How Legal Is Your EHR?: Identifying Key Functions That Support a Legal Record

Save to myBoK

*by **Michelle Dougherty**, RHIA, CHP*

Criteria from standards organization HL7 help organizations evaluate their electronic record systems as legally sound business records.

Medical records are submitted as evidence in many kinds of litigation, including malpractice, employment, and workers compensation. Traditionally healthcare providers submitted paper records as evidence (or printouts from their electronic systems). The attention of the courts and attorneys is now increasingly turning to electronic systems.

Attorneys are recognizing the treasure trove of information available within electronic records. The federal court system has implemented rules for discovery of electronically stored information, and state courts are following suit. Healthcare organizations thus must recognize that their EHRs will be used in litigation, and they should take steps to ensure that the systems they have deployed provide mechanisms that establish the trustworthiness of the record during legal proceedings.

That's easily said, but the industry overall has been struggling with how it's done. A newly released set of criteria from standards organization Health Level Seven (HL7) should help. It assists organizations in identifying the EHR functions that support a legally sound record.

The RM-ES Functional Profile

In December 2007, HL7's EHR Technical Committee balloted the EHR-S[ystem] Records Management and Evidentiary Support (RM-ES) Functional Profile. The profile identifies the key infrastructure functions that support the management of health records within the system for business and evidentiary purposes.

The EHR Technical Committee referenced a variety of resources and standards in developing the profile, including ISO, ASTM, Canada Health Infoway, the Certification Commission for Healthcare Information Technology, HL7 messaging standards, and e-discovery resources. The result was a comprehensive technical standard that identified new system functions and expresses legal EHR concepts in the framework of functional statements and conformance statements.

Once the profile passes the ballot stage, it will become a draft standard for trial use. This is expected by mid-year. Organizations can use the draft standard to evaluate new or existing applications, single applications, or entire record systems.

The RM-ES profile focuses on the necessary underlying functionality regardless of the content being captured by a specific application. For example, to support the evidentiary needs of the organization, the system or application must have appropriate security features, properly retain records, apply audit functionality, correctly amend entries, and manage succession (versions) of records.

Following are functions, description, and legal rationale excerpted from the profile that illustrate new or important functionality in support of a legally sound record. The criteria detailed in the eventual draft standard should be applied to all EHR applications that collect content for the medical record (e.g., ED, radiology, OB, outpatient, or a full EHR suite).

The RM-ES profile is available for download from www.hl7.org/ehr. The conformance criteria may be incorporated into an evaluation tool for comprehensive systems assessment. Updates on the profile's status are available at the same address.

The profile is also available from AHIMA in the FORE Library: HIM Body of Knowledge at www.ahima.org. For guidance on the structure, terminology, and use of the standard for system assessment, see the AHIMA practice brief "Using HL7 Standards to Evaluate an EHR," also available in the Body of Knowledge.

Security Functions

An EHR's security practices and functions have the potential to play a role in litigation because they support the integrity and trustworthiness of the health record maintained within the system.

In litigation, the organization's security practices may be called into question in an attempt to cast doubt on the validity of the record. The organization's adherence to applicable security laws (such as HIPAA) and standards (such as the Joint Commission) may also be called into question during litigation.

