Maintaining a Legally Sound Health Record: Paper and Electronic

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

The health record is the legal business record for a healthcare organization. As such, it must be maintained in a manner that follows applicable regulations, accreditation standards, professional practice standards, and legal standards. The standards may vary based on practice setting, state statutes, and applicable case law. An attorney should review policies related to legal documentation issues to ensure adherence to the most current standards and case law.

HIM professionals should fully understand the principles of maintaining a legally sound health record and the potential ramifications when the record's legal integrity is questioned. This practice brief will review the legal documentation guidelines for entries in and maintenance of the health record—both paper and electronic. Many of the guidelines that originally applied to paper-based health records translate to documentation in electronic health records (EHRs). In addition, new guidelines and functionalities have emerged specific to maintaining legally sound EHRs. It is of the utmost importance to maintain EHRs in a manner that will support a facility's business and legal processes, otherwise duplicate paper processes will need to be maintained.

AHIMA convened an e-HIM® work group to re-evaluate and update the 2002 practice brief "Maintaining a Legally Sound Health Record" to address the transition many organizations face in the migration from paper to hybrid to fully electronic health records. Issues unique to EHRs are addressed specifically if they are different or require expansion. Many organizations use a hybrid record (which includes both paper and electronic documentation), scanning paper documents into an electronic document management system. Even though a scanned document ends up in an electronic state, the documentation principles for paper-based records still apply. If there are unique issues for scanned records, they are specified in this brief.

Authentication for Legal Admissibility

Generally, statements made outside the court by a party in a lawsuit are considered hearsay and not admissible as evidence. Documentation in the health record is technically hearsay; however, Federal Rules of Evidence (803(6)) and the Uniform Business and Public Records Act adopted by most states allow exception to the hearsay rule for records maintained in the regular course of business, including health records. All records must be identified and authenticated prior to admissibility in court.

Four basic principles must be met for the health record to be authenticated or deemed admissible as evidence. The record must have been:

- Documented in the normal course of business (following normal routines)
- Kept in the regular course of business
- Made at or near the time of the matter recorded
- Made by a person within the business with knowledge of the acts, events, conditions, opinions, or diagnoses appearing in it

EHRs are admissible if the system that produced them is shown to be accurate and trustworthy. The Comprehensive Guide to Electronic Health Records outlines the following facts to support accuracy and trustworthiness:

- Type of computer used and its acceptance as standard and efficient equipment
- The record's method of operation
- The method and circumstances of preparation of the record, including:

- The sources of information on which it is based
- The procedures for entering information into and retrieving information from the computer
- The controls and checks used as well as the tests made to ensure the accuracy and reliability of the record
- The information has not been altered[1]

As EHRs become more commonplace, the federal courts are beginning to differentiate the standards to be applied to authenticate EHRs, based on the type of information stored. For example, when a computer record contains the assertions of a person, such as a progress note or dictated report, the record must fit within the hearsay exception to be admissible. These records are referred to as computer-stored.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Examples may include decision-support alerts and machine-generated test results. The admissibility issue here is not whether the information in the record is hearsay, but whether the computer program that generated the record was reliable and functioning properly (a question of authenticity). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business.

Testifying about Admissibility

Typically, the health record custodian is called upon to authenticate records by providing testimony about the process or system that produced the records. An organization's record-keeping program should consist of policies, procedures, and methods that support the creation and maintenance of reliable, accurate records. If so, the records will be admissible into evidence.

Electronic and imaged health records. Case law and the Federal Rules of Evidence provide support to allow the output of an EHR system to be admissible in court. The rule states "if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"[2] As a result, an accurate printout of computer data satisfies the best evidence rule, which ordinarily requires the production of an original to prove the content of a writing, recording, or photograph. Organizations that maintain EHRs should clearly define those systems that contain the legal EHR or portions of the EHR. Each of these systems should be configured and maintained, ensuring that entries originated in a manner consistent with HIM principles and their business rules, content, and output meet all standards of admissibility.

An important component of this effort is to establish methods to authenticate the electronic data stored in the EHR, namely to verify that data has not been altered or improperly modified consistent with Federal Rules of Evidence. HIPAA security implementation standards require organizations to authenticate protected electronic health information as a means of ensuring data integrity, including data at rest and transmitted data. Cryptographic applications commonly used to authenticate include message authentication codes and digital signatures.

Authorship

Authorship is the origination of recorded information. This is an action attributed to a specific individual or entity, acting at a particular time. Authors are responsible for the completeness and accuracy of their entries in the health record.

AHIMA recommends that anyone documenting in the health record (regardless of media) have the authority and right to document as defined by the organization's policies and procedures. Individuals must be trained and competent in the fundamental documentation practices of the organization and legal documentation standards. Organizations should define the level of record documentation expected of their practitioners' licensure, certification, and professional experience.

Authentication of Entries

Authentication shows authorship and assigns responsibility for an act, event, condition, opinion, or diagnosis. Health Level Seven (HL7) has defined a legally authenticated document or entry as "a status in which a document or entry has been signed manually or electronically by the individual who is legally responsible for that document or entry."[3] Each organization should establish a definition of a legally authenticated entry and establish rules to promptly authenticate every entry in the health record by the author responsible for ordering, providing, or evaluating the service furnished.

Many states have regulations or rules of evidence that speak to specific characteristics required for authenticating entries. Before adopting any authentication method other than written signature, the organization should consult state statutes and regulations regarding authentication of entries. The medical staff bylaws (where applicable) or organizational policies should also approve computer authentication and authentication of scanned entries and specify the rules for use. Organizations automating health records in a state that does not expressly permit the use of computer keys to authenticate should seek permission from the applicable state agency.

Types of Signatures

For paper-based records, acceptable methods to identify the author generally include written signature, rubber stamp signature, or initials combined with a signature legend on the same document. Acceptable methods of identifying the author in EHRs generally include electronic or digital signatures or computer key. Acceptable methods for authenticating a scanned document may follow paper or electronic guidelines.

