Legal Process and Electronic Health Records

Save to myBoK

The custodian of an electronic health record (EHR) has the same concerns as the custodian of a paper health record when the record becomes involved in the legal process. Most often this occurs in some form of lawsuit in which a party seeks to discover and introduce evidence from the record. The custodian must determine whether to release the record, what portions of the record should be released, and whether the record is admissible as evidence.

However, the custodian of an EHR has several additional concerns when an EHR is involved in litigation. These include whether any difference exists between releasing patient data maintained electronically from that maintained on paper, what parts of the EHR should be released, and whether printouts of electronic data qualify as admissible evidence. This practice brief will review the EHR custodian's responsibilities in the legal process.

Definition of the 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."[1]

Who Is the Custodian of the EHR?

The health information custodian is the person who has been designated responsible for the care, custody, and control of the health record for such persons or institutions that prepare and maintain records of healthcare. The official custodian or designee should be authorized to certify records and supervise all inspections and copying or duplication of records. The HIM professional or designee is often considered the custodian of the health record and may be called to testify to the admissibility of the record. He or she may be asked to verify the timeliness and normal business practices used to develop and maintain the health record.[2]

Authentication for Legal Processes

Authentication is an attestation that something, such as a medical record, is genuine. The purpose of authentication is to show authorship and assign responsibility for an act, event, condition, opinion, or diagnosis.[3] Every entry in the health record should be authenticated and traceable to the author of the entry. The Rules of Evidence indicate that the author of the entry is the only one who has knowledge of the entry. The Federal Regulations/Interpretive Guidelines for Hospitals (482.24(c)(1)(i)) require that there be a method for determining that the author did, in fact, authenticate the entry.[4] This process should be defined in HIM written policies and procedures and substantiates the authentication of an entry in a legal process.

If allowed by state, federal, and reimbursement regulations, electronic signatures are acceptable as authentication. Electronic signature technology should provide verification of the identity of the author.[5]

Certifying Health Records when Requested for the Legal Process

The certification process verifies that the copy provided is an exact duplicate of the original. Certification may be provided using a written certification letter stating that the copy provided is an exact copy of the original. State laws may differ in requirements for certification. Generally, a statement and signature of the record custodian are sufficient; however, some states may require a witness or notary signature as well.

There are some simple steps you can take when responding to requests for EHRs for legal process:

1. **Determine if the request is valid**-verify identity and authority of the requestor. Request legal picture identification, such as a driver's license or passport.

2. **Validate that the format of the request meets state legal requirements** for a valid subpoena or court order. Check state law for specific requirements.
3. **Determine the legal power of the document:**

    a. Patient or legal guardian request via phone-information may not be disclosed without written authorization.
    b. Patient or legal guardian request via e-mail-these requests are difficult to authenticate. Organizations should outline a policy to deal with these requests in accordance with state laws.
    c. Patient or legal guardian request via formal HIPAA-appropriate written authorization-information may be disclosed according to patient or legal guardian wishes.
    d. Patient or legal guardian request via fax-same as formal authorization, if state law allows.
    e. Legal request from a lawyer with authorization attached-information may be disclosed.
    f. Subpoena-information may be disclosed depending on state law and hospital or clinic policy.
    g. Court order-information may be disclosed.
    h. In accordance with Health Care Proxy-information may be disclosed to the proxy if the patient is deemed incompetent.
    i. Workers' compensation-information may be disclosed depending on state policy.

4. **Disclose the information to the designated recipient.** The information should be disclosed to the intended recipient according to the patient or legal guardian, court, or lawyer designated on the subpoena or court order or as outlined in number 1, above.

Determining if Healthcare Information May Be Disclosed

Having reviewed and established that the request is HIPAA compliant, determine if the information may be disclosed based on the context of the request received. Be sure to review and verify that federal rules and regulations have been met and that a conflict does not exist with state-specific statute(s). Confirm that state law does not require a subpoena or court order prior to disclosing the information. Verify compliance with pertinent state statutes prior to disclosing the requested information.