ID and Name	Function Description	Legal Rationale
IN.1.1 Authentication	Authenticate EHR-S users and/or entities before allowing access to an EHR-S. Examples of authentication include: • Username/Password • Digital certificate • Secure token • Biometrics	Authentication is a critical component to maintaining the legal integrity of the health record contained within the EHR-S. One of the foundational underpinnings of the validity of the record is identification of the users and assurances that they are accurately identified. As a result, the method used by the organization is very important. One of the most common and cost-effective methods of authentication is user ID and password. Other methods of authentication are considered stronger than user ID and password. Over time, as legal standards evolve, it is anticipated that the bar will be raised and stronger methods of authentication will need to be utilized by healthcare organizations to assure that their users are accurately identified in the system.
IN.1.2 Authorization	Manage the sets of access-control permissions granted to entities that use an EHR-S (i.e., users). Enable EHR-S security administrators to grant authorizations to users, for roles, and within contexts.	The authorization process is important legally because it provides the system rules and context for actions recorded within the EHR system. The actions and individuals may be called into question retrospectively. Authorization functionality is also important to constrain users to the system rules such as limiting printing or output capability. This is important legally to maintain controls on the location of outputs from the system.
IN.1.3 Entity Access Control	Verify and enforce access control to all EHR-S components, EHR information and functions for end users, applications, sites, etc., to prevent unauthorized use.	Controls to limit access to only authorized users are important for supporting the authenticity and trustworthiness of the electronic health record.
IN.1.4 Patient Access Management	Enable a healthcare delivery organization to allow and manage a patient's access to the patient's personal health information.	Similar to above, access controls, including patient access, are important for maintaining the electronic health record's integrity and trustworthiness.
IN.1.5 Nonrepudiation	Limit an EHR-S user's ability to deny (repudiate) the origination, receipt, or authorization of a data exchange by that user.	Nonrepudiation is a critical function in support of a legally sound record. System functionality must support the integrity of the data and record and prevent against denial of origination or receipt.
IN.1.6 Secure Data Exchange	Secure all modes of EHR data exchange.	It is important that the information received and used for patient care comes from a trusted source and that standards/protocols are in place to ensure that the data sent are the same as the data received.

IN.1.7 Secure Data Routing	Route electronically exchanged EHR data only to/from known, registered, and authenticated destinations/sources (according to applicable healthcare-specific rules and relevant standards).	It is important that the information exchanged is from a trusted and authenticated source and is securely transported.
IN.1.8 Information Attestation	Manage electronic attestation of information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information.	Legally it is critical that the author of an entry (including all contributors or co-authors) be accurately identified and that every entry has an author who is responsible for the content. Over time it is anticipated that the bar will be raised and that stronger authentication/attestation processes will be required to prevent someone from refuting that they were the author.
IN.1.9 Patient Privacy and Confidentiality	Enable the enforcement of the applicable jurisdictional and organizational patient privacy rules as they apply to various parts of an EHR-S through the implementation of security mechanisms.	Organizational practices related to privacy and security jurisdictional laws (e.g., HIPAA) could be called into question during a legal proceeding. Adherence to applicable laws supports the credibility and trustworthiness of the organization.
Source: HL7 EHR-S Records Management and Evidentiary Support Functional Profile		

Health Record Information and Management Functions

The information and management section of the profile identifies the fundamental electronic records management functionality that helps ensure the system can support the business and legal needs of the organization.

ID and Name	Function Description	Legal Rationale
IN.2.1 Data Retention, Availability, and Destruction	Retain, ensure availability, and destroy health record information according to scope of practice, organizational policy, or jurisdictional law.	Adherence to organizational retention and destruction policies that comply with jurisdictional law is critical in legal proceedings to prevent accusations of spoliation of evidence and establish that the organization destroyed records as part of their good faith practices. Organizations must develop a policy which defines their official medical record for official disclosure purposes (reimbursement, litigation, regulatory, etc.) The EHR-S must be able to support the retrieval of the elements the organization considers part of their legal medical record. This includes business context data (such as metadata) retained by the system which may provide context of when a record was created, by whom, etc.
IN.2.1.1 Record Preservation	Preserve data from normal destruction practices including a duty to preserve material evidence when the organization reasonably should know that the evidence (health record information) may be relevant to anticipated litigation.	Organizations have a duty to preserve information that is or could be relevant to a legal proceeding whether litigation is threatened (the potential for) or impending. Systems must provide the ability for users to place a legal hold on electronic health information (suspend their normal destruction practices for all potentially relevant information) and prevent from loss, destruction, alteration, or unauthorized use.
IN.2.2 Auditable Records	Provide audit capabilities for system access and usage indicating the author, the modification (where pertinent), and the date and time at which a	The audit functionality provides traceability to show the activities "behind the scenes." With traceability