Signatures are the usual method to authenticate entries in a paper-based record. The Centers for Medicare and Medicaid Services (CMS) Interpretive Guidelines for Hospitals 482.24(c)(1) require name and discipline at a minimum. A healthcare organization can choose a more stringent standard requiring the author's full name with title or credential to assist in proper identification of the writer. Healthcare organization policies should define the acceptable format for signatures in the health record.

A **countersignature** requires a professional to review and, if appropriate, approve action taken by another practitioner. Countersignatures should be used as required by state licensing or certification statutes related to professional scope of practice. The entries of individuals who are required to practice under the direct supervision of another professional should be countersigned by the individual who has authority to evaluate the entry. Once countersigned, the entry is legally adopted by the supervising professional as his or her own entry. For example, licensed nurses who do not have the authority to supervise should not countersign an entry for a graduate nurse who is not yet licensed. Practitioners who are asked to countersign should do so carefully. The CMS Interpretive Guidelines for Hospitals (482.24(c)(1)(I)) require that medical staff rules and regulations identify the types of documents or entries nonphysicians may complete that require a countersignature by a supervisor or attending medical staff member.

Rubber stamp signatures are acceptable if allowed by state, federal, and reimbursement regulations. From a reimbursement perspective, some fiscal intermediaries have local policies prohibiting the use of rubber stamp signatures in the health record even though federal regulation allows their use. Healthcare organization policies should state if rubber stamp signatures are acceptable and define the circumstances for their use after review of state regulations and payer policies.

When rubber stamp signatures are used, a list of signatures should be maintained to cross reference each signature to an individual author. The individual whose signature the stamp represents should sign a statement that he or she is the only one who has the stamp and uses it. There can be no delegation to another individual for use of the stamp. Sanctions should be established for unauthorized or inappropriate use of signature stamps.

Initials can be used to authenticate entries such as flow sheets, medication records, or treatment records. They should not be used for such entries as narrative notes or assessments. Initials should never be used for entries where a signature is required by law. Authentication of entries by only initials should be avoided because of the difficulty in positively identifying the author of an entry based on initials alone and distinguishing that individual from others having the same initials.

If a healthcare organization chooses to use initials in any part of the record for authentication of an entry, there should be corresponding full identification of the initials on the same form or on a signature legend. A signature legend may be used to identify the author and full signature when initials are used to authenticate entries. Each author who initials an entry must have a corresponding full signature on record. For EHRs, apply recommendations for computer key signatures.

Fax signatures. The acceptance of fax documents and signatures is dependent on state, federal, and reimbursement regulations. Unless specifically prohibited by state regulations or healthcare organization policy, fax signatures are acceptable. The Federal Rules of Evidence and the Uniform Rules of Evidence allow for reproduced records used during the course of business to be admissible as evidence unless there is a genuine question about their authenticity or circumstances dictate that the originals be admissible rather than the reproductions. Some states have adopted the Uniform Photographic Copies of

Business and Public Records Act, which allows for the admissibility of a reproduced business record without the original. The Uniform Business Records as Evidence Act also addresses the admissibility of reproductions. When a fax document or signature is included in the health record, the document with the original signature should be retrievable from the original source.

Electronic signatures are acceptable if allowed by state, federal, and reimbursement regulations. In 2000 the US government passed the Electronic Signatures in Global National Commerce Act, which gives electronic signatures the same legality as handwritten signatures for interstate commerce. State regulations and payer policies must be reviewed to ensure acceptability of electronic signatures when developing healthcare organization policies. ASTM and HL7 have standards for electronic signatures. Electronic signature software binds a signature or other mark to a specific electronic document. It requires user authentication such as a unique code, biometric, or password that verifies the identity of the signer in the system.

If electronic signatures are used in the EHR, the software program or technology should provide message integrity—assurance that the message sent or entry made by a user is the same as the one received or maintained by the system. If electronic signatures are used in the EHR, the software program or technology should also provide for nonrepudiation—assurance that the entry or message came from a particular user. It will be difficult for a party to deny the content of an entry or having created it.

A **digital signature** provides a digital guarantee that information has not been modified, as if it were protected by a tamper-proof seal that is broken if the content were altered.[4]

A **computer key** or other code is an acceptable method to authenticate entries in an EHR if allowed by state, federal, and reimbursement regulations. When computer codes are used, a list of codes should be maintained that links each code to an individual author. Authorized users should sign a statement ensuring that they alone will use the computer key. Sanctions should be established for unauthorized or inappropriate use of computer key.

Digital ink or digitized signatures differ from electronic signatures in that they use handwritten signatures on a pen pad. The actual written signature is converted into an electronic image. Digitized signatures are acceptable if allowed by state, federal, and reimbursement regulations. State regulations and payer policies must be reviewed to ensure acceptability of digitized signature when developing healthcare organization policies.

Specific Authentication Issues

There are a number of unique authentication scenarios and issues that organizations must address.

Auto-authentication. The author of each entry should take specific action to verify that the entry is his or her entry or that he or she is responsible for the entry and that the entry is accurate. Computer technology has provided opportunities to improve the speed and accuracy of the authentication process. However, authentication standards still require that the author attest to the accuracy of the entry. As a result, any auto-authentication technique that does not require the author review the entry is likely to fall short of federal and state authentication requirements and place the organization at legal risk.

Failure to disapprove an entry within a specific time period is not an acceptable method of authentication. A method should be in place to ensure that authors authenticate dictated documents after they are transcribed. Auto-authentication methods where the dictator is deemed to have authenticated a transcribed document if no corrections are requested within a specified period of time are not recommended.

Authenticating documents with multiple sections or completed by multiple individuals. Some documentation tools, particularly assessments, are set up to be completed by multiple staff members at different times. As with any entry, there must be a mechanism to determine who completed information on the document. At a minimum, there should be a signature area at the end of the document for staff to sign and date. Staff who have completed sections of the assessment should either indicate the sections they completed at the signature line or initial the sections they completed.

Some EHR documentation tools, particularly assessments, are also intended to be completed by multiple staff members at different times. Here too there must be a mechanism to determine who completed information in the document.

