Health Information Management and Litigation: How the Two Meet

Save to myBoK

Editor's Note: This Practice Brief supersedes the November-December 2013 "E-Discovery Litigation and Regulatory Investigation Response Planning: Crucial Components of Your Organization's Information and Data Governance Processes" and October 2005 "Legal Process and Electronic Health Records" Practice Briefs.

Every healthcare provider and business associate, if they haven't already, will likely be involved in litigation at some point, either as a party or a nonparty from which information is sought. That information might be in the form of a physical item such as a tissue sample or paper documentation. However, as we continue the transition into the world of electronic health records (EHRs), the information at issue will more often be electronic. This Practice Brief focuses on that electronic information—known by its legal term of electronically stored information or "ESI." Selected readings with additional information on this topic appear in Appendix A: Selected Reading, available online in AHIMA's HIM Body of Knowledge at http://bok.ahima.org.

This Practice Brief will go beyond discovery of ESI and regulatory responses and will also consider the roles that health information management (HIM) professionals may be asked to perform by attorneys in litigation. The Practice Brief will also discuss regulatory responses. These attorneys may be "in-house," meaning that the attorneys are employees of a healthcare provider or business associate involved in litigation, or they may be "retained." Retained attorneys are outside counsel selected by a healthcare provider or business associate to represent it during particular litigation.

This Practice Brief is not intended to provide legal advice. Rather, it is intended to assist the reader in understanding how the legal system operates and how he or she might be called upon to assist in litigation.

The Practice Brief will look to the Federal Rules of Civil Procedure (FRCP) as it walks through litigation and the roles that HIM professionals might be asked to perform. However, the reader should understand that most litigation in the United States takes place at the state or local level and not in federal courts. This Practice Brief uses the FRCP because these rules are well known, create a nationwide standard, and have served as a model for the formulation and interpretation of state rules. The FRCP began to address e-discovery in 2006 and were amended in 2015 to further address e-discovery.

The Structure of Litigation

Civil litigation can be seen as a continuum from beginning to end. This continuum consists of a number of stages during which the HIM professional might be called upon to assist attorneys in various ways. Here are the stages, all of which are focused on when the HIM professional is likely to become involved:

- Preservation of information
- Legal hold processes
- Collection of information
- Internal review and organization of information
- Production of information in response to formal requests
- Depositions of witnesses, managers of information, and experts
- Summary judgement (which may or may not conclude pending litigation)
- Trial

During these stages, the HIM professional might be asked to do any or all of the following:

- Be responsible for or implement the preservation of relevant ESI or other information
- Be responsible for or implement the collection of relevant ESI or other information

- Be responsible for or implement the production of ESI or other information in response to requests for production or interrogatories served by other parties or in response to subpoenas
- Participate or prepare others to participate in information meetings with attorneys to describe, among other things, how ESI is created, stored, or managed
- Execute affidavits or declarations about preservation, collection, or production
- Testify at depositions, hearings, or trials on various subjects, including those described above, and authenticate particular ESI so that it might be introduced into evidence

The reader should bear in mind that throughout the stages of litigation the HIM professional might, at the direction of an in-house or retained attorney, work with a third-party vendor or consultant to perform one or more of these tasks.

The Role of Information Governance in Litigation

AHIMA defines information governance (IG) as "an organization-wide framework for managing information throughout its lifecycle and for supporting the organization's strategy, operations, regulatory, legal, risk, and environmental requirements."

In the litigation context, IG is essential to reasonably ensure that the relevant information is available at the right time and the right person has access for litigation-related purposes, whether for discovery, motion practice, or trial. An IG framework allows an organization's information to be managed to that end (in addition to other purposes). Indeed, "Regulatory and Legal" is one of the 10 Information Governance Adoption Model (IGAM™) competencies.