	record was created, modified, viewed, extracted, or deleted. Auditable records extend to information exchange, to audit of consent status management, and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records or for an EHR-S.	comes trustworthiness in the electronic records to be used in legal proceedings.
IN.2.2.1 Metadata (Point of Record, System and Software Application)	Metadata is an inextricable part of electronic records management and is utilized for a variety of functions and purposes. In a legal setting, metadata may be used to authenticate the evidentiary value of electronic information and/or describe contextual processing of a record. Metadata at the point of patient record capture includes information about the context of record creation, the business context, the agents involved, and metadata about the content, appearance, structure, and technical attributes of the record itself. System metadata is information about the physical structure of the EHR system itself. This function includes defining, collecting, and storing important data to describe the EHR architecture, hardware/physical systems and the infrastructure in use over a definable time range. Software application metadata is information about the software/applications used in the EHR. This function includes defining, collecting, and storing important data to describe the EHR software, its components, and their evolution over time.	Metadata (data about data) can validate and quantify the authenticity, reliability, usability, and integrity of information over time and enable the management and understanding of electronic information (physical, analogue, or digital). The metadata collected and retained may vary by organization and within jurisdictions according to: • Business needs • Jurisdictional regulatory environment • Risks affecting business operations Effective utilization of metadata requires appropriate management of metadata information. All EHR applications must adhere to established standards, which enable the creation, registration, classification, access, preservation, and disposition of records through time and within and across information systems. Metadata supports the interoperability strategies by enabling the authoritative capture of records created in diverse technical and business environments and is sustained for as long as required. (Reference - ISO 23081)
IN.2.4 Extraction of Health Record Information	Manage data extraction in accordance with analysis and reporting requirements. The extracted data may require use of more than one application and it may be preprocessed (for example, by being de-identified) before transmission. Data extractions may be used to exchange data and provide reports for primary and ancillary purposes.	Extraction may be needed in response to a request from the court or an opposing party.
IN.2.5 Store and Manage Health Record Information	Store and manage health record information as structured and unstructured data.	Organizational policies on creation, capture, storage, and maintenance of health record information may be called into question during legal proceedings. Adherence to organizational policy, standards of practice, and jurisdictional law will be critical.
IN.2.5.3 Manage Record States: • Pending State • Amended, Corrected, and	Manage health record information during the various states of completion. Health record information may be started, updated, but not completed. The records, although not complete, can represent an important piece of	Health record information may reside in various states that must be managed. An important underlying principle for managing record states is the need to retain health information records that have been viewed for patient care purposes even if it has not been completed or attested, was created or placed in

Augmented State • Document Succession Management and Version Control • Retracted State	healthcare information particularly if viewed for patient care purposes. Updates to health record information made after finalization (or the signature event) will be handled as an amendment, correction, or augmentation. A system shall retain previous versions of a document and manage document succession. A system shall provide the ability to remove (retract) a document from view if it is deemed erroneous and cite the reason.	error, was in a previous version or has been amended. This principle has important legal impact because it provides a record of what the provider relied on for clinical decision making. Proper amendment and correction procedures are just as important in electronic systems as they were in paper-based record systems. When changes are made they should be transparent—a user or reviewer should be able to access the original entry and determine when and by whom amendments and corrections were made. The trustworthiness and integrity of the record can be called into question or placed under suspicion when previous entries are destroyed.
IN.2.5.4 Redaction	Remove from view (redact) for disclosure or reporting purposes portions of an EHR (at either the data or record level) and cite the authority for doing so.	Systems must provide the ability to redact information at the data level or at the record level, provide a mechanism to capture the reason for redaction, and retain a copy of the redacted records that were disclosed. Redaction may be used for a variety of purposes such as protecting certain types of confidential or privileged information from being disclosed including disclosure for litigation purposes.
IN.2.5.5 Health Record Completeness	Support the ability to identify a report or record as complete and identify the status as defined by the organization.	Prior to disclosure for legal proceedings or other official purposes, an organization analyzes the health record for completeness. EHR systems must provide the ability to define a minimum set of content to be analyzed for timeliness and completeness and provide a report of the status.
IN.2.5.6 Chronology of Events	Support the ability to view and disclose the patient care events that happened over a range of time in chronological order.	Functionality to support chronology of events allows the organization to display or disclose the patient care events in the sequence that they occurred. This view provides a beneficial retrospective look at the unfolding of events and timing of decision making which is important in the audit and review process and legal process.
IN.2.5.7 Replication of Views	Supports the ability to replicate or recreate a view (both read and write) to the extent possible from metadata.	Replication of views may be required for litigation to see information the way a clinician would have viewed, entered, or used it at a given time. Those handling litigation might expect the EHR system to capture a “snapshot” of every EHR action taken by the clinician to diagnose and treat each given patient. The ability to produce a replicated view is not guaranteed and is limited to audit and metadata. “Best practice” for replication of view approaches will evolve over time.
IN.2.5.8 Downtime Procedures, Storage and Back-Up	Provide mechanisms for reliable and consistent availability of the system and data.	EHRs and/or data transmitted and retained in an interoperable HIT system must be stored and be secure from access by unauthorized and unidentified