If state and federal laws have been satisfied, conduct the appropriate analysis to determine if a signed consent by the patient is required or if the request requires that protected health information be de-identified prior to disclosure. If so, obtain the appropriate authorization from the patient or refer to the disclosure of minimum necessary information to comply with law enforcement type requests.

At this time, paper is generally an acceptable means to submit copies; however, organizations may want to refer to specific state law for the availability of alternative methods, if applicable. Examples of electronic disclosures include the creation of media such as electronic faxing, CD, DVD, PC-to-PC transmissions, and digital images.

Since federal and state laws will be challenged with the need to address the electronic disclosure of protected health information, routine assessment of acceptable alternative options to comply with such disclosures is recommended. If conflict exists, guidance should be sought from legal counsel for further clarification. The HIPAA security rule should be referenced if the information is released electronically. Appropriate safeguards must be in place if the transaction is covered by the security rule.

Unless otherwise directed, a response in a paper format as the certified copy is considered acceptable. State law should be evaluated to ensure that information is not required in a format other than paper. If submission of the information is recommended or required in another format, confirm whether it is possible to meet these terms based on hospital policy and procedure.

Information that May Be Disclosed for the Discovery Process

Healthcare organizations involved in a lawsuit are subject to the discovery phase of the legal process. Parties involved in a lawsuit can obtain or discover any nonprivileged matters including EHRs that are relevant to the lawsuit. Information or documentation is discoverable even if inadmissible at trial if it is "reasonably calculated" to lead to discovery of admissible evidence.

Processes used in discovery include subpoenas, depositions, interrogatories, request for admissions, and production of documents. The electronic era has changed the way discovery is conducted. Paper is no longer the only source of

documentation to be disclosed. Computer files, erased files, and e-mail can also be subpoenaed. The most common discovery method to discover EHRs is to serve the healthcare organization with a subpoena duces tecum.

Every state has established time frames to comply with the discovery request. It is vital that organizations adhere to these dates. The custodian should consult with the organization's attorney for advice on disclosure of healthcare information. The attorney may authorize disclosure or seek protective relief from a court.

Admissibility of Health Records

Historically, health records were considered hearsay and inadmissible in legal proceedings. However, the Federal Rules of Evidence and the Uniform Rules of Evidence codified the business records exception to the hearsay rule, thereby allowing health records to be used at trial.[6]

The key to admissibility of business records at trial is that they are prepared and maintained in accordance with the Federal Rules of Evidence (803(6)). The person testifying or certifying the records for trial must be conversant with the policies and the processes used to ensure accuracy of the records.[7]

Printing Documents

The HIM department should promulgate a policy that provides for a consensus-driven schedule and migration path for the transition of each record set (e.g., diagnostic reports from laboratory and radiology and transcribed reports) from paper through hybrid to an EHR system. This transition schedule must include time frames to stop or disable printing of these record sets predicated on agreed-upon criteria being met (e.g., EHR access, EHR uptime, and availability).

The printed document policy must include the formal processes for review and (if warranted) approval-control over new requests for access and printing from the EHR. Additionally, the policy should designate where copies of an EHR may be printed in an organization coupled with methods to control or dispose of paper copies immediately following authorized use.

The printing of electronic health record sets by authorized users should include a watermark or automated label with the following information:

- Confidential health information
- Instructions for use, such as "do not file in patient record," "do not remove from facility," or "discard copy in designated disposal area"
- For all unauthenticated reports, indication that the report has not been reviewed for accuracy or authenticated

If the EHR system allows, standard sets for release types should be predefined in the system. If this is not possible, a printing matrix must be developed that coincides with the organization's EHR migration and transition plan.

Information such as data released from the nursing units for patient transfers must be generated from the published features of the electronic software and should not include screen prints.

As custodian of the medical record and EHR, HIM professionals should have control over subsequent printing of paper versions of the medical record or EHR pursuant to authorized release of protected health information. HIM professionals should ensure that there are defined policies, audit trails, and controls over the printing of the medical record.

Advocacy for Uniform Legislation

It is clear from the variation in state laws that HIM professionals have an opportunity to be advocates for consistent, comprehensive federal regulations.