Documenting care provided by a colleague. Individuals providing care are responsible for documenting that care. Documentation must reflect who performed the action. Patient care carried out by another provider, as well as clinical information supplied by another person to the writer of the entry, should be clearly attributed to the source.

Some EHR systems provide the capability to indicate differences between the person who enters information and the author of a document. In either case, documentation must reflect who performed the action. If documentation of care is entered for another provider, at a minimum the document should contain the identification of the person who entered the information along with the date the entry was made and authentication by the actual provider of care with the corresponding date of authentication.

Documentation Principles

Regardless of the format, text entries, canned phrases, or templates should follow fundamental principles for the quality of the entry. Content should be specific, objective, and complete.

Use **specific** language and avoid vague or generalized language. Do not speculate. The record should always reflect factual information (what is known versus what is thought or presumed), and it should be written using factual statements. Examples of generalizations and vague words include patient doing well, appears to be, confused, anxious, status quo, stable, as usual. If an author must speculate (i.e., diagnosis is undetermined), the documentation should clearly identify speculation versus factual information.

Chart **objective** facts and avoid using personal opinions. By documenting what can be seen, heard, touched, and smelled, entries will be specific and objective. Describe signs and symptoms, use quotation marks when quoting the patient, and document the patient's response to care.

Document the **complete** facts and pertinent information related to an event, course of treatment, patient condition, response to care, and deviation from standard treatment (including the reason for it). Make sure the entry is complete and contains all significant information. If the original entry is incomplete, follow guidelines for making a late entry, addendum, or clarification.

Other Documentation Issues

Organizational policies must address the use of approved abbreviations in the health record. A second emerging documentation issue is the cut and paste functionality in EHRs. Organizations must consider whether they will allow cutting and pasting and how they will handle cut-and-paste content from one entry to another.

Use of abbreviations. Every healthcare organization should have a goal to limit or eliminate the use of abbreviations in medical record documentation as part of its patient safety efforts. Healthcare organizations should set a standard for acceptable abbreviations to be used in the health record and develop an organization-specific abbreviation list. Only those abbreviations approved by the organization should be used in the health record. When there is more than one meaning for an approved abbreviation, chose one meaning or identify the context in which the abbreviation is to be used. Every organization should have a list of abbreviations, acronyms, and symbols that should not be used.

EHRs. Abbreviations should be eliminated as information is formatted for the EHR. Electronic order sets, document templates for point-and-click or direct charting, voice recognition, or transcribed documents can be formatted or programmed to eliminate abbreviations.

Cut, copy, and paste functionality is not generally regarded as legitimately available in the paper record. Analogous functions in paper records include photocopying a note, cropping it, and pasting or gluing it into the record. The primary issue with the cut, copy, and paste functionality in the EHR is one of authorship—who is the author and what is the date of origination for a copied entry?

Cutting and pasting saves time; however, it also poses several risks:

- Cutting and pasting the note to the wrong encounter or the wrong patient record
- Lack of identification of the original author and date

- The acceptability of cutting and pasting the original author's note without his or her knowledge or permission

Organizations should develop policy and procedures related to cutting, copying, and pasting documentation in their EHR systems. By following these guidelines and training clinical staff, providers can allow cutting and pasting within certain boundaries.

- In general, the original source author and date must be evidenced in copied information. If users are allowed to copy forward from a previous entry by another person, an attribution statement referring to the original document, date, and author should be attached or incorporated where applicable.
- Cutting, copying, and pasting must not be perceived as "OK unless proven otherwise" but instead should be considered "not OK until proven otherwise."
- Each potential function must be evaluated for policy or procedure acceptance or rejection by a practice.
- In some settings, copy and paste may be acceptable for legal record purposes but not for others (clinical trials data, quality assurance data, pay-for-performance data).
- In the hybrid environment, audit tracking of copy and paste may not be available because it involves different systems.
- In some contexts, it is never legitimate, including settings where the actual function takes personal health information outside the security environment.
- Some systems have an intermediate step allowing information to be brought forward but require another validation step.
- As a mitigation step, boilerplate text or libraries may be devised to describe common or routine information as agreed upon by the organizational standards.

Linking Each Patient to a Record

Every page in the health record or computerized record screen must identify patients by name and health record number. Patient name and number must be on both sides of every page as well as on every form and computerized printout. Paper and computer-generated forms with multiple pages must have the patient name and number on all pages.

EHRs. Each data field in the health record must be linked to the patient's name and health record number. Patient name and number must be on every page of printed, viewed, or otherwise transmitted information. The system in use must have a means of authenticating information reported from other systems.

Referencing another patient in the paper record. If it is necessary to refer to another patient to describe an event, the patient's name should not be used—the record number should be referenced in its place.

Timeliness and Chronology of Entries

Timeliness of an entry is critical to the admissibility of a health record in court as required by the Uniform Rules of Evidence. Entries should be made as soon as possible after an event or observation is made. An entry shall never be made in advance. If it is necessary to summarize events that occurred over a period of time (such as a shift), the notation shall indicate the actual time the entry was made with the narrative documentation identifying the time events occurred, if time is pertinent to the situation.

Timeliness of an entry presumes that the medium to which the entry is made is accessible. The principle of availability has been recognized as also consistent with timeliness, with the understanding that an entry would be made as soon as the record or system is available.

EHRs. Facilities must define what constitutes the legal health record in their organizational policies. Procedures must be in place to define timeliness for each component of the EHR system where there are no real-time automated links between subsystems.

Chronology

The record must reflect the continuous chronology of the patient's healthcare. Tools should be provided for caregivers to view episode-based information. The chronology must be readily apparent in any given view. It is recommended that organizations

have a facility-wide standard view. EHR systems should have the capability of producing an output that chronicles the individual's encounter.

Date and Time

Every entry in the health record must include a complete date (including month, day, and year) and a time. Time must be included in all types of narrative notes even if it may not seem important to the type of entry.

