in a timely manner.

**Rule 26 – Duty to Disclose; General Provisions Governing Discovery.** Among other things, Rule 26 discusses discovery scope and limitations. The most important provisions from the standpoint of the LHR deal with ESI. The rule states that all pertinent ESI must be disclosed and that all relevant ESI must be produced on request. The rule allows some leeway for ESI that is "not reasonably accessible" such as data in obsolete systems or on backup tapes that is difficult to recover. However, no firm guidelines are given for interpreting “reasonably accessible.” Rule 26 has direct implications for record retention and destruction policies especially as it relates to an organization's ability to locate and retrieve data as well as to know exactly what data it has stored.

**Rule 34 – Producing Documents and Electronically Stored Information.** Addresses the format of documents and ESI provided as part of discovery. It provides for delivery of ESI in the format in which it normally appears as a part of regular business activity or in a “reasonably usable form.” The requesting party can state the format in which it prefers the ESI or it may be left to the discretion of the providing party. Since ESI may be stored in a variety of media and in a variety of file formats (e.g., video, sound, photos, e-mails, XML files, data files), organizations must be careful to ensure that they can easily reproduce the data they have in its original format. Note that printing out electronic data is not an acceptable alternative because metadata (information about the data as opposed to the data itself) is also included as a discoverable type of information under the definition of ESI.

**Rule 37 – Safe Harbor Provision.** The safe harbor provision addresses the real possibility that data may be lost or unavailable as a part of routine operations or unavoidable circumstances without incurring any liability for failure to produce information as requested. However, organizations that fail to produce data due to carelessness, ill-defined retention and destruction policies, or mismanagement may face significant liabilities.
The LHR and E-Discovery

The changing legal landscape and the advent of the new e-discovery amendments place new burdens on healthcare organizations as they define and manage electronic versions of the LHR. Disclosure, which is a key function of the electronic LHR for clinical and legal purposes, can no longer remain focused mainly on the documents defined by the organization as being part of its legal record. This "document-centric" approach to defining the LHR was quite reasonable for paper-based records. However, in the era of electronic records, "documents" are virtual entities that are created from underlying data and presented to users as necessary. This requires a different approach, one that is focused on data management more so than physical documents. Since data that make up a single virtual document may reside in multiple systems, which are themselves geographically separate, a data-centric approach to managing organizational information and defining the LHR is required in addition to the traditional document-centric approach.

The data-centric view of the electronic LHR regards the EHR as a collection of data that exists in multiple systems and in multiple formats. The data-centric view recognizes the realities of e-discovery in that disclosures may require organizations to provide information that may include anything from discharge summaries and medication lists to instant messages and e-mail header files.

The data-centric view requires a new approach to information management as well. Managing the LHR within a document-centric, paper-based environment is straightforward and that function naturally resides within the health information management department. Management of the electronic LHR in a data-centric environment requires additional technical skills and closer cooperation between administrative units especially health information management, information technology, and senior managers. It also requires well-defined policies and procedures for (1) identifying all pertinent data across applications such as e-mail, voice mail, instant messaging; (2) marking records for retention or destruction; (3) security management; and (4) disaster recovery. Healthcare organizations must carefully consider the administrative and technical requirements imposed by the e-discovery amendments to the FRCP as they move forward in adopting electronic systems.

Document-Centric Approach to Defining the LHR

When determining the content of the LHR, organizations need to consider internal needs, external requirements, and the level of technology within the organization. Traditionally, organizations relied on the various parts of the paper medical record to determine their legal business record. A listing of this information was incorporated into a policy that was approved for use by the organization and served as the roadmap for disclosure. This
document-centric approach can still be used as long as the complexity of today’s LHR and the healthcare environment, in general, is taken into consideration.

It is important to understand what a business record is.\(^8\) Information documented in a health record is considered by the courts to be hearsay. The business record provides an exception to the hearsay rule and is applied to the health record of a provider organization. This exception allows the courts to receive into evidence health record information that is prepared and kept in the ordinary course of business. In order to be accepted, the record-keeping associated with the health record must conform to certain established guidelines. These guidelines are:

- The record was compiled during the regular course of business.
- The record entries were made promptly.
- The entries were made by an individual or individuals who had first-hand knowledge of the acts, events, conditions, and opinions.
- The organization maintaining the health record utilizes control processes to ensure accuracy and reliability of information.
- The healthcare organization has policies and supporting procedures to protect the record from alteration and tampering.
- The healthcare organization has policies and supporting procedures to prevent loss of stored data.

