Developing a Legal Health Record Policy

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Health records serve a variety of purposes. Their primary purpose is to document the care and services provided to patients. However, health records must also be maintained for business and evidentiary purposes.

In order to serve as business records, health records must be maintained in a manner that complies with applicable regulations, accreditation standards, professional practice standards, and legal standards. These standards may vary based on care setting, legal jurisdiction, and location.

Therefore, an organization must identify the content required for its legal health record as well as the standards for maintaining the integrity of that content. This applies regardless of the media used to create and store health records—paper, electronic, or hybrid.

This practice brief guides healthcare organizations in creating a legal health record policy for business and disclosure purposes. It provides considerations and questions that organizations transitioning to electronic health records (EHRs) should address. (Additional considerations for specialty institutions and specialty records such as behavioral health are not addressed in this article.)

This practice brief is not intended as legal advice. Organizations should consult with their legal counsel to develop their legal health record policy.

Legal Health Record Policy Template

Policy Name: The Health Record for Legal and Business Purposes

Effective Date:

Departments Affected: HIM, Information Systems, Legal Services, *[any additional departments affected]*

Purpose: This policy identifies the health record of *[organization]* for business and legal purposes and to ensure that the integrity of the health record is maintained so that it can support business and legal needs.

Scope: This policy applies to all uses and disclosures of the health record for administrative, business, or evidentiary purposes. It encompasses records that may be kept in a variety of media including, but not limited to, electronic, paper, digital images, video, and audio. It excludes those health records not normally made and kept in the regular course of the business of *[organization]*.

> *Note:* The determining factor in whether a document is considered part of the legal health record is not where the information resides or its format, but rather how the information is used and whether it is reasonable to expect the information to be routinely released when a request for a complete health record is received. The legal health record excludes health records that are not official business records of a healthcare provider. Organizations should seek legal counsel when deciding what constitutes the organization's legal health record.

Policy: It is the policy of [organization] to create and maintain health records that, in addition to their primary intended purpose of clinical and patient care use, will also serve the business and legal needs of *[organization]*.

It is the policy of [organization] to maintain health records that will not be compromised and will support the business and legal needs of *[organization]*.

Responsibilities

It is the responsibility of *[the health records manager or other designated position]* to:

- Work in conjunction with information services, legal services, and *[other stakeholders]* to create and maintain a matrix or other document that tracks the source, location, and media of each component of the health record. *[Reference an addendum or other source where the health record information is found.]*
- Identify any content that may be used in decision making and care of the patient that may be external to the organization (outside records and reports, PHRs, e-mail, etc.) that is not included as part of the legal record because it was not made or kept in the regular course of business.
- Develop, coordinate, and administer a plan that manages all information content, regardless of location or form that comprises the legal health record of *[organization]*.
- Develop, coordinate, and administer the process of disclosure of health information.
- Devise and administer a health record retention schedule that complies with applicable regulatory and business needs.
- *[Other responsibilities]*

It is the responsibility of the information services department *[or other appropriate department(s)]* to:

- Ensure appropriate access to information systems containing components of the health record
- Execute the archiving and retention schedule pursuant to the established retention schedule
- *[Other responsibilities]*

[Additional responsibilities for other individuals or departments]

Maintaining EHR Integrity

As EHR systems become more prevalent, more healthcare organizations need to redefine their legal health record policy. Many EHR systems have limitations that may affect their use for legal purposes. However, regardless of the media they use, organizations must have a single set of health information that forms their legal health record.

Organizations that have transitioned to or are in the process of transitioning to EHRs must consider the following issues to maintain the integrity of the legal health record. These issues will need to be addressed procedurally. They can either be addressed as part of the legal health record policy or in separate policies.

During the transition to electronic health records, organizations should document the information that comprises the health record for business and legal purposes, the various sources and location of the information, and the media in which the information are maintained. This document can then be used to identify the information that will be disclosed upon receipt of an authorized request for health records.

Health information exchange. Healthcare organizations should develop policies and procedures addressing acceptance and retention of documents, images, waveforms, and other information received from external facilities. Generally physicians should determine the efficacy of the information received. The decision on whether to include the information in the legal health record should be based on its content and clarity. If acceptance is not possible, the policy should further address the retention or destruction of noncompatible information.