IG is essential for legal and regulatory initiatives such as e-discovery, legal holds, and chain of custody so that organizations have standardized processes for responding to legal requirements. It is also necessary to manage the changing healthcare landscape such as the Internet of Things (IoT) and increased connectivity. IoT has enabled the healthcare industry to increase the speed and volume of connectivity through devices that are all linked through a common network. IoT is a great benefit for organizational efficiency and innovation but also creates a variety of new ESI sources that are discoverable.

Mobile devices such as cellphones and tablets, patient monitoring machines, implantable devices (pacemaker, insulin pump), telemedicine, and more are all "things" that can be connected to a common network within an organization. These sources create outputs that can be useful for clinical and business decisions as well as for litigation. It is important that organizations determine the best methods for integrating these sources into existing systems and protections so that data can be managed within the EHR and so that the outputs can be utilized appropriately and accurately reproduced in the event of litigation. The IG concepts should be applied to the information produced, stored, and shared to ensure usability.

ESI of any kind and from any source can serve as evidence. This includes, but is not limited to, text, clinical images, video (including security video recordings), voice, databases, spreadsheets, legacy systems, tape, smartphones, tablets, instant messages, email, calendar files, and websites. HIM professionals should be mindful of the various ESI sources when performing daily job functions.

IG is an important step for handling the large quantities of discoverable electronic information. It is critical that organizations refine their current processes for e-discovery and implement a new strategy and standardized approach for compliance through IG.

Certain subdomains within AHIMA's IGAM are key contributors to the overall maturity of IG; those considered the foundational core competencies are Data Governance, Enterprise Information Management, and Information Technology Governance (ITG). Legal and Regulatory, in conjunction with the core competencies, supports both e-discovery and litigation response planning. The definitions that further articulate those domains as stated in AHIMA's IGAM include:

- **Data Governance (DG):** "Provides for the design and execution of data needs planning and data quality assurance in collaboration with the strategic information needs of the organization. DG includes data modeling, data mapping, data audit, data quality controls, data quality management, data architecture, and data dictionaries."
- **Enterprise Information Management (EIM):** "Includes the policies and processes for managing information across the organization, throughout all phases of its life: creation/capture, processing, use, storage, preservation, and disposition. EIM also includes management of enterprise practices for information sharing, release and exchange practices, chain of custody, and long-term digital preservation."

- **Information Technology Governance (ITG):** "Serves as a vehicle to achieve organizational strategy, goals, and objectives. IT governance establishes a construct for aligning IT strategy with the strategy of the business, and a means of fostering success in achieving those strategies. In addition to this alignment, IT Governance includes: use of best practices in technology solutions selection and deployment, ensuring and measuring the value/benefit created through IT investments, management of resources, mitigating risks, measuring the performance of the IT function, and ensuring stakeholder input is incorporated into IT strategy."
- **Legal and Regulatory:** Refers to "the organization's ability to respond to regulatory audits, e-discovery, mandatory reporting, and releases to patients upon requests, but also on compliance with information-related requirements of any/all regulatory and other bodies of authority."

Maturity in each of the competencies is vital to information fitness and its use for litigation purposes. Culled out of the IG framework, e-discovery practices and mechanisms expedite the identification, preservation, and production of ESI.

The HIM professional should consider the following in ESI delineation:

- Source identification
- Method of creation
- Mode of access
- Maintenance and retention requirements
- Disposition practice (i.e., policies and procedures)
- Any necessary third-party participation

Policies Enable e-Discovery Readiness

E-discovery hinges on the ability to locate, retrieve, and produce information based on a request. An inability to access ESI increases the risk for non-compliance with ESI requests. The use of embedded IG policies and practices allow for timely, standardized, and consistent legal and e-discovery responses. Succinct response to legal and regulatory requests for information is contingent upon an organization's knowledge of pertinent laws and regulations along with processes that will support and adhere to those requests; this is best accomplished using IG practices.