Becoming an advocate is as easy as phoning, writing, or e-mailing your elected representatives about the need for consistent, comprehensive federal regulations regarding the release of health information. AHIMA's Advocacy Assistant helps identify elected officials, information on how to contact them, and provides sample letters (log on at www.ahima.org/dc). Check with your component state association to determine which activities it is involved in and become a volunteer. Support AHIMA's Hill Day activities. Read local newspapers and carry the message to your community and work setting.

Notes

1. AHIMA. "Update: Guidelines for Defining the Health Record for Disclosure Purposes." *Journal of AHIMA* 76, no. 8 (2005): insert.
2. AHIMA. "Maintaining a Legally Sound Health Record." *Journal of AHIMA* 73, no. 2 (2002): insert.
3. Ibid.
4. Ibid.
5. Ibid.
6. Skupsky, Donald S. and John C. Montana. *Law Records and Information Management: The Court Cases*. Denver, CO: Information Requirements Clearinghouse, 1994, 40.
7. Ibid.

Appendix A: Legal Process Glossary of Terms

Abstract: A condensation of a record.

Administrative agency: created by statute or the Constitution. They may hear disputes arising from administrative law. A common example would be a case dealing with workmen's compensation. Administrative law: Rules and regulations developed by various administrative bodies empowered by Congress. This falls under the umbrella of public law.

Administrative regulation: a rule issued by an administrative agency to regulate the area in which Congress created the agency to execute governmental policy. Courts rank regulations below statutes when they conflict, but otherwise regulations have the force of law.

Arbitration: a dispute that is submitted to a third party or panel of experts outside the judicial trial system. All parties involved in the dispute must agree to have their differences heard and settled by an arbitrator or arbitration panel and agree that the settlement will be binding.

Authentication: an attestation that something, such as a medical record, is genuine. Authentication refers to both verifying a computer user's identity and professional responsibility for the entries in the medical record.

The purpose of authentication is to show authorship and assign responsibility for an act, event, condition, opinion, or diagnosis. Entries in the healthcare record should be authenticated by the author.[1]

Verification of the identity of a user or other entity is a prerequisite to allowing access to information systems.[2]

Business records: an exception to the hearsay rule that permits the court to receive into evidence records prepared and kept in the regular course of business. Medical records fall under this exception provided that method of record keeping conforms to certain established guidelines:

- The record was made in the regular course of business.
- The entries in the record are made promptly.
- The entries were made by the individual within the enterprise with first-hand knowledge of the acts, events, conditions, and opinions.
- Process controls and checks exist to ensure the reliability and accuracy of the record.
- Policies and procedures exist to protect the record from alteration and tampering.
- Policies and procedures exist to prevent loss of stored data.

Case law: law originating from court decisions where no applicable statutes exist; also known as common law.

Confidentiality: protection given to health records and other patient information to guard personal, private information about patients and their care.

Consent to use and disclose information: written permissions given by a patient to a healthcare provider to use and disclose healthcare information for the purpose of treatment, payment, or healthcare operations.

Court order: the power of a court jurisdiction, whether state or federal, to order the production of medical records without the patient's informed consent, as opposed to a subpoena, which may be signed by a lawyer.

Custodian of records (aka record custodian): a person who has charge or custody of an institution's records whether stored in paper or electronic format.

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.

Database: a collection of data organized for rapid search and retrieval.

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

Data entity: a discrete form of data, such as a number or a word.

Data integrity: state of data being complete, accurate, consistent, and up to date.

Defendant: individual or company that is the object of a lawsuit.

Deposition: a discovery device under which an attorney questions a witness under oath to learn about matters in the case and to preserve testimony for use at a subsequent testimony.

Digital signature: a block of data that is appended to a message in such a way that the recipient of the message can verify the contents and verify the originator of the message.

Digital signatures apply an algorithm to an electronic document, yielding a unique string of characters known as a message digest. The digest uses private key encryption, and the signature is placed on the electronic document.

Discovery: stage in the litigation process during which both parties use strategies to discover information about a case, the primary focus of which is to determine the strength of the opposing party's case. Discovery may involve requests for admissions, interrogatories, subpoenas, and other methods of discovering potential evidence.