Charting time as a block (e.g., 7 a.m.–3 p.m.) is not advised, especially for narrative notes. Narrative documentation should reflect the actual time the entry was made. For certain types of flow sheets, such as a treatment record, recording time as a block could be acceptable. For example, a treatment that can be delivered any time during a shift could have a block of time identified on the treatment record with staff signing that they delivered the treatment during that shift. For assessment forms where multiple individuals are completing sections, the date and time of completion should be indicated as well as who has completed each section (Time is not required on standardized data sets such as the MDS and OASIS).

EHR systems must have the ability to date- and time-stamp each entry as the entry is made. Every entry in the health record must have a system-generated date and time based on current date and time. Date and time stamps must be associated with the signature at the time the documentation is finalized. For businesses operating across time zones, the time zone must be included in the date and time stamp. The date and time of entry must be accessible by the reviewer. Systems must have the ability for the documenter to enter date and time of occurrence for late entries.

Imaged records. The same standards for paper records apply to imaged records. Additionally, all scanned documents must be date- and time-stamped with the date scanned.

Legibility and Display

All entries to the record should be legible. If an entry cannot be read, the author should rewrite the entry on the next available line, define what the entry is for, referring back to the original documentation, and legibly rewrite the entry. For example: "Clarified entry of [date]" and rewrite entry, date, and sign. The rewritten entry must be the same as the original. All entries to the record should be made in black ink to facilitate legible photocopying of records. Entries should not be made in pencil.

Labels should be procured from a specific vendor to ensure adhesiveness and not placed over documentation. Organizations should review written documents as detailed in the practice brief "Ensuring Legibility of Patient Records."[5]

EHRs. Graphic user interface display options should accommodate ergonomic needs of all users (e.g., visual acuity). Critical results should not rely on color due to consideration for color-blind users. Asterisks or labels can be used as additional visual cues. Screen resolution should be adjustable for individual user preference. Imaged documents incorporated in the system should require a minimal number of clicks and keystrokes to open. Devices such as bar codes should be part of an organization's quality check protocol. If data are used in multiple organizational systems, legibility should be a shared quality check between applications. Free-text entries should be spellchecked to ensure the legibility requirement of ability to understand.

Imaged records. All entries to be scanned into the record should be made in black ink to facilitate legible reproduction of records. Entries should not be made in pencil. Paper records as well as corresponding microfilm should be retained for the period defined by facility policy.

Legibility of all records, including scanned records, should be included in an organization's quality control processes.

Computer screens must be of sufficient size and resolution to display information appropriate for the intended use and intended users. Displays must support viewing information in its entirety without scrolling. PACS images, especially scanned documents, require close attention to display support of required legibility.

Corrections, Errors, Amendments, and Other Documentation Problems

There will be times when documentation problems or mistakes occur, and changes or clarifications will be necessary. Proper procedures must be followed in handling these situations. ASTM and HL7 have standards that apply to error correction.

Error Correction Process

When an error is made in a health record entry, proper error correction procedures must be followed:

- Draw a line through the entry. Make sure that the inaccurate information is still legible.
- Write "error" by the incorrect entry and state the reason for the error in the margin or above the note if room.
- Sign and date the entry.
- Document the correct information. If the error is in a narrative note, it may be necessary to enter the correct information on the next available line, documenting the current date and time and referring back to the incorrect entry.

Do not obliterate or otherwise alter the original entry by blacking out with marker, using whiteout, or writing over an entry.

EHRs. Correcting an error in an electronic or computerized health record system should follow the same basic principles. The system must have the ability to track corrections or changes to the entry once the entry has been entered or authenticated. When correcting or making a change to an entry in a computerized health record system, the original entry should be viewable, the current date and time should be entered, the person making the change should be identified, and the reason should be noted. In situations where a hard copy is printed from the EHR, the hard copy must also be corrected.

Every entry should be date-, time-, and author-stamped by the system. A symbol that indicates a new or additional entry that has resulted in an additional version should be viewable. It must be clear to the user that there are additional versions of the data being viewed. A preferred method is to apply a strikethrough for error with commentary and date-, time-, and author-stamp or equivalent functionality to retain original versions linked to the corrected version.

Hybrid records. Organizational policy must define how errors are corrected in imaged documents while preserving in a readable form the original document or image. The practice brief "Electronic Document Management as a Component of the Electronic Health Record" provides guidelines for retraction, resequencing, and reassignment:

- **Retraction** involves removing a document for standard view, removing it from one record, and posting it to another within the electronic document management system. In the record from which the document was removed, the document would not be considered part of the designated record set or visible to anyone. Someone should be designated by the organization to view or print the retracted documents. An annotation should be viewable to the clinical staff so that the retracted document can be consulted if needed.
- **Resequencing** involves moving a document from one place to another within the same episode of care. No annotation of this action is necessary.
- **Reassignment** (synonymous with misfiles) involves moving the document from one episode of care to a different episode of care within the same patient record. As with retractions, someone in the organization should be designated to view or print the reassigned document. An annotation should be viewable to the clinical staff so that the reassigned document can be consulted if needed.[6]

Late Entry

When a pertinent entry was missed or not written in a timely manner, a late entry should be used to record the information in the health record.

- Identify the new entry as "late entry."
- Enter the current date and time. Do not try to give the appearance that the entry was made on a previous date or time.
- Identify or refer to the date and incident for which the late entry is written.
- If the late entry is used to document an omission, validate the source of additional information as much as possible (e.g., where you obtained the information to write the late entry).
- When using late entries, document as soon as possible. There is no time limit to writing a late entry; however, the more time that passes, the less reliable the entry becomes.

Amendments

An addendum is another type of late entry that is used to provide additional information in conjunction with a previous entry. With this type of correction, a previous note has been made and the addendum provides additional information to address a specific situation or incident. When making an addendum:

- Document the current date and time.
- Write "addendum" and state the reason for the addendum referring back to the original entry.
- Identify any sources of information used to support the addendum.
- When writing an addendum, complete it as soon after the original note as possible.
- In an electronic system it is recommended that organizations have a link to the original entry or a symbol by the original entry to indicate the amendment. ASTM and HL7 have standards related to amendments.