Every organization has a responsibility to respond to all legal and e-discovery requests in an expeditious manner. Collaborative response involves stakeholders such as legal, HIM, and IT to enable prompt compliance and mitigate the risks associated with noncompliance. Establishment of enterprise-wide policies and procedures sets the standards, expectations, and accountabilities for e-discovery. Key policies to support e-discovery readiness should include:

- Timeframes for response to and processing of legal and e-discovery requests
- Legal hold
- Record retention schedule
- Chain of custody
- Legal health record definition
- Attorney-client privilege

The Project That Sets Up e-Discovery Compliance

A cornerstone IG project is the completion of an information asset inventory (IAI). It is essential for the classification and categorization of data and information. As a centrally controlled inventory of the organization's records and information, it is an initial and critical project in IG. An IAI establishes the support structure to ensure appropriate information mapping, information lifecycle management, accountabilities, and risk and security management. Given its purpose, an IAI will increase an organization's internal transparency and capacity to effectively comply with legal and e-discovery requests.

An IAI will improve several areas within an organization, including but not limited to:

- Identify what information is where (increased visibility), determine specific attributes that are important for classification (i.e., public, private, confidential), and ensure version control
- Assign accountabilities for the various sources/systems listed in the IAI

- Set and comply with retention policies
- Centralize and store information
- Enable technology to effectively place legal holds on data and information subject to litigation needed for e-discovery

More information about IAIs can be found in AHIMA's Information Asset Inventory Practice Brief, available online in AHIMA's HIM Body of Knowledge.

Technology to Support e-Discovery

ITG functions as a mechanism for an organization to achieve its strategy, reach optimal IT performance results, and maximize the return on its investment in enterprise information technology. With an ITG framework in place, information is available and protected, which reduces risks and potential threats. Effective ITG reduces legal and regulatory response time, providing a means to retrieve all appropriate and relevant ESI in an efficient manner when deadlines for legal submission are in play. An organization must be able to sift through systems quickly in response to e-discovery to identify the source of ESI, ensure that ESI is protected from improper alteration or destruction, and confirm that discoverable information can be placed on legal hold or audited through standardized methods.

A proactive approach in the management and support of e-discovery through sound IG practices will help organizations to:

- Define enterprise-wide IG policies to meet legal and regulatory compliance with e-discovery
- Create an enterprise-wide IAI to establish an inventory of information to centralize, classify, and protect information
- Use stakeholder engagement to enable the protection, retrieval, storage, etc. of ESI
- Ensure ESI can be placed on legal hold or audited when necessary to meet regulations and legal requests
- Employ policies and practices in the defensible deletion of ESI through a record retention schedule
- Provide continual education and training on enterprise-wide e-discovery policies and practice

These IG processes will improve an organization's response to litigation and e-discovery and will allow organizations to prove compliance through a documented and consistent process that can be traced back in time.

Concepts of Litigation

This section discusses litigation concepts of which it is important for HIM professionals to be aware.

The Duty to Preserve

This is likely to mark the beginning of the HIM professional's involvement in litigation. A duty to preserve relevant information arises when a healthcare provider or business associate becomes aware of litigation or when litigation is reasonably foreseeable. When asked to do so by an attorney or supervisor, the HIM professional will help the organization meet its preservation obligations and will communicate the parameters of the hold to others. The attorney or supervisor should be expected to provide:

- The applicable dates for which data preservation should begin and end
- The "scope" of preservation
- The methods by which ESI should be preserved

The scope of the preservation effort may require extensive research, as well as discussion with the attorney or management staff. This is because of the nature of ESI. It can, for example, be voluminous as well as widely distributed. ESI can be stored with individual custodians, in different departments or divisions of a healthcare provider or business associate, in "the cloud," or with other third parties such as providers of remote services or IT applications. The HIM professional might be asked a series of questions by an attorney or management staff to locate these sources of ESI and, in essence, to map out where relevant ESI might be located.

The easiest way to describe preservation is to keep, in whatever form it may exist, relevant ESI. Preservation means that relevant ESI should be locked down and should be exempted from deletion, destruction, or loss under any records retention policy until further notice. This process is often referred to by attorneys as the "litigation hold."