The LHR should not be confused with the designated record set required by HIPAA.\(^9\) The LHR defines the official business record for evidentiary purposes. The designated record set determines the level of access and amendment rights of individuals under the HIPAA standards. These standards provide rights to individuals to inspect their records, to obtain copies of their records, and to amend medical and billing information that is or may be used for medical decision-making. Although the LHR and designated record set often share the same data, there are differences and it is important for organizations to understand the distinctions. For example, physician super bills or hospital billing claim forms are deemed to be part of the designated record set, but are not part of the LHR.

In light of the new electronic discovery rule and because of the growth of electronic records, all healthcare organizations should be redefining their legal or business record. In addition, any definition that is created should be re-assessed on a regular basis as technology continues to proliferate within the organization. It is recommended to begin with a formal team of key stakeholders who can assess the internal needs, external requirements, and level of organizational technology. This team should determine the LHR definition. Departments and individuals to be considered in this group include:

- Information Technology (IT) Services
- Health Information Management (HIM) Services
- Legal Counsel
- Administrative Services
- Risk Management Services
- Medical Staff Services
• Nursing Services
• Privacy Officer
• Information Security Officer

This group should also be charged with determining the release of information and record retention policies and procedures for the organization. The team should work with the various departments within the organization who are using computerized systems to record and maintain their patient information.

When determining internal needs, what should be considered first and foremost is that the health record serves as a communication tool between clinicians. Regardless of the media used to document this information, this mission continues to serve as one of the primary reasons for maintaining a health record. The record plays other important roles which should also be recognized. For example, the record supports billing for services and serves as the key source of data for clinical quality improvement and outcomes research. It also plays a significant role in the ongoing education of healthcare practitioners. These are important organizational considerations that will need to be taken into account when determining what comprises the record and its use and handling. Of considerable concern will be ease of access to various pieces of patient information due to the hybrid nature of today’s records while organizations move from paper-based record systems to electronic.

From an external perspective, the organization will need to consider federal and state laws and regulations, accrediting body requirements, and the needs of third party payers. In addition, any needs identified due to participation in a RHIO or any type of health information exchange will also need to be taken into account.

From a technology perspective, it is recommended that an organization inventory all patient-identifiable healthcare documentation maintained on the services provided to a patient. The inventory should identify whether the documentation is directly related to patient care or is administrative in nature. The organization should identify all patient-identifiable source data that further supports the provision of care. Lastly, the inventory should identify how the information is maintained. If the same information is maintained in both an electronic and paper format, then the inventory should identify which media will serve as the LHR for evidentiary purposes. If the information is part of the HIPAA designated record set, this should also be indicated. An example of an inventory is displayed in Figure 1.
## Figure 1

### Examples of Patient-identifiable Healthcare Documentation:

<table>
<thead>
<tr>
<th>Document</th>
<th>Manual</th>
<th>Electronic</th>
<th>Permanent Storage (System)</th>
<th>Part of LHR</th>
<th>Part of HIPAA DRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admission Assessment</td>
<td></td>
<td>✓</td>
<td>HIS Assessments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admission Assessment</td>
<td></td>
<td></td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anesthesia Record</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Consent for Treatment</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Documentation Resulting from an Alert, Reminder</td>
<td></td>
<td>✓</td>
<td>HIS Progress Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation Resulting from an Alert, Reminder</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Face Sheet</td>
<td>✓</td>
<td></td>
<td>HIS ADT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Face Sheet</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>History &amp; Physical Exam</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Laboratory Report</td>
<td>✓</td>
<td></td>
<td>HIS Clinical Repository</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laboratory Report</td>
<td></td>
<td></td>
<td>Laboratory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laboratory Report</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Medication Record</td>
<td></td>
<td>✓</td>
<td>Medication Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medication Record</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Patient-submitted documents</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Pharmacy Orders</td>
<td>✓</td>
<td></td>
<td>Pharmacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pharmacy Orders</td>
<td></td>
<td>✓</td>
<td>HIS Orders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pharmacy Orders</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Physician Orders (Other)</td>
<td></td>
<td>✓</td>
<td>HIS Orders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physician Orders (Other)</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Examples of Patient-identifiable Healthcare Documentation:

<table>
<thead>
<tr>
<th>Document</th>
<th>Manual</th>
<th>Electronic</th>
<th>Permanent Storage (System)</th>
<th>Part of LHR</th>
<th>Part of HIPAA DRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan of Care</td>
<td>✔</td>
<td>✔</td>
<td>HIS Plan of Care</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan of Care (Nursing)</td>
<td>✔</td>
<td>Document Imaging</td>
<td>HIS Progress Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Progress Notes (Nursing)</td>
<td>✔</td>
<td>Document Imaging</td>
<td>HIS Progress Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Progress Notes (Physician)</td>
<td>✔</td>
<td>Document Imaging</td>
<td>HIS Progress Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radiology Report</td>
<td>✔</td>
<td>HIS Clinical Repository</td>
<td>Radiology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radiology Report</td>
<td>✔</td>
<td>Document Imaging</td>
<td>Radiology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respiratory Assessment</td>
<td>✔</td>
<td>Document Imaging</td>
<td>HIS Assessments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respiratory Assessment</td>
<td>✔</td>
<td>Document Imaging</td>
<td>HIS Assessments</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Examples of Patient-identifiable Source Data:

<table>
<thead>
<tr>
<th>Document</th>
<th>Manual</th>
<th>Electronic</th>
<th>Permanent Storage (System)</th>
<th>Part of LHR</th>
<th>Part of HIPAA DRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio of Dictation</td>
<td>✔</td>
<td>Digital Dictation</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnostic Films/Images</td>
<td>✔</td>
<td>PACS</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fetal Monitor Strips</td>
<td>✔</td>
<td>HIM Department</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Photographs</td>
<td>✔</td>
<td>Document Imaging</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Photographs</td>
<td>✔</td>
<td>HIS ADT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pathology Slides</td>
<td>✔</td>
<td>Pathology Department</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Videos of Procedure</td>
<td>✔</td>
<td>Surgery Department</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Examples of Administrative Data:

<table>
<thead>
<tr>
<th>Document</th>
<th>Manual</th>
<th>Electronic</th>
<th>Permanent Storage (System)</th>
<th>Part of LHR</th>
<th>Part of HIPAA DRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Trails</td>
<td></td>
<td>✓</td>
<td>HIS</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Birth/Death Certificates</td>
<td></td>
<td>✓</td>
<td>Document Imaging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Birth/Death Registries</td>
<td></td>
<td></td>
<td>Med Record Abstracting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim Form (Technical)</td>
<td></td>
<td></td>
<td>Document Imaging</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Claim Form (Technical)</td>
<td></td>
<td></td>
<td>HIS Patient Accounting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claim Form (Professional)</td>
<td></td>
<td></td>
<td>Document Imaging</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Claim Form (Professional)</td>
<td></td>
<td></td>
<td>HIS Practice Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tumor Registry Data</td>
<td></td>
<td></td>
<td>Tumor Registry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilization Review Records</td>
<td>✓</td>
<td></td>
<td>Case Management Dept.</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Creating an information inventory will allow the organization to identify all information that is being generated and it will serve as a source document for the preparation of policies and procedures related to security, release of information, retention, maintenance, archiving, and eventual destruction of organizational information consistent with federal and state law. The inventory can also aid in disaster planning which will ensure business continuity in the event of a disaster.

**Validity of the LHR**

As noted earlier, an organization must follow established guidelines for record-keeping in order for its electronic health record to be considered for evidentiary purposes. However, this is only part of the story. In order for an electronic record to be truly admissible, an organization must also attest to the trustworthiness of the record. This requires attesting to the following items.10

- The computer is accepted as standard and efficient equipment.
- There is a method of operation for this computer.
- The operators of the computer are competent to operate it.
- There is a method for preparing a record including identifying the sources of information; defining how information is entered and retrieved; defining controls and checks; and defining the tests used to ensure record accuracy and reliability.
- There are methods in place that will inhibit one’s ability to alter a record once complete.
Thus, ensuring the validity of the health record is equally important to ensuring appropriate record-keeping. Example of items to consider for valid records include:

- Reconciliation procedures for interfaced data.
- Appropriate record completion processes.
- Use of electronic signatures.
- Co-signature of documents authored by others.
- Amending completed data.
- Document versioning of changed records.
- Carrying forward information from visit to visit.
- Addressing patient changes to data within the LHR.