Healthcare organizations should have policies to address how a patient or his or her representative can enter amendments into the record. The HIPAA privacy rule requires specific procedures and time frames be followed for processing an amendment. A separate entry (progress note, form, typed letter) can be used for patient amendment documentation. The amendment should refer back to the information questioned, date, and time. The amendment should document the information believed to be inaccurate and the information the patient or legal representative believes to be correct. The entry in question should be flagged to indicate a related amendment or correction (in both a paper and electronic system). At no time should the documentation in question be removed from the chart or obliterated in any way. The patient cannot require that the records be removed or deleted.

Version Management

An organization must address management of document versions. Once documentation has been made available for patient care, it must be retained and managed regardless of whether the document was authenticated (if authentication applies). Organizations must decide whether all versions of a document will be displayed or just the final, who has access to the various versions of a document, and how the availability of versions will be flagged in the health record.

It is acceptable for a draft of a dictated and transcribed note or report to be changed before authentication unless there is a reason to believe the changes are suspect and would not reflect actual events or actions. Facility 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 late entry or amendment. The original document must be maintained along with the new revised document.

Chart Content

Organizations must define the content of their legal health records based on regulations and standards of practice. This step is critical in determining the information disclosed upon request that documents clinical encounters and the documentation that must be retained and protected for required periods of time. The practice brief "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes" provides information on determining the health record content.[7] The following topics address unique content issues.

Decision Support

Decision support, including system-generated notifications, prompts, and alerts, should be evidence-based, validated, and accepted by the organization. The patient health record 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 does no documentation mean).

Notification and Communication with Patients or Family

If notification of the patient's physician or family is required or a discussion with the patient's family occurs regarding care of the patient, all such communications (including attempts at notification) should be documented. Include the time and method of all communications or attempts. The entry should include any orders received or responses, the implementation of such orders, and the patient's response. Messages left on answering machines should be limited to a request to return call and are not considered a valid form of notification. An organization should determine whether copies of letters to patients are retained as part of the legal patient record, if they should be disclosed to others, and their retention period.

Informed Consent

Informed consent entries include explanation of the risks and benefits of a treatment or procedure, alternatives to the treatment or procedure, and evidence that the patient or appropriate legal surrogate understands and consents to undergo the treatment or procedure. This type of information should be carefully documented. Laws, regulations, and organization policy define the format of informed consent (e.g., must it be a distinct form or a documented discussion).

EHRs. With electronic consent, the patient views the consent and electronically signs it. An organization should verify that the electronic signature or authentication protocol meets all legal and regulatory requirements. The informed consent shall contain enough information for the patient to clearly choose various options of care and treatment during the episode of care. The informed consent should not allow for any "striking out" or deleting, but rather a document that provides for standard inclusions or exclusions.

Imaged records. When imaging, regulations, laws, or organization policies should define whether the original paper form or the patient's original ink signature be retained, the retention period, and the retrieval expectation. Policy should define if the legal medical record and a legal signature include a scanned image of the document or signature. Storage and retention should be consistent with the organization's policy for all other contents of the legal patient record.

Managing Data from Other Facilities or the Patient

Clinical information received from other facilities or from the patient should be evaluated by the clinician. The organization's policy should define whether the data in its entirety or just the data abstracted and transferred by the clinician is incorporated into the patient's health record. The source of the clinical data should be documented.

EHRs. If medical images are received from outside healthcare organizations or the patient, the images may be uploaded into the core clinical system. Retain attribution detail of source organization, author, and date.

Hybrid records. Organizations should define the procedure for the transfer of clinical information received on CD or DVD into the hybrid record. Options may include print to paper then image or upload into EHR or interface with the hybrid record. It must be determined whether laws, regulations, or organization policy require retention of the original media or a photocopy.

Customized Clinical Views

If the EHR system can provide customized clinical views, the organization should determine who is authorized to create and maintain the customized views. When clinical data are pulled into a customized view and used for clinical decision making, the logic or programming should be retained and made retrievable by the organization. The organization is encouraged to retain the methods and logic of customized clinical views; however, the system logic is not considered part of the legal health record.

Templates, Boilerplates, Canned Text

Care must be taken that these methods support clinical care and accurate documentation, not simply to expedite the process. Creation and periodic review of these tools should be based on clinically appropriate, standards-based protocol for common or routine information. Documentation by this method should require an active choice in response to the interaction between the patient and provider. When a clinician reviews and authenticates, the author is indicating he or she reviewed and completed the documentation and accepted the accuracy as his or her own.

Flowsheets

Organization policy should establish form design and documentation standards, including frequency of documentation. All entries are date-, time-, and author-stamped. The policy should define the frequency and standard time frame for documentation of clinical observations and assessments. In paper, if initials identify author only, full signature should be elsewhere on the form for easy reference.

EHRs. Organization policy should outline the frequency of data entry or capture and standard intervals for display of information (e.g., exact time, every five seconds, every 10 minutes, every 30 minutes, every hour). Policy should define the frequency of data captured directly from clinical monitoring systems, machine to machine (e.g., continuous, every five seconds, every 15 minutes). All data are date- and timed-stamped with the author noted. The standard frequency for view or print of archived flow sheet data should be defined. The system should provide views of archived data by date, time, author, or data field.

Output Format

Organization policy should determine whether the record must be complete before output is generated and who has the authority to generate output from the EHR. The EHR system must have the capability of providing a chronological record of the patient's encounter. When the EHR output is generated for disclosure, the organization must define the standardized forms, formats, and order based on user needs (e.g., different views, formats, and order for lawyers, insurance companies, patients, or healthcare providers). Organizations must also decide what versions of documents will be provided.

The organization should define a standard technology for output according to the information system capability, privacy and security standards, and user need and capability to use the format chosen.

Printing Guidelines

The organization must define the standard form and format of the paper health record and define who can reproduce paper documents for internal or external disclosure. The organization must also define the scope and reasons for printing paper internally. Printing can be a legal challenge if clinicians print from the EHR and then document on the printouts rather than in the system. Strict control of printing policies should be in place.