Of course, once the ESI is located, preservation must be implemented. The HIM professional might be tasked to communicate the duty to preserve whatever ESI is relevant to individuals or departments where the ESI resides. There might also be times when the HIM professional is asked to collect the preserved ESI. Moreover, the HIM professional might be asked to monitor implementation of preservation or collection by individuals or departments. These various functions might be performed by others such as third-party consultants or IT personnel. However, the HIM professional might be asked to participate in some or all of these functions and, if he or she does so, might be called upon to explain what was done.

The Scope of the Duty to Preserve

As noted above, the HIM professional should expect to be advised by an attorney or supervisor about what should be preserved. To give the reader an idea of the scope of preservation, here is FRCP 26(b)(1), which sets forth the scope of discovery in the federal courts:

> Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

As a general proposition, the scope of the duty to preserve can be considered as the scope of discovery, although risk-averse parties may want to err on the side of preserving some ESI that may only be considered marginally relevant, such as system logs or metadata related to clearly relevant ESI.

Although decisions as to the scope of production are for attorneys and judges, the HIM professional should alert counsel if a particular category of ESI or source of ESI might be unduly expensive to preserve or produce. This is known as proportionality. In addition, the HIM professional can alert counsel when ESI is preserved in a format that will require special software or hardware to read or access. For example, readings from an eye scan would be meaningless without appropriate software that would allow one to read the data.

Proportionality also arises in another concept covered in the FRCP, namely that of "not reasonably accessible" ESI. FRCP 26(b)(2)(B) states:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

If a party can demonstrate that certain protected health information sought is not reasonably accessible because of undue burden or cost, that ESI may no longer be required to be produced (i.e., a piece of hardware where there is no longer any software available to support or reproduce). However, note that a court can nevertheless order that the ESI be produced on a showing of "good cause" by the requesting party, bearing in mind the proportionality factors of FRCP 26(b)(1) referenced above. Therefore, prudence dictates that it be preserved until a determination is made that the not reasonably accessible ESI is outside the scope of discovery.

The scope of preservation and discovery also extends beyond the "four walls" of a party. FRCP 34(a)(1) allows discovery of any relevant information "within the possession, custody, or control of a party." That means that the HIM professional might be tasked with, for example, locating ESI that is held by a third-party vendor and reaching out to that vendor to preserve relevant information. Moreover, ESI that may not be considered part of a record may still be within the scope of discovery. Preservation of that ESI may be required. Such ESI could, for example, consist of email or text messages that may reside within or outside the organization's IT systems.

Remember that states have their own discovery rules that might vary from those of the federal courts. Discovery under state rules might be broader or it might be more constrained. The most stringent rules should apply.

The Essential Role of the Custodian of the Record

Responding to a discovery request, or the anticipation of one, is a coordinated effort with the professionals from organizational legal counsel, HIM, and IT departments as key players of the e-discovery response team. This team is assembled at the initial receipt of a request for information (RFI), subpoena, court order, or notice of claim, when the organization is seriously considering litigation against another party, or to assess the need for preservation and eventual production of ESI and to determine specifically what ESI is to be collected and how it can be produced.

Legal counsel will serve as the primary source of communication between the requesting or opposing party and the healthcare organization and will coordinate all conversations throughout the discovery process. HIM and IT staff provide information related to the availability and producibility of ESI. While the breadth of involvement that IT has in e-discovery is far more involved, HIM is involved in production of ESI relative to the EHR only, as well as ancillary sources that feed into the EHR such as a diagnostic system. Determining what information is made available is guided by organizational retention schedules and destruction logs. If ESI that should have been retained—either by statute, regulation, or retention schedule—is somehow "lost" or inadvertently destroyed, then there might be adverse consequences.

Participating in Meetings

FRCP 26(f) is the "meet-and-confer" rule. It requires parties to discuss a number of topics and prepare a discovery plan that will be submitted to a federal judge and lead to the issuance of a scheduling order by the judge. These topics include "any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced." Productive discussion of this topic by attorneys may require the assistance of HIM professionals. It is expected that staff fully cooperate in a courteous and professional manner, providing answers only to the questions posed.