Downtime documentation. To ensure an accurate legal record, organizations should develop a procedure addressing documentation when EHR systems are unavailable due to planned or unplanned downtime. All clinical staff should be instructed to immediately begin documenting patient care on downtime health record forms according to the policy. The start and stop times of the downtime should be documented in the health record to ensure accuracy of the legal record.

The documentation process should account for the length of downtime. For example, if the system is unavailable for less than 30 minutes, an organization may decide that the information documented on paper will be entered into the EHR once the system becomes available.

The pros and cons of transferring downtime documentation into the EHR must be fully evaluated. For example, one benefit is having all information in one location with no need to maintain two systems. However, long downtimes could result in large amounts of paper documentation, and it may not be feasible to enter this information at a later date.

A multidisciplinary group of individuals representing physicians, nurses, allied health, HIM, compliance, and IT should be included in this discussion. Organizations may want to seek input from their vendors to ensure that the EHR application meets the organization's requirements for entering information after the fact. Vendors can also advise if their systems can indicate the existence of a separate paper record, if one exists.

Critical data to enter into the EHR post-downtime might include those elements that the EHR uses to calculate totals (e.g., intake and output) and data that have patient safety rules and alerts (e.g., medications, height, and weight). The policy should address the timeliness of data entry post-downtime, staff responsible for entry, and how original paper documents will be retained, entered into the EHR, or scanned.

Document completion (lockdown). Organizations must determine when users can no longer create or make changes to electronic documentation. Organizations with several source systems (i.e., systems that do not automatically record the date and time of entries and systems that allow editing documents without tracking changes) should consider locking down documents at some determined time after a patient encounter. This will help ensure health records are accurate and meet spoliation expectations.

Because EHRs allow users to access the information from anywhere access is allowed, the EHR documentation function must control when an individual can document in an EHR. There may be limitations with how the EHR handles this function, which organizations will need to factor into their policies. Organizations must determine how long the documentation function will be available. The multidisciplinary group should be included in discussions to determine when electronic documentation will be considered complete.

Amendments and corrections. Procedures should address how amendments and corrections should be made to the EHR. Amendments and corrections should be in chronological order and included with the original document both online and in printed format. If possible, the system should clearly identify amendments including date, time, and author. Corrections to the EHR should be visible to anyone with access. Identification and tracking of corrections should not be limited to a background or back-end program visible only to IT staff.

Authentication. The person entering the data should authenticate individual health record entries. Electronic entry should automatically record the person documenting the care with his or her full name and credentials, the date, and time. Consideration should also be given to situations where multiple individuals are responsible for creating documentation. An admission assessment, for example, may contain sections requiring input from a variety of caregivers. An organization's policy should address how this is accomplished in coordination with the functionality within the EHR application.

There may be times when an individual forgets to enter documentation at the time of care delivery and another individual makes entries on his or her behalf. Policy must indicate when this is appropriate and how it will be handled based on functionality within the EHR. To ensure adherence to state regulatory requirements, organizations should also review state-specific guidelines on authenticating orders.

Documents prepared outside the EHR (e.g., transcribed documents and scanned images) should be assigned an electronic signature that is automatically date- and time-stamped. This type of authentication should clearly state "electronically signed" to identify the source of the document. Authentication of each health record entry should be visible to anyone with access. Authentication should not be limited to a background or back-end program visible only to IT staff. Authentications should be readable when EHR documents are printed.

Organizations should also define their cosignature policy and procedures including the positions that require cosignatures. The policy and procedures should outline how and where cosignatures should be documented (e.g., whether the cosignature occurs

in the designated EHR, the source system, or the scanning system). The cosignature method should be evaluated to determine whether documentation will be considered legal if two people need to authenticate the same documentation.

If digital signatures are used in the EHR, staff will not be able to cosign, as the second signature will invalidate the first signature along with the documentation. Organizations may need to consider allowing the first author to indicate that they have reviewed the documentation and the second person to actually authenticate the information. If the EHR does not include digital signatures for authentication, the process of cosigning done on paper should be imitated in the EHR.

Timing of cosignatures should be addressed in policy as well. Some states regulate the timing of cosignatures on verbal orders. The Centers for Medicare and Medicaid Services' guidelines for physicians at teaching hospitals state that "the teaching physicians must review with each resident during or immediately after each visit the beneficiary's medical history, physical exam, diagnosis, and record of tests and therapies."[1] From a legal perspective, cosignatures should not be done once a shift while supervising students as it appears that oversight might not be managed in a timely manner.