EHRs. Organizations must decide if they will reproduce the EHR in paper format. If printing from the EHR system is allowed, organization policies should define who has the authority to print and under what circumstances. Printing should be tracked in the audit trail and information on user and location available if needed. Policies should also define the form and format of documents that print from the EHR. For example, is it a screen print of the clinician view or a form that mimics the traditional paper record forms? What interval of time is printed as a standard—by encounter, date ranges, any point in time, or at discharge?

Organizations must decide which version is printed—only the most current version of a document or other versions as well. If other versions are printed, determine under what circumstances previous archived versions are printed. Organizations must decide whether to print the traditional final lab results report versus all the preliminary results and whether lab result trends are printed. When separate covered entities share a clinical data repository and use shared information for clinical decision making, the organization should define what information from the repository can be printed. An organization should also determine if preliminary, unauthenticated reports can be printed and under what circumstances.

Permanency

All entries in the health record, regardless of form or format, must be permanent (manual or computerized records). The Rules of Evidence require policies and procedures be in place to prevent alteration, tampering, or loss. The organization must consider the issue of permanency of records in its records management policies. In a paper system, permanency is affected by lifespan of the actual paper or microfilm that health information is recorded on. Retention policies and schedules developed by the organization determine the permanency of the information.

EHRs. The organization must consider the issue of permanency of records in its electronic records management policies. In an electronic system, permanency is affected by the digital nature of data, which may be more readily subject to change or technology obsolescence than is information recorded on paper. This includes changes to the actual data itself or changes that

occur over time in data formats and storage devices. Use of standard file formats and clinical nomenclatures may facilitate data conversion as technology changes and are a major consideration for permanency. Procedures to protect against data degradation and loss of integrity during system conversions must be addressed.

Other Permanency Issues

Ink color. For hard-copy paper records, blue or black ink is preferred to ensure readability when records are copied. The ink should be permanent (no erasable or water-soluble ink should be used). Never use a pencil to document in the health record. Black ink is preferred for records that will be imaged.

Printer. When documentation is printed from a computer for entry in the health record or retention as the permanent record, the print must be permanent. For example, a laser printer should be used rather than an ink-jet printer, because the latter ink is water soluble.

Fax copies. When fax records are maintained in the health record, assurance must be made that the record will maintain its integrity over time. For example, if thermal paper is used, a copy must be made for filing in the health record because the print on thermal paper fades over time. (See section on fax signatures for admissibility as evidence.)

Photocopies. The health record should contain original documents whenever possible. There are times when it is acceptable to have copies of records and signatures, particularly when records are sent from another provider.

Carbon copy paper. If there is a question about the permanency of the paper (e.g., NCR or carbon paper), a photocopy should be made. Policy should indicate when items are copied and how the original is disposed. At times, carbon copies of documents may be used on a temporary basis and the original will replace the carbon.

Use of labels. Labels and label paper (adhesive-backed paper) are used for a variety of reasons including patient demographics, transcription of dictated progress notes, printing of physician orders for telephone orders, medication, or treatment records. When labels are used in the record, a number of issues or concerns must be considered and addressed before implementation. Organization policies and practices should address how and where labels will be placed. Information may not be obscured by the label, and the adhesiveness of the label must be adequate for the retention period of the document.

Retention

Organizations must establish retention schedules for the content of the legal health record that comply with federal and state regulations and the needs for patient care, research, and administrative purposes (e.g., legal and compliance).

EHRs. Electronic storage media such as magnetic and optical formats must meet the organization's retention schedule and include retention of all types of data including discrete data, text, audio, video, and images. Policies should address backup procedures to ensure retention and protect against data loss.

Organizations should also address retention of data and information associated with the EHR but which may not be strictly part of the EHR—items such as audit trails, alerts and reminders, and metadata associated with structured as well as unstructured data. This may be important in certifying the integrity of the information for risk management and legal purposes.

Retention policies should comply with accreditation standards and federal and state law and regulations. Information life cycle management should be built into EHR systems in the development phase. If an EHR crosses multiple disparate information systems, retention policies must be applied to each component. EHR systems must include a function or feature that allows for litigation holds that exempt specific records from the retention policy due to legal, compliance, or other business needs.

Imaged records. With imaged documents, an organization needs to decide how long to retain the paper after scanning. Considerations include provisions for quality assurance in the scanning process, the organization's definition of its legal record (paper, electronic, or both), and the frequency and timing of backups of the scanned images.

Other considerations in retention of paper may include state regulations, requirements of the organization's malpractice risk carrier, and in the case of organizations that conduct research, FDA regulations. When paper is retained after scanning, there

must be an established cataloguing and indexing method so that it can be retrieved. Schedules or guidelines for conversion of document images from magnetic to optical storage should be addressed.

Depending on the organization's need for longevity of scanned images, it may also wish to consider converting scanned images to microfilm for longer retention periods. Occupational health records, for example, must be retained for 30 years.

Storage

An organization must store health records in a way that prevents loss, destruction, or unauthorized use. Traditional methods for storing paper records include open-space shelving for active files and off-site box storage for archived records.

EHRs. Organizations must ensure that EHR systems provide basic database storage standards, including appropriate security measures. Major considerations include how to store information in order to convey it to an external user in an acceptable medium and the volume of records to be stored (e.g., what types must be included).

Obsolescence of Technology

Stored records must be accessible for the length of the retention period regardless of the technology used. When records are stored as microfilm and microfiche, an organization must retain hardware to access or reproduce the records for the length of the retention period.

EHRs. Organizations require a plan to access or reproduce EHR data. As technology changes, consideration must include "backwards compatibility" or some type of access to previous systems from the new or upgraded system.

Purging and Destruction

Records should be purged and destroyed in a consistent manner based on an established retention schedule, plan, and procedure. Destruction is acceptable unless there is a concern that certain records or documents were selected for destruction. When this happens, behavior is considered suspect, and it can appear that information that was harmful to the organization was destroyed. Plans should include method of destruction (e.g., shredding, burning) and should consider security of the destruction process.