Discovery process: compulsory disclosure of pertinent facts or documents to the opposing party in a civil action, usually before a trial begins.

Duplicate: one of two or more documents that are the same. Many state and federal laws provide that certain duplicates are duplicate originals and admissible in evidence to the same extent as an original. A common example of a duplicate is an imaged record.

Electronic health record (EHR): medical information compiled in a data-gathering format for retention and transferal of protected information via a secured, encrypted communication line. The information can be readily stored onto an acceptable storage medium, such as a compact disk.

Electronic medical record (EMR): an electronic system to automate paper-based medical records.

Electronic signature: technology that uses a unique personal identification number, electronic identification, or biometric scans to place a signature on an electronic document.

Emancipated minor: an individual not of the age of majority but who is given adult status due to life events in accordance with the applicable statutes (e.g., high school graduate, not cohabitating with a parent or legal guardian, member of the US military, is or has been legally married or divorced, is or has been pregnant).

Enumeration: to count off or designate one by one; to list.

Encryption: method of scrambling data so that they cannot be read unless uncoded. A method of securing data by transforming data into a coded format that cannot be accessed without the appropriate decoding mechanism.

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

Health information: in HIPAA privacy provisions, any information (oral or recorded) that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and relates to the physical or mental health of an individual, the provision of healthcare to an individual, or payment for the provision of healthcare.

Hearsay: general statements made outside of court not admissible as evidence in a court proceeding.

Individually identifiable health information: under HIPAA, a subset of health information (see above), including demographic information collected from an individual. The information:

- Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse
- Relates to past, present, or future physical or mental health or condition of an individual, the procession of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual
- Identifies the individual
- Is a reasonable basis to believe the information can be used to identify the individual

Integrity: correctness. Verification that information remains in its original form and has not been altered, manipulated, or modified in an unauthorized manner.

Interrogatories: a discovery device in which one party asks written questions of another, such as the name of the individual responsible for the proper maintenance of your medical records.

Law enforcement: the detection and punishment of violations of the law.

Legal process: all of the summons or writs that are issued by a court during a legal action, or by an attorney in the name of the court but without court review.

Legal representatives: a parent, guardian, or other person who has authority to act on behalf of a minor patient in making decisions related to healthcare unless the minor patient can legally consent to healthcare services without the consent of an adult. For adult patients, legal representative means the legal guardian of an incompetent patient, the healthcare agent designated in an incapacitated patient's healthcare power of attorney, or the personal representative or spouse of a deceased patient. If no spouse survives a deceased patient, legal representative also means an adult member of the deceased patient's immediate family.

Liability: legal responsibility, often with financial repercussions, for any adverse occurrence. Enforceable by civil remedy or criminal punishment.

Media: the materials upon which information is stored such as microfilm or optical disk. Any physical places that store or have the capacity to store information.[3]

Medical record: a record that identifies the patient and documents the diagnosis and care the patient received.

Microfilm: a photographic storage medium on which documents can be greatly reduced in size.

Minor: a person who has not yet reached the age of majority so as to be considered an adult by law.

Motion to quash: the procedural device used to challenge the validity and seeking to nullify a subpoena.

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

Peer review: scrutiny of a healthcare professional by other such professionals to determine whether he or she is qualified to practice his or her profession in a facility and to identify and remedy patterns of unacceptable behavior.

Plaintiff: individual who brings a lawsuit.

Protected health information: according to HIPAA, any information, whether oral or recorded in any form or medium, that (1) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and (2) relates to past, present, or future physical or mental health or condition of an

individual, the procession of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual.

Psychotherapy notes: under the HIPAA privacy rule, notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the content of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individuals medical record. Notes exclude medication prescription and monitoring, counseling session start or stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. The privacy rule gives such notes extra protection as may state law.

Record: the preservation of information or data on some storage medium so that it may be read at some future time.

Record custodian (aka custodian of records): a person who has charge or custody of the institution's records whether stored in paper or electronic format.

Record retention program: a facility's plan that specifies how long the facility keeps its records in accordance with the applicable regulatory statutes.