Versioning. Organizations must address management of document versions. This will relate primarily to transcribed reports that are made available for viewing prior to authentication or review by the author. Organizations must decide whether all versions of a document will be displayed or just the final version; who has access to the various versions of a document; and how the availability of versions will be flagged in the EHR. A multidisciplinary group of physicians, risk management, HIM, and IT professionals should be included in the discussion.

An organization risks severe legal implications if it is unable to produce the original report after information was initially distributed or made available in the EHR and then later changed or updated. It is acceptable for a draft of a dictated and transcribed note or report to be changed before authentication unless there is reason to believe the changes are suspect and don't reflect actual events or actions.

Organization policy should define the acceptable period of time allowed for a document to remain in draft form before the author reviews and approves it (e.g., 24 to 72 hours). Once a document is no longer considered a draft or has been authenticated, any changes or alterations should be made following the procedures for a correction, late entry, or amendment. The original document must be maintained along with the new revised document.

Metadata. Organizations need to be aware of the metadata stored in their EHR systems. Metadata will not be routinely disclosed as part of the legal health record, but this information could be requested for legal purposes as part of electronic discovery. Organizations should determine how long this information must be kept. Data retention policies should include metadata.

Clinical decision support. Currently there are no generally accepted rules on including decision support such as system-generated notifications, prompts, and alerts as part of the legal record. The decision is up to individual organizations, with input from physicians, legal counsel, risk management, and administration.

At a minimum the EHR should include documentation of the clinician's actions in response to decision support. This documentation is evidence of the clinician's decision to follow or disregard decision support. The organization should define the extent of exception documentation required (e.g., what no documentation means).

Definitions

Organizations may also find it helpful to include the following definitions in their legal health record policy. Other key terms included in the organization's final policy should be defined and added to this list.

Business record: "a recording/record made or received in conjunction with a business purpose and preserved as evidence or because the information has value. Because this information is created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligation or in the transaction of business, it must consistently deliver a full and accurate record with no gaps or additions."[2]

Data: basic facts about people, processes, measurements, and conditions represented in dates, numerical statistics, images, and symbols. An unprocessed collection or representation of raw facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or automatic means.[3]

Data element: a combination of one or more data entities that forms a unit or piece of information, such as patient identifier, a diagnosis, or treatment.[4]

Electronic health record: medical information compiled in a data-gathering format for retention and transferral of protected information via secured, encrypted communication line. The information can be readily stored on an acceptable storage medium such as compact disc.[5]

Evidence: information that a fact finder may use to decide an issue. Information that makes a fact or issue before court or other hearing more or less probable.[6]

Legal health record: AHIMA defines the legal health record as "generated at or for a healthcare organization as its business record and is the record that would be released upon request. It does not affect the discoverability of other information held by the organization. The custodian of the legal health record is the health information manager in collaboration with information technology personnel. HIM professionals oversee the operational functions related to collecting, protecting, and archiving the legal health record, while information technology staff manage the technical infrastructure of the electronic health record."[7]

The legal health record is a formally defined legal business record for a healthcare organization. It includes documentation of healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare organization.[8], [9] The health record is individually identifiable data in any medium, collected and directly used in documenting healthcare or health status. The term also includes records of care in any health-related setting used by healthcare professionals while providing patient care services, reviewing patient data, or documenting observations, actions, or instructions.[10]

Metadata: descriptive data that characterize other data to create a clearer understanding of their meaning and to achieve greater reliability and quality of information. Metadata consist of both indexing terms and attributes.[11]

Original document: an authentic writing as opposed to a copy.[12]

Personal health record: an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure private environment, with the individual determining access rights. The PHR is separate from and does not replace the legal health record of any provider.[13]

Regular course of business: doing business in accordance with the normal practice of business and custom, as opposed to doing it differently because an organization may be or is being sued.[14]

Source systems: The systems in which data were originally created.

- **Primary source system:** an information system that is part of the overall clinical information system in which documentation is most commonly first entered or generated.
- **Source of legal health record:** the permanent storage system where the documentation for the legal health record is held.