EHRs. The organization should have a plan for destruction of storage media, including hard drives and portable media such as diskettes and USB drives. Consideration should be given to determining if an EHR system can indicate records to be purged based on the organization's policy. The organization should have a policy that defines purging versus archiving and how the system will support the policy.

Data Integrity: Access, Audit Trail, and Security

Integrity is defined as the accuracy, consistency, and reliability of information content, processes, and systems. Information integrity is the dependability or trustworthiness of information, which is an important concept in a legal proceeding. Integrity of the health record is maintained through access, network security, audit trail, security, and disaster recovery processes.

To protect the integrity of the paper legal health record, organizations should define the policy and procedures regarding the content and reconciliation processes to ensure accuracy and completeness of the health record.

EHRs. To protect the integrity of the electronic legal health record, policies and procedures must be in place:

- Regarding the reconciliation of electronic processes (e.g., process for checking individual data elements, reports, files)
- To assess potential data corruption, data mismatches, and extraneous data
- Regarding managing different iterations of documents (version control), with clear indication of when each version is viewable by caregivers for use in making clinical decisions
- To define when the record is complete and permanently filed (locking the record with view-only access), including temporary locking of high-risk charts by certain users
- Regarding downtime processes and ability to capture data following downtime through direct entry or scanning

Performance criteria and functionality should define and minimize the intrinsic risks by appropriate design, deployment, development, and detection of the EHR. Performance criteria and functionality should also define and minimize the extrinsic risks by appropriate test conversion planning, testing and data validation, and minimization of system downtime.

Access Control

Access control is the process that determines who is authorized to access patient information in the health record. Controlling access is an important aspect of maintaining the legal integrity of the health record. In the paper world this is controlled through physical security safeguards, chart tracking, and out guide systems.

EHRs. Access control and validation procedures must be in place to validate a person's access to the system based on role or function. Access should be terminated automatically after a predetermined period of inactivity. Organizations must also define access to information for emergency situations (break-the-glass access). Policies must address facility access controls to meet the HIPAA security rule.

Audit Trail

An audit trail is a business record of all transactions and activities, including access, associated with the medical record. Elements of an audit trail may include date, time, nature of transaction or activity, and the individual or automated system linked to the transaction or activity. Transactions may include additions or edits to the medical record. Activities may include access to view or read, filing, and data mining. Audit trail functionality is important to support the legal integrity of the record. The purpose of an audit trail is to create a system control to establish accountability for transactions and activities as well as compliance with facility policies, procedures, and protocols related to medical record access and maintenance.

For the paper medical record, an audit trail may include a sign-out sheet, a manual or electronic chart tracking system (e.g., flagging devices or software), or a log book.

EHRs. Audit trails are critical legal functionality for EHR systems because they record key information on data creation, access, and revision. An audit trail may be one of the following types of business records:

- Electronic file of transactions and activities (data creation, access, revision along with date and time)
- Hard-copy report of transactions and activities
- Batch file processing report
- Information system data transmission or interface report
- Exception report of unauthorized access attempts

Special Considerations for an EHR Audit Trail

Teaching environment—academic medical centers. The high turnover of students, interns, and residents in an academic facility or a specific clinical department may necessitate the need to maintain a large file of unique EHR access codes or requirements. Timely activation and deactivation of identification and authentication tools may affect the reliability of audit trail data and must be addressed by organization policies to prevent negative impact on legal integrity of the record.

Health systems—mergers, acquisitions, and divestitures. Physicians and other clinicians who provide direct patient care at multiple locations or facility management and staff who work at other institutions may have more than one EHR access code or level of access when facilities merge or acquire other patient care sites with similar EHR software.

EHR Audit Trail Performance Criteria and Functionalities

- Make sure audit trail functionality is turned on in EHR applications.
- Include date and time stamps on all transactions.
- Do not allow back-door access by a staff member (e.g., system administrator) to make alterations in the EHR without an audit trail record. If back-door access is possible, have the software vendor fix the problem to ensure the EHR retains integrity in a legal proceeding.

Network Security

Electronic network security protects EHR data from unauthorized internal or remote access or illegitimate internal or remote transactions. The purpose of an electronic network security protocol is to preserve the integrity of EHR data and to protect patient privacy, consistent with facility and regulatory requirement, as well as accreditation standards. Electronic network security protocols must address the following access mechanisms:

- Remote access through virtual private network
- Remote access through a local area network
- Remote access through wireless network
- Remote access through a workstation
- Internal access through a workstation

Disaster Recovery and Business Continuity

An important aspect of maintaining a legally sound health record is securing the record to prevent loss, tampering, or unauthorized use. Rules of evidence require an organization to have policies and procedures in place to protect against alterations, tampering, and loss. Systems and procedures should also be in place to prevent loss (such as tracking and sign-out procedures), establish secure record storage areas or systems, and limit access to only authorized users.

Organizations should develop and implement controls to safeguard data and information, including the clinical record, against loss, destruction, and tampering. Organizations should:

- Develop and implement policies when removal of records is permitted
- Protect data and information against unauthorized intrusion, corruption, or damage
- Prevent falsification of data and information
- Develop and implement guidelines to prevent the destruction of records
- Develop and implement guidelines for destroying copies of records
- Protect records in a manner that minimizes the possibility of damage from fire and water

EHRs. Establish (and implement as needed) policies and procedures for responding to an emergency such as fire, vandalism, system failure, and natural disaster that damages systems containing electronic protected health information. Organizations must address and develop the following to adequately prepare for a disaster and prevent loss or destruction of information:

- Data backup plan
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revision procedures
- Applications and data criticality analysis

Business Continuity

Disaster recovery planning includes information and plans on how operations are to continue in the event of a disaster. If a department, business unit, or system is unavailable, a plan must be in place to continue operations. To develop a plan consider the following:

- List all departments that are directly or indirectly affected by extended system downtime
- List all daily procedures that must be followed to maintain acceptable levels of operations
- List actions (manual procedures) completed during downtimes for each department
- Expand the process to plan for the system if it were unavailable for an extended period of time
- Outline specific details steps to integrate backlogged data maintained during the downtime
- List additional procedures to be followed after recovery activities are complete

Conclusion

Maintaining a legally sound health record covers a vast territory from the content of the health record and how entries are recorded to the functionality in the system to access, audit trails, and security. While the electronic age brings new variables to an old and complex problem, the foundation remains the same: health records must be maintained in a manner that follows applicable regulations, accreditation standards, professional practice standards, and legal standards. HIM professionals play a critical role in the transition from paper to electronic records and must partner with clinical, legal, and information technology to adequately address the legal business issues for the health record.