As noted, these are examples. There are many other items to consider when designing and using computerized records and careful thought should go into ensuring the accuracy and trustworthiness of the record produced.

The Hybrid Health Record

Although this paper has stressed issues related to the electronic record, the reality is that most healthcare organizations are dealing with hybrid health records at this time. What is a hybrid health record? A hybrid health record is comprised of information that is generated both electronically and manually. It may also include older patient information stored on microfilm or microfiche and as noted throughout this paper, it includes other media compiled and maintained on the care of a patient. With the hybrid health record, both manual and electronic processes are used to manage the information.\textsuperscript{11} Obviously, this introduces a new level of complexity for records management. What was once 100% on paper and centralized is now maintained on multiple types of media and distributed throughout the organization. It is anticipated that it will take many years to fully transition to an electronic record. In addition, for certain types of documentation, there may always be some form of paper. Given these challenges, the complexity of the hybrid environment needs to be suitably addressed in order to assure quality care and to preserve the integrity of the health record.

In the book \textit{The Legal Health Record},\textsuperscript{12} the author documents guidelines for access and disclosure of hybrid health records. These 14 guidelines include:

- Being protected with a rigorous information security structure.
- Supporting organizational initiatives for electronic security audits.
- Allowing the organization to authorize or limit record access.
- Providing access regardless of storage medium for patient care.
- Providing for retrieval on a timely basis without compromising data or confidentiality.
- Bringing together information contained in multiple systems.
- Facilitating retrieval, display, reporting and dissemination of data and information individually, comparatively, and collectively.
• Minimizing the need for printing.
• Facilitating printing, when needed.
• Facilitating electronic requests.
• Giving patients the opportunity to see, copy, and amend information in their designated record set.
• Supporting electronic tracking.
• Supporting a personal health record.
• Supporting the delivery of patient care, decision support, performance improvement, HIM functions, and other organizational business functions.

In the hybrid environment it is important to know where all patient information resides. As noted earlier, this information should be well-documented in order to ensure appropriate access and retrieval, when needed. A record should be kept of all disclosures, both electronic and manual, as patients have a right to know what information was disclosed and to whom, upon request.

**Release of Information**

All medical facilities are required to maintain privacy and confidentiality of protected health information (PHI), including electronic records, paper records, and oral communications. An important element necessary to satisfy this requirement involves establishing policies for releasing PHI. Health information management departments receive numerous requests each day. These requests may be as simple as a telephone request for a patient’s date of discharge or a more time-consuming request for replication of a 16-volume inpatient record. Although verbally verifying a patient’s date of discharge requires considerably less time and resources than the latter request, it is just as important to follow procedures to determine whether the patient’s information should be released. In most cases, a written request must be mailed or faxed to the medical facility in order to obtain PHI. As outlined by HIPAA, a valid request for release of PHI should include the following elements:

• The name of the institution/individual authorized to release the information.
• The name of the institution/individual authorized to receive the information.
• A description of the information to be disclosed that identifies the information in a specific and meaningful fashion, including dates of treatment.
• A description of each purpose for the requested use or disclosure.
• An expiration date, or an expiration event, that relates to the patient or the purpose of the request.
• The signature of the patient (or his/her personal representative) and the date signed.
• A description of the representative’s authority to act on the patient’s behalf (if the patient’s personal representative signs the authorization).

45 C.F.R. §§ 164.501 (Federal Rules of Civil Procedure)\(^\text{13}\) notes the exceptions that allow for release of PHI without the patient’s authorization. These circumstances include requests for information for the purpose of providing treatment to the patient, obtaining payment for healthcare services provided and for the healthcare provider’s internal
operation. Also, state and federal laws may impose specific limitations on disclosure of specific PHI, such as patients admitted to an alcohol or drug abuse program as well as for psychiatric admissions. Some states have similar limitations for HIV/AIDS patients.

Once validity has been verified, the facility reviews the request and sends only the requested information as specified. Documents such as incident reports and records from other hospitals would be excluded, even if the entire record has been requested. Charges may be billed for the copying of records when applicable.

Figure 2 provides examples of requests for PHI and authorization requirements.