Appendix A: Developing a Legal Health Record Policy

The tables below provide examples of a matrix tool that can help organizations identify and track the paper and electronic portions of the legal health record during and up to the full implementation of a paperless environment. Items for special consideration as to whether to include on the matrix may include those listed below. It is up to each individual organization to determine what health information is considered a part of their legal health record.

- **Alerts, reminders, pop-ups**
- **Continuing Care Records** (unless used in the provision of patient care)
- **Administrative data/documents:** patient-identifiable data used for administrative, regulatory, healthcare operations, and payment (financial) purposes

- **Derived data/documents:** information aggregated or summarized from patient records so that there are no means to identify patients.
- **Data/documents:** documentation of patient care that took place in the ordinary course of business by all healthcare providers.
- **Data from source systems:** written results of tests. Data from which interpretations, summaries, notes, flowcharts, etc., are derived.
- **New technologies:** audio files of dictation or patient telephone calls, handwritten nursing shift-to-shift reports, telephone consultation audio files, videos of office visits, and videos of procedures or telemedicine consultation.
- **Personal health records** (PHRs): copies of PHRs that are created, owned, and managed by the patient and are provided to a healthcare organization (s) might be considered part of the legal health record if so defined by the organization.
- **Research records:** organizational policy should differentiate whether research records are part of the legal health record and how these records will be kept.
- **Discrete structured data.** Laboratory orders/refills, orders/medication orders/MARs, online charting and documentation and any detailed charges.
- **Diagnostic image data:** CT, MRI, ultrasound, nuclear medicine, etc.
- **Signal tracing data:** EKG, EEG, fetal monitoring signal tracings, etc.
- **Audio data:** heart sounds, voice dictations, annotations, etc.
- **Video data:** ultrasound, cardiac catheterization examinations, etc.
- **Text data:** radiology reports, transcribed reports, UBS, itemized bills, etc.
- **Original analog document – document image data:** signed patient consent forms, handwritten notes, drawings, etc.

Legal Health Record Matrix

Type of Document	Media Type: Paper (P) or Electronic (E)*	Primary Source System Application (non-paper)	Source of the Legal Health Record	Electronic Storage Start Date	Stop Printing Start Date	Fully Electronic Record (drill down composition)
History and physical	P/E	Transcription system	EHR	1/2/2007	3/2/2007	12/17/2007
Physician orders	E	CPOE system	EHR	1/2/2007	3/2/2007	12/17/2007
EKG	P					

*Includes scanned images

Maintaining the Legal EHR: Verification Legend Document Principles

Report/Document Type	Audit	Authentication	Authorship	Copy/Paste	Amend	Correct	Clarify
Encounter history	O*	O	O	X*	O	O	O
Encounter physical	O	O	O	X	O	O	O
Medical history	O	O	O	X	O	O	O

O* Allowed and monitored-based on reported and randomized audits to determine adherence to policies and procedures for accurate, timely, and complete documentation principles.
X* Prohibited and monitored-based on reported and randomized audits to determine prohibited use of copy and past, pull forward, etc.

Notes

1. Centers for Medicare and Medicaid Services. “Documentation Guidelines for E&M Services.” Available online at www.cms.hhs.gov/MLNEdWebGuide/25_EMDOC.asp.

2. AHIMA e-HIM Work Group on e-Discovery. "New Electronic Discovery Civil Rule." *Journal of AHIMA 77*, no. 8 (Sept. 2006): 68A–H.
3. AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." *Journal of AHIMA 76*, no. 8 (Sept. 2005): 64A–G.
4. Ibid.
5. Ibid.
6. Ibid.
7. Ibid.
8. Amatayakul, Margaret, et al. "Definition of the Health Record for Legal Purposes." *Journal of AHIMA 72,* no. 9 (Oct. 2001): 88A–H.
9. AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes."
10. Ibid.
11. Fenton, Susan, Kathy Giannangelo, Crystal Kallem, et al. "Data Standards, Data Quality, and Interoperability." *Journal of AHIMA 78,* no. 2 (Feb. 2007): 65–68.
12. AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes."
13. AHIMA e-HIM Personal Health Record Work Group. "The Role of the Personal Health Record in the EHR." *Journal of AHIMA 76,* no. 7 (Jul.–Aug. 2005): 64A–D.
14. AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes."