Regular course of business: doing business in accordance with your normal practice and custom, as opposed to doing it differently because you may be sued or are being sued.

Regulation: a rule issued by a government agency other than the legislature. Unless a regulation conflicts with a constitution or a statute, it has the force of law.

Request for admissions: a pretrial discovery device in which one party requests the other to admit deny or object to certain facts, such as that a medical record was kept in the regular course of business.

Res ipsa loquitor: an exception to the general principle that a patient must prove negligence in order to establish liability. The thing speaks for itself. The doctrine is applicable where a court determines, as a matter of law, that the occurrence is such as in the ordinary course of things would not have happened if the party exercising control or management had exercised proper care.

Res judicata: a doctrine that courts follow to avoid duplicate litigation and conflicting decisions which means an issue that has been settled by a judgment.

Respondeat superior: the doctrine holding an employer or principal liable for the employee's wrongful acts. Let the superior make the answer.

Retention schedule: a document specifying which records an entity will maintain and for how long. Generally a retention schedule is drawn up in conjunction with state and federal retention requirements.

Risk management: oversight of the medical, legal, and administrative operations within a healthcare organization to minimize its exposure to liability.

Rules of evidence: court or administrative agency rules that specify what evidence a fact-finder may consider and under what circumstances.

Signature: with respect to an electronic health record, the verification by a user generated by a private key.

Spoliation (of evidence): the intentional destruction, alteration, or concealment of potential evidence. Spoliation may have such adverse consequences as a court order instructing the jury that they may presume the document was adverse; discovery sanctions, such as fines; or even a separate lawsuit.

Subpoena ad testificandum: a written order commanding a person to appear and to give testimony at a trial or other judicial or investigative proceeding.

Subpoena duces tecum: a written order commanding a person to appear, give testimony, and bring all documents, papers, books, and records described in the subpoena. The devices are used to obtain documents during pretrial discovery and to obtain testimony during trial.

Subpoena validity: those authorized to issue a subpoena vary from state to state. A subpoena usually contains the following:

- Name of the court (or other official body in which the proceeding is being held)
- Names of the plaintiff and the defendant
- Docket number of the case
- Date, time, and place of the requested appearance
- Specific documents sought (if a subpoena duces tecum)
- Name and telephone number of the attorney who caused the subpoena to be issued
- Signature or stamp and seal of the official empowered to issue the subpoena

Notes

1. AHIMA. "Maintaining a Legally Sound Health Record." *Journal of AHIMA* 73, no. 2 (2002): insert.
2. Amatayakul, Margret, Steven Lazarus, Tom Walsh, and Carolyn Hartley. *Handbook for HIPAA Security Implementation*. Chicago, IL: AMA Press, 2004.
3. Ibid.

Prepared by

Wanda Bartschat, MSA, RHIA
Alicia Blevins, RHIA
Lauren Burnette, RHIA
Kerry Costa, RHIA
Michele D'Ambrosio, MBA, RHIA
Gladys Glowacki, CCHRA(C)
Karen B. Griffin
Marina Katrompas
Frances LaPrad, RHIT, CPHQ
Susan Manning
Meg McElroy, RHIA
Randall L. Patton, RHIA
Carol Ann Quinsey, RHIA, CHPS
Barbara J. Riesser, RN, CCS, CCS-P, CPC
Joseph J. Russo, JD, Esq
Janet Sayer, JD, MS, RHIA
Kathleen Schleis, RHIA, CHP
Rita Scichilone, MHSA, RHIA, CCS, CCS-P, CHC
Barbara Ann Thompson, RHIT
Jonathan P. Tomes, JD

Acknowledgments

AHIMA e-HIM Work Group on Defining the Legal Health Record
Kathleen A. Frawley, JD, MS, RHIA
Andrea B. Thomas, MBA, RHIA

This work group was supported by a grant to the Foundation of Research and Education of AHIMA (FORE) from Precyse Solutions, Inc.

Article citation:
AHIMA e-HIM Work Group on Defining the Legal Health Record. "The Legal Process and Electronic Health Records." *Journal of AHIMA* 76, no.9 (October 2005): 96A-D. [expanded online version]