**Figure 2**

<table>
<thead>
<tr>
<th>Requesting Party</th>
<th>Scenario</th>
<th>Is Patient Authorization Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
<td>Patient wants a copy of their recent MRI for his/her own personal health record.</td>
<td>Yes</td>
</tr>
<tr>
<td>Insurance Company</td>
<td>Blue Cross/Blue Shield is requesting a copy of the patient’s last inpatient visit.</td>
<td>Yes/No*</td>
</tr>
<tr>
<td>Attorney</td>
<td>The patient is applying for disability and his/her attorney wants copies of outpatient visits for the last year. Patient’s current inpatient attending wants to see previous admissions for this patient.</td>
<td>Yes</td>
</tr>
<tr>
<td>Hospital Staff Physicians</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Risk/Claims Mgmt.</td>
<td>Patient had an incident during the hospital stay that requires follow up by risk management.</td>
<td>No</td>
</tr>
<tr>
<td>Peer Review Organizations</td>
<td>Records are being audited for a medical coding review by a PRO.</td>
<td>No</td>
</tr>
<tr>
<td>Acute Care Hospital</td>
<td>Patient is visiting a neighboring state and was rushed to the ER following an epileptic seizure with loss of consciousness.</td>
<td>Yes/No**</td>
</tr>
</tbody>
</table>

* Depending upon the insurance contract, the patient may have authorized release of all medical information at the time of enrollment in the plan. If that is the case, an authorization would be unnecessary.

** When PHI is requested from another hospital, patient authorization should be required prior to releasing information. However, in emergency or life-threatening situations where the patient is not able to authorize, information may be released prior to receiving authorization.

**Subpoenas**

A subpoena is a written order requiring someone to come before the court to testify. It is common for medical facilities to receive request for PHI in the form of a Subpoena.
Duces Tecum, which requires coming before the court with records or documents named in the order. Depending on the law of the state, subpoenas may be issued by judges, court clerks or even attorneys. Although the form of the subpoena may vary by state, a set of elements which generally should be included are as follows:\textsuperscript{14}

- A docket number.
- The names of the parties (plaintiffs and defendants) involved in the case.
- The name of the court or agency before which the proceeding is being held.
- The details as to when and where the record custodian’s appearance is being requested.
- The documents that must be brought.
- The signature and seal of the official issuing subpoena.

Even if the facility chooses not to disclose the requested PHI, responses to subpoenas are required.\textsuperscript{15} Figure 3 identifies three different ways to respond to a subpoena.

\textbf{Figure 3}

<table>
<thead>
<tr>
<th>Ways to Respond to Subpoenas</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
<tr>
<td>Formally challenge the subpoena, working through your attorney, who may file a motion to quash or modify the subpoena.</td>
</tr>
</tbody>
</table>

\textit{Managing Requests/Subpoenas in a Hybrid System}

As previously mentioned, PHI may include information in electronic records. With the evolving transition from paper to electronic and hybrid systems, facilities must be prepared to accurately and consistently track and reproduce PHI for requests and subpoenas. Additionally, patients have the right to review disclosures of their records, which means providers must keep a log, tracking release of certain PHI. Patients may also request to review their records and make amendments to their records. These aspects of releasing information must also be considered in developing policies and procedures with electronic and hybrid systems.

\textit{Retention, Availability and Destruction of the LHR}

Whether the LHR is maintained on paper or electronically, it needs to be retained based on the organization’s retention schedule. This schedule must be based on the statute of limitations for the state in which the system and organization resides. In addition, the needs of the organization need to be taken into consideration. For example, many teaching facilities choose to retain their records beyond the statute of limitations because
of the teaching and research mission of their organizations. Certainly, all information defined as part of the LHR needs to be retained per statute. In addition, any accreditation requirements of an organization need to be taken into consideration when developing a retention schedule. Besides the LHR, an organization should address retention of other types of health information including diagnostic images, fetal monitor strips, indices such as the master patient index, diagnosis index, operative index, etc. For all information, an established process for destruction should be outlined.

Lastly, multiple registries should also be taken into consideration when developing policies for retention such as the birth register, death register, and register of surgical procedures. These registers should be maintained permanently for the organization and never destroyed. Of special consideration is the replacement of legacy systems, placing legal holds on records, and retaining data from source systems. These areas are explained in more detail below.