The FRCP 26(f) meeting is not intended to be a "drive-by." Rather, as is often true in complicated litigation, it may require multiple meetings as attorneys attempt to resolve disputes and reach agreements that will be incorporated into orders. The HIM professional might be asked to attend one or more of these meetings and provide information about what his or her organization can or cannot do. Moreover, meetings such as these may occur beyond the FRCP 26(f) context whenever there is a dispute between the parties during litigation. Cooperation and transparency were emphasized when the FRCP were amended in 2015. The HIM professional might be called on by an attorney or a court to explain what he or she can and cannot do to comply with a request made by another party to, for example, produce ESI of a given volume or in a particular form.

Assisting with Written Discovery

Interrogatories or requests for production comprise written discovery and are served under FRCP 33 and FRCP 34, respectively. Interrogatories are written questions served to a party such as a healthcare provider or business associate to be answered by that party in writing and under oath. The HIM professional might be asked by an attorney to assist in gathering information so that a particular interrogatory can be answered.

Requests for production are exactly that—requests made by a party for another party to produce relevant information, including formal records or documents. Disputes often arise with the "form or forms" in which ESI will be produced. In that regard, FRCP 34(b) allows a party to request that ESI be produced in a certain form—for example, in "native form" or as a PDF. The responding party can do the following, per FRCP:

> (D) *Responding to a Request for Production of Electronically Stored Information.* The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use.
>
> (E) *Producing the Documents or Electronically Stored Information.* Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

> (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
>
> (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
>
> (iii) A party need not produce the same electronically stored information in more than one form.

The HIM professional might be asked to discuss with his or her organization's attorney possible objections to production of ESI in a form requested by another party. They may also be asked to discuss the manner in which the organization "ordinarily" maintains that ESI or whether it can produce ESI in a "reasonably useable form or forms." The latter is likely to entail discussion of metadata. Metadata is often requested along with the electronic document itself to assist in determining whether the document is authentic and determining the integrity of the document. If an organization's attorney anticipates that metadata will be requested in discovery, that expectation is likely to have significant consequences for the method of preservation selected at the onset of litigation.

Whatever written discovery is requested, the HIM professional might be asked to execute an affidavit or declaration that would be submitted to a court if the court is asked to resolve a dispute about production.

Subpoenas

Subpoenas are a form of written discovery. Subpoenas are directed to a nonparty and request the nonparty to produce certain information, including ESI, for use in an action. Subpoenas are governed by FRCP 45. Among other things, the rule provides:

> A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

The HIM professional may be tasked with compiling ESI in response to a subpoena and, if compliance would result in "undue burden or expense," participating in a meeting with the party that served the subpoena or executing an affidavit about that burden or expense.

Being Deposed

The deposition is a procedure in which an individual answers questions posed by other attorneys under oath. Depositions are governed by FRCP 30. Depositions can also be sought under FRCP 45 pursuant to a subpoena. The reader should not be concerned about which rule applies.

Depositions can seek either specific knowledge from a particular person or can be directed to an organization. The latter is known as a "30(b)(6) deposition." FRCP 30(b)(6) provides:

> In its notice or subpoena, a party may name as the deponent a public or private corporation, a partnership, an association, a governmental agency, or other entity and must describe with reasonable particularity the matters for examination. The named organization must then designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on its behalf; and it may set out the matters on which each person designated will testify. A subpoena must advise a nonparty organization of its duty to make this designation. The persons designated must testify about information known or reasonably available to the organization. This paragraph (6) does not preclude a deposition by any other procedure allowed by these rules.

In other words, a deposition noticed under FRCP 30(b)(6) does not require an organization to produce a specific individual. Instead, the deposition is for "matters" and, for each such topic, the organization must designate someone to testify. That individual must know or learn about information in response to the matter. It is not uncommon for HIM professionals to be deposed in their business capacity about their organization's information systems, policies, and procedures under Rule 30(b)(6).