		persons or users. This applies to all data regardless of storage location. Records must be retained—unaltered, readable, and retrievable—and record retention must comply with all applicable laws and regulations. Regardless of the physical location where the EHR is stored, the EHR must at all times be actually available, by legal process or as otherwise authorized by law, to patients, governmental and private payers, and law enforcement.
S. 2.2 Report Generation and Health Record Output	Support the export of data or access to data necessary for report generation and ad hoc analysis. Support the definition of the formal health record, a partial record for referral purposes, or sets of records for other necessary disclosure purposes.	Report generation functionality is important to provide an output of relevant information from EHR systems for legal proceedings. Reports are not limited to the formal medical record, but any kind of system. Systems should also have the ability to provide a report of audit record and metadata for disclosure if required for litigation.
Source: HL7 EHR-S Records Management and Evidentiary Support Functional Profile		

Business Rules and Workflow Management

The security and health record and information functions outlined above have the most potential to affect the legal EHR. The RM-ES profile identifies 20 additional functions that play a role and could be called into question when an EHR is submitted as evidence.

Two functions—business rules management and workflow management—may have particular relevance in a legal proceeding because they establish the organization's standard of practice or can show a deviation from the standard.

ID and Name	Function Description	Legal Rationale
IN.6 Business Rules Management	Manage the ability to create, update, delete, view, and version business rules including institutional preferences. Apply business rules from necessary points within an EHR-S to control system behavior. An EHR-S audits changes made to business rules, as well as compliance to and overrides of applied business rules.	The care delivery and documentation process captured within an EHR-S is based on system business rules. These rules will likely be called into question during a legal proceeding to understand the organization's good faith practices and when practices deviated from the norm.
IN.7 Workflow Management	Support workflow management functions including both the management and set up of work queues, personnel lists, and system interfaces as well as the implementation functions that use workflow-related business rules to direct the flow of work assignments.	The workflow processes that support care delivery and documentation capture within an EHR-S will likely be called into question during a legal proceeding to understand the organization's good faith practices and when practices deviated from the norm.
Source: HL7 EHR-S Records Management and Evidentiary Support Functional Profile		

References

HL7 EHR-S Records Management and Evidentiary Support Functional Profile. Released for ballot December 5, 2007. Available online at www.hl7.org.

Quinsey, Carol Ann. "Using HL7 Standards to Evaluate an EHR." Journal of AHIMA 77, no. 4 (Apr. 2006): 64A–C.

Michelle Dougherty *(michelle.dougherty@ahima.org) is director of practice leadership at AHIMA.*

Article citation:
Dougherty, Michelle. "How Legal Is Your EHR?: Identifying Key Functions That Support a Legal Record" *Journal of AHIMA* 79, no.2 (February 2008): 24-30.