**Replacing Legacy Systems**

As records become more automated in nature, and clinical information is recorded and maintained in an electronic format, it is imperative that organizations consider how they will retain the information on a legacy system for legal purposes when it is being replaced. Certainly the information will need to be retained per the statute of limitations and retention schedule of the organization. When determining this retention, it is important to consider that the LHR is more than the organization’s primary healthcare information system. The LHR is a portfolio of integrated systems that maintain different data and files for the organization. All of these systems comprise the LHR and replacement of any one component will necessitate careful consideration of retention of that information.12

**Placing Legal Holds on Records**

The new e-discovery rule requires that organizations place a legal hold on an electronic record when litigation is presented or anticipated.16 This is no different than current practices exercised with the paper record. When a subpoena is presented to an organization maintaining paper records, the record is generally removed from a HIM department’s permanent file and placed under lock and key. The record is kept locked up until the litigation is resolved. Electronic records introduce a new level of complexity that does not exist with the paper record. Since the LHR is a portfolio of many different systems, it will necessitate that the organization’s record custodian have a thorough understanding of the retention and destruction procedures in place for all organizational systems. If systems are set up such that they automatically purge information, then the destruction of the information in question will need to be suspended until the reason to retain the information no longer exists. In addition, an organization will need to ensure that the information cannot be altered in any way so that validity of the information can be attested to when presented in court. This is known as “spoliation” and is addressed in the e-discovery rule. An organization, along with its vendors, will need to attest to the
methods established to prevent destruction, tampering with, alteration or concealment of information.

**Retaining Data from Source Systems**

In healthcare organizations much of the data is generated in source systems and retained in both the source system and secondary and tertiary systems. For example, a radiology information system produces radiology interpretations that are retained in the radiology system along with being retained in the clinical repository of the healthcare information system. Furthermore, this same data can also be stored in a document imaging system. Organizations will need to decide which system will serve as the data source for the LHR. This decision should be documented via organizational policy. It should also be recognized that even though this policy exists within an organization, as electronic information becomes more frequently requested for legal purposes, requests for information from both primary and secondary systems may become the norm in the future.

In summary, it is recommended that all organizations give this topic careful attention. Retention schedules and policies and procedures should be well-documented. Information produced by the Sedona Conference is an excellent source for policy development. This institute develops best practices for legal practices and the electronic record. A free copy of their guidelines can be downloaded from [www.thesedonaconference.org](http://www.thesedonaconference.org). This would be an excellent place to start.

**Data-Centric Issues and the LHR**

The realities of e-discovery require that organizations adopt a data-centric approach to managing information in addition to the traditional document-centric approach used for the LHR. A key reason for the change in approach is that information that in the past was not deemed part of the LHR is increasingly subject to legal scrutiny. A good example of this phenomenon is the Nursing Shift report. Historically, this information was informally kept and used by nursing to convey patient information from shift to shift. As this information becomes more automated, it is now falling under the umbrella of the LHR. Given this, care should be taken in the design, recording, and ongoing maintenance of this and other types of information that historically were not part of the organization’s business record. PDAs used by clinical staff are another example. Clinical information maintained in the units for patient care purposes could easily be the subject of a subpoena. Other areas worth noting are voice files such as the audio of a medical dictation, video files, e-mail, and instant messaging. With e-discovery, these automated files, along with others computerized files, may be open to discovery and requests for this information will become more frequent in the future. Thus, information management policies and procedures must address the storage and management of ALL data stores, regardless of whether they are defined formally as part of the LHR.

The new discovery amendments place specific constraints on the provision of data in response to a subpoena. The amendments require that all data be presented in the format.
in which it existed at the time of its initial use. This has implications for data needing retrieval from an obsolete system as well as for the reporting requirements for current systems. Care must be taken to ensure that complete access to all forms of application data is possible. One practical implication for this would be to avoid systems that have limited reporting capability or that do not permit ready access to all underlying data elements including audit trails.

With the broadening of the scope of data stores that are subject to subpoena under the new e-discovery amendments, there is a new urgency to review compliance with the HIPAA Security Rule. Care must be taken to ensure that that risk assessment procedures for all data stores including threat and vulnerability analyses along with required policies and procedures are applied equally across all systems. For example, deletion of data from a PDA that is critical for a malpractice case could be extraordinarily damaging to an organization. Also, now that federal courts are permitting HIPAA to be used as a “standard of care” for private lawsuits, additional steps must be taken to prevent unauthorized access and unintended disclosures of data whether through theft or laxity in security policies and procedures.