Notes

1. *Comprehensive Guide to Electronic Health Records*, 2000 ed. New York, NY: Faulkner and Gray, 2000.
2. Department of Justice Bulletin on Computer Records and the Federal Rules of Evidence. March 2001.
3. Health Level Seven. "Glossary of Terms." Available online at www.hl7.org.au/Docs/HL7%20Glossary%20-%202001.pdf.
4. Tech Encyclopedia. "Digital Signature." Available online at www.techweb.com/encyclopedia.
5. Glondys, Barbara. "Ensuring Legibility of Patient Records." *Journal of AHIMA* 74, no. 5 (2003): 64A–D.
6. AHIMA. "Electronic Document Mangement as a Component of the Electronic Health Record." October 2003. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.
7. AHIMA. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." *Journal of AHIMA* 76, no. 8 (2005): 64A–G.

References

AHIMA. *Health Information Management Practice Standards: Tools for Assessing Your Organization.* Chicago, IL: AHIMA, 1998.

AHIMA. "E-mail as a Provider-Patient Electronic Communication Medium and Its Impact on the Electronic Health Record." October 2003. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

AHIMA. "Implementing Electronic Signatures." October 2003. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

AHIMA. "The Strategic Importance of Electronic Health Records Management." *Journal of AHIMA* 75, no. 9 (2004): 80A–B.

Amatayakul, Margret. "Access Controls: Striking the Right Balance." *Journal of AHIMA* 76, no. 1 (2005): 56–57.

Anderson, Ellen Miller. "Online Clinical Documentation in the Electronic Legal Medical Record." 2004 IFHRO Congress and AHIMA Convention Proceedings. October 2004. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

ASTM. *Annual Book of ASTM Standards.* Volume 14.01, Healthcare Informatics, Section 8, Signature Attributes. West Conshohocken, PA: ASTM, 2000.

Centers for Medicare and Medicaid Services. Interpretive Guidelines for Hospitals. Available online at www.cms.hhs.gov/manuals/107_som/som107ap_a_hospitals.pdf.

Dougherty, Michelle. "Maintaining a Legally Sound Health Record." *Journal of AHIMA* 73, no. 8 (2002): 64A–G.

Fox, Leslie, and Walter Imbiorski. *The Record That Defends Its Friends,* 6th ed. Chicago, IL: Care Communications, 1994.

"Health Insurance Reform: Security Standards; Final Rule." 45 CFR Parts 160, 162, and 164. Federal Register 68, no. 34 (2003). Available online at www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf.

Health Level Seven. Ann Arbor, MI: Health Level Seven, 1997, Sections 9.4.5-9.4.11, 9.5.5–9.5.10.

Hirsh, Harold L. "Will Your Medical Records Get You into Trouble?" *Legal Aspects of Medical Practice* 6, no. 9 (1978): 46–51.

Huffman, Edna K. *Health Information Management,* 10th ed. Berwyn, IL: Physicians' Record Co., 1994.

Joint Commission on Accreditation of Healthcare Organizations. *2005 Comprehensive Accreditation Manual for Hospitals, Update 3.* Oakbrook Terrace, IL: Joint Commission, 2005.

Murer, Cherilyn G., Michael A. Murer, and Lyndean Lenhoff Brick. *The Complete Legal Guide to Healthcare Records Management.* Washington, DC: Healthcare Financial Management Association, 2000.

National Institute of Standards and Technology. Security Considerations in Information System Development Life Cycle. Revised 2004. Available online at http://csrc.nist.gov/publications/nistpubs.

Quinsey, Carol Ann. "A HIPAA Security Overview." *Journal of AHIMA* 75, no. 4 (2004): 56A–C.

Roach, William H. Jr., and the Aspen Health Law and Compliance Center. *Medical Records and the Law,* 3d ed. Chicago, IL: Aspen Publishers, 1998.

Rollins, Gina. "The Prompt, the Alert, and the Legal Record: Documenting Clinical Decision Support Systems." *Journal of AHIMA* 76, no. 2 (2005): 24–28.

Scott, Ronald W. *Legal Aspects of Documenting Patient Care.* Annville, PA: Aspen Publishers, 1994.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (2000). Available online at www.hhs.gov/ocr/hipaa/finalreg.html.

Waller, Adele, and Oscar Alcantara. "Ownership of Health Information in the Information Age." *Journal of AHIMA* 69, no. 3 (1998): 28–38.

Acknowledgments

AHIMA e-HIM Work Group on Maintaining the Legal EHR:

Deborah Adair, MPH, MS, RHIA
Sharon Baigent, BA, CCHRA(A)
Joyce Booker, RHIT
Melanie Brighton, RHIT
Michelle Dougherty, RHIA, CHP
William French, MBA, RHIA, CPHQ
Marie Gardenier, RHIA, CHPS
Reed Gelzer, MD, MPH, CHCC
Marge Klasa, DC, APRN, BC
Nancy Korn-Smith, RHIT
Karanne Lambton, CCHRA(C)
Richard Leboutillier, MPA, CPHQ
Marlie Nunes, CMT
Suzanne Reviere, RHIA
Melissa Swanfeldt
Anne Tegan, MHA, RHIA, HRM
Andrea Thomas, MBA, RHIA
Lydia Washington, MS, RHIA, CPHIMS
Shelley Weems, RHIA, CCS
Kathy Westhafer, RHIA, CHPS

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

Article citation:
E-HIM Work Group on Maintaining the Legal EHR. "Maintaining a Legally Sound Health Record: Paper and Electronic" *Journal of AHIMA* 76, no.10 (November 2005): 64A-L.