HIM professionals might also be served with subpoenas to testify as individuals in ongoing litigation involving their organization, in which case they should immediately contact the responsible attorney or supervisor.

Executing Affidavits or Declarations

An attorney might seek an affidavit or declaration from the HIM professional at other times. One such time might be when summary judgment motions are made or sanctions are sought. Sanctions are addressed below.

FRCP 56(a) describes the summary judgement motion:

> A party may move for summary judgment, identifying each claim or defense—or the part of each claim or defense—on which summary judgment is sought. The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law. The court should state on the record the reasons for granting or denying the motion.

The HIM professional may be called upon to submit an affidavit or declaration when his or her organization moves for or opposes summary judgement. There may also be times when the HIM professional is called on to testify when there is a hearing before a judge on a summary judgment motion.

Seeking or Opposing Sanctions for the Loss of ESI

HIM professionals may, as noted above, have a role to play whenever discovery-related disputes are submitted to judges for determination. That role, unsurprisingly, may extend to disputes related to the "loss" of ESI that has been requested in written discovery. Any such loss is referred to as "spoliation."

Imposition of sanctions for the loss of ESI in federal litigation is governed by FRCP 37(e). That rule provides in full:

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the infor- mation was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Think of FRCP 37(e) and consider what role an HIM professional might play in these scenarios:

- Assuming that there was a duty to preserve ESI that has been lost or inadvertently destroyed, were "reasonable steps" taken to preserve that ESI? This may require an affidavit or testimony from the HIM professional on what was done to preserve the lost ESI.
- Can the lost ESI be "restored or replaced?" This could require the HIM professional to search for, locate, and collect ESI that resides somewhere in an organization or to testify about the nature or content of the lost or inadvertently destroyed ESI.
- Whatever relief a court awards, the HIM professional might be asked to testify at trial about how and why the ESI was lost or inadvertently destroyed for the benefit of the finder of fact, whether that be a jury or a judge.

There are two important caveats to note:

1. FRCP 37(e) applies only to the loss of ESI. There are different, and varying, standards that federal courts apply for the loss of physical things, including paper.
2. FRCP 37(e) applies only in federal litigation. The states have their own rules for the loss of relevant information. Some state rules are specific as to the loss of ESI. Other states have "general" rules applicable to the loss of both ESI and physical things.

Being a Trial Witness

Trials do take place and HIM professionals may be called as a witness by the attorney representing his or her organization or by another party. Please note, if you are served with a trial subpoena you should advise your organization's attorney immediately.

The Federal Rules of Evidence (FRE) govern the testimony of witnesses and introduction of evidence at trial.

FRE 401 defines evidence to be relevant if:

(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and

(b) the fact is of consequence in determining the action.

The HIM professional might be called to testify if he or she can offer relevant evidence, based on personal knowledge, of how particular records were created, maintained, and produced, or about an organization's management of information in general. The HIM professional might also be asked to offer opinion testimony about accepted records management practices as a "lay witness" under FRE 701 under certain circumstances:

If a witness is not testifying as an expert, testimony in the form of an opinion is limited to one that is:

(a) rationally based on the witness's perception;

(b) helpful to clearly understanding the witness's testimony or to determining a fact in issue; and

(c) not based on scientific, technical, or other specialized knowledge within the scope of Rule 702.

When the HIM professional is called as a witness to testify regarding the authenticity of the organizational EHR or other sources of ESI either through deposition, trial testimony, or interrogatories, those requests should be vetted through organizational legal counsel who will then prepare the HIM professional. While questions related to clinical content will not be posed, the following questions may be asked to establish credibility of the HIM professional/records custodian and management of the EHR:

- What is your position/title?
- Who is the custodian of health records?
- How long has the "custodian" of health records been employed?
- Do you currently have possession of the record(s) in question?
- How and when was the record prepared?
- Is there health information from another organization contained in the patient's record?
- Was this information received in the normal course of business?
- Can you attest to the recordkeeping practices of the organization?
- How was this set of documents put together/chosen?
- For electronic records, what were the search parameters?
- From what systems, and from what areas of each system, were electronic documents produced?
- Can you describe the logs that record when and by whom data were created, edited, authenticated, and accessed?
- What does a system definition of an "edit" encompass?
- How are logs organized and what types of information do they contain?1

There is one specific area in which the HIM professional might be expected to submit an affidavit or declaration in lieu of being called as a witness at trial and that has to do with "authentication" of ESI. Under FRE 901, a party proposing to introduce a specific item of evidence must demonstrate to the trial judge that the item is "what the proponent claims it is." This could require the HIM professional to testify about how a particular item of evidence derived from ESI was created, stored, and produced. However, there are categories of information that FRE 902 deems to be self-authenticating and do not require "extrinsic evidence of authenticity in order to be admitted." This category, described in FRE 902(11) as "certified records of a regularly conducted activity," is often used to authenticate information:

> The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.

Attorneys attempt to authenticate relevant ESI under FRE 902(11) and, to do so, are likely to ask for a certification from the HIM professional. However, some courts have not accepted certifications related to ESI, but instead require extrinsic evidence through the HIM professional at trial. In an attempt to remedy this, FRE 901 was amended effective December 1, 2017, to create two new categories of self-authenticating information. These are:

> (13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).
>
> (14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11).

The difference between these two categories is subtle, yet important. FRE 902(13) addresses the authentication of a "record"—that is, a document generated by a computer system such as a report, file, email, or spreadsheet. FRE 902(14) addresses the collection of "raw" data from a computer system or other electronic device, usually for a forensic examination. Note that both categories require a "certification of a qualified person." Again, here is a possible role for the HIM professional.

Regulatory and Investigative Agencies

Receiving a request for ESI from regulatory or investigative agencies is an occurrence for which healthcare organizations must be prepared. Organizational policies and procedures should be written to address each specific type of regulatory or investigatory request/demand for information, detailing the level of response team that is activated, and the processes for identification, collection, and presentation of information.

Listed below are examples of agencies in which access to ESI is to be provided upon request and, oftentimes, without authorization from the patient or legally authorized representative (as permitted under law). These requests can be received via informal records request, investigative records demand, subpoena, or other means.

- Office of Inspector General
- Department of Justice
- Department of Health and Human Services
- Office for Civil Rights
- Attorney General (State or Federal)
- State Department of Safety/Regulation
- State Department of Health

Requests and demands for ESI from a regulatory or investigative agency should be treated with the same level of urgency and follow-through as with other litigation investigation—beginning with a consultation with legal counsel and activation of a response team. A regulator's request can be triggered by a periodic reporting requirement, by the outcome of an audit, by a report of potential fraud or abuse, by a patient complaint, by a patient injury or safety incident, or by any other event that warrants further assessment or investigation.

The request letter for ESI will provide clear expectations in terms of timeliness of a response. Should the healthcare organization not be able to provide the information in the format requested within the timeframe defined, communication and negotiation through the organization's legal counsel or compliance officer is required. Due to the nature of the review/investigation, the ESI request letter will detail the expected format in which the information should be provided. Often, the format requested is the basis for their review—for example, the view as a clinician would see it during the normal course of business or specific access logs to the EHR. The healthcare organization is expected to make every effort to provide this in the manner requested. In addition, the agency may provide defined processes in which the information is to be submitted to them.

For example, suppose an investigatory letter is received from OCR. The letter is typically in a standard format in that it details the name of the complainant (if not anonymous), and possibly the nature of the complaint. It contains an explanation of what HIPAA is, OCR's responsibility for enforcing HIPAA, and a description of OCR's authority. OCR sets a response date, which can be difficult to meet depending on the extent of the data request. Communication between the organizational legal counselor, compliance officer, and OCR should occur to discuss potential extension of the due date, if needed. A secured portal is the proposed method to submit such ESI. Organizations that do not have a secured portal