**Metadata**

There are many changes on the horizon that will present new challenges for healthcare organizations in the definition of their LHR. One area frequently talked about is the use of metadata by attorneys who practice litigation. Metadata is data about the data and under the e-discovery rule can be requested. An example of metadata is the time an entry was made in a record. Metadata records this time. If this time does not correlate with the presented facts of a case, then the case can become suspect. Metadata will increasingly be used as a tool to challenge the integrity of the healthcare record. Metadata also identifies when records are accessed and if they have been altered in any way. It will be important for the users of electronic systems to adhere to the guidelines established for business records outlined earlier in this paper. This will ensure the integrity of the information and the integrity of the author who recorded that information in the LHR.

For several years now, clinical decision support has been promoted as a means to ensure quality care and to standardize the care provided to a patient based on evidence that supports best practice. Clinical decision support within an information system provides the physician and other care providers with alerts and reminders. These prompts can help the physician avoid prescribing a contraindicated drug or they can remind a nurse to complete an assessment per policy. They are tools to aid clinicians in providing appropriate, cost-effective care. However, it is becoming increasingly apparent that these tools have the potential to expose the provider to liability if an alert or reminder is ignored by the clinician. It is not the alert or reminder that the courts are questioning, but the clinician’s response to the alert or reminder. It is recommended that all providers document their responses in the LHR so that the rationale for following or ignoring these prompts is documented. In addition, careful thought should go into the selection and use of alerts and reminders. The goal of cost-effective, quality care must be weighed against the associated risk these may cause a provider if the provider chooses to ignore them or
become irritated due to over-use. These tools are highly recommended, but should not be instituted without thoughtful deliberation by the clinicians who will use them.

Preparing for E-Discovery

In preparing for e-discovery, organizations will need to develop a well thought out plan. In addition, it will be imperative for IT, HIM, and the clinical areas using systems to fully understand the systems being utilized. Lastly, it is recommended that organizations maintain only what is vital as anything stored will probably be open to e-discovery in the future. Thus, unless the data has a business or legal reason to be maintained, it is recommended that it be discarded and not permanently stored. Figure 4 offers a few steps in preparing for e-discovery changes.

Figure 4

<table>
<thead>
<tr>
<th>No.</th>
<th>Preparing for E-Discovery Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify all organizational data stores that contain personal health information or clinical information. Be sure to include PDAs, voice-mail, e-mail, videos, along with paper and traditional clinical applications (CPOE, radiology, etc.).</td>
</tr>
</tbody>
</table>
| 2.  | Create a data map that clearly delineates the following for each data store:  
   • Location  
   • Data elements  
   • Application name and version  
   • Data/file formats  
   • Date of initial operation  
   • Date retired from operation  
   • Security management (risk assessments, threats, vulnerabilities, safeguards, back-up/disaster recovery plans)  
   • Operational management (responsible administrative unit; policies and procedures for managing the systems; maintenance schedules; etc.) |
| 3.  | Identify key “documents” within data stores that comprise the self-identified LHR. These will be used for sharing with other providers, billing, and routine legal requests for the patient chart. |
| 4.  | Determine if all systems provide adequate reporting capabilities that will allow access to all data elements in the original format as they would appear during normal use. Also ensure that complete access to all metadata is readily available. |
| 5.  | Review the interactions between IT and HIM to ensure that all data stores are monitored by the respective departments for issues that pertain to their areas of expertise. |
| 6.  | Identify an organizational e-discovery “go to” person for legal action. This individual must understand where data is stored within all systems and understand the business rules associated with each system. These rules define the process for documenting, updating, maintaining, archiving, and eventual destruction of the data residing within each system. This individual will need to answer what is accessible, what is not accessible, and why data may not be accessible in any given system. |
HIMSS wishes to thank the following volunteers for their participation in the creation of this white paper:

Jerome H Carter, MD, Chair HIMSS EHR Adoption Task Force, CEO NTM Informatics, Inc.

Cecilia Backman, Co-Chair HIMSS EHR Adoption Task Force, Consultant

Melissa King, Member HIMSS EHR Adoption Task Force, Clinical Documentation Specialist, Mercy Hospital, Miami, Florida

JoAnn W. Klinedinst, CPHIMS, PMP, FHIMSS
HIMSS Staff Liaison
Enterprise Information Systems Steering Committee

Juanita Threat
HIMSS Staff Liaison
Coordinator, Enterprise Information Systems Steering Committee

References


**Additional Resources**


Developing a Legal Health Record Policy: Appendix A. *Journal of AHIMA.* 2007; 78(9):