References and Resources

Relevant State and Federal Laws and Regulations

California Civil Discovery Law. Available online at http://californiadiscovery.findlaw.com/index.htm.

Discovery Resources. Available online at www.discoveryresources.org.

"Federal Rules of Civil Procedure." December 1, 2006. Available online at http://judiciary.house.gov/media/pdfs/printers/109th/31308.pdf.

Findlaw. Available online at http://findlaw.com.

The Library of Congress. Thomas. Available online at http://thomas.loc.gov.

LexisNexis. Law Library. Available online at www.lexisnexis.com/applieddiscovery/lawLibrary/default.asp.

National Conference of State Legislatures. Available online at www.ncsl.org.

US Courts. Available online at www.uscourts.gov/rules.

US Courts. "Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure." Available online at www.uscourts.gov/rules/jc09-2000/Summ.htm.

Accreditation Standards

Joint Commission. "The Joint Commission Standards." Available online at www.jointcommission.org/Standards.

Practice Standards

AHIMA Electronic Health Record Practice Council. "Resolution on the Legal Health Record." 2006. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

AHIMA e-HIM Work Group on the Legal Health Record. "Update: Maintaining a Legally Sound Health Record—Paper and Electronic." *Journal of AHIMA 76,* no. 10 (Nov.–Dec. 2005): 64A–L.

AHIMA e-HIM Work Group on the Legal Health Record. "The Legal Process and Electronic Health Records." *Journal of AHIMA 76,* no. 9 (Oct. 2005): 96A–C.

AHIMA Work Group on Electronic Health Records Management. "The Strategic Importance of Electronic Health Records Management." Appendix A: Issues in Electronic Health Records Management. *Journal of AHIMA 75,* no. 9 (Oct. 2004): Web extra.

Black's Law Dictionary 8th ed. 2004. See Hannah v. Heeter, 213 W.Va. 704, 584 S.E.2d 560 (W.Va. 2003).

Cottrell, Carlton. "Legal Health Record: A Component of Overall EHR Strategy." *Journal of AHIMA 78,* no. 3 (Mar. 2007): 56–57, 66.

Kohn, Deborah. "When the Writ Hits the Fan." *Journal of AHIMA 75,* no. 8 (Sept. 2004): 40–44.

McWay, Dana C. Legal Aspects of Health Information Management. Albany, NY: Delmar Publishers, 1997.

Patzakis, John. "How the New Federal Rules Will Likely Change eDiscovery Practice." The Metropolitan Corporate Counsel, June 2006. Available online at www.metrocorpcounsel.com.

Quinsey, Carol Ann. "Is 'Legal EHR' a Redundancy?" *Journal of AHIMA 78,* no. 2 (Feb. 2007): 56–57.

The Sedona Conference Working Group Series. "The Sedona Principles Addressing Electronic Document Production." July 2005. Available online at www.sedonaconference.org.

The Sedona Conference Working Group Series. "The Sedona Conference Glossary for E-Discovery of Digital Information Management." May 2005. Available online at www.sedonaconference.org.

The Sedona Conference Working Group Series. "The Sedona Guidelines for Managing Information and Records in the Electronic Age." September 2005. Available online at www.sedonaconference.org.

The Sedona Conference Working Group Series. "The Sedona Principles Addressing Electronic Document Production." July 2005. Available online at www.sedonaconference.org.

Tomes, Jonathan P. "Spoliation of Medical Evidence." *Journal of AHIMA 76,* no. 9 (Oct. 2005): 68–72.

University of Sydney. "Records Management Services." Available online at www.usyd.edu.au/arms/rms/body.htm.

Withers, Kenneth, J. Esquire Federal Judicial Center and Sedona Conference Observer, MER Conference, Chicago, IL, May 24, 2006.

Prepared by

Members of the AHIMA EHR Practice Council:

Kathleen Addison
Barbara Demster, RHIA
Terri Hall, RHIT
Beth Liette, RHIA
Keith Olenik, MA, RHIA, CHP
Mary Ellen Mahoney, MS, RHIA
Ann Tegen
Lydia Washington, MS, RHIA, CPHIMS
Victoria Weaver, RHIA
Lou Ann Wiedemann, MS, RHIA

Article citation:
AHIMA EHR Practice Council. "Developing a Legal Health Record Policy" *Journal of AHIMA* 78, no.9 (October 2007): 93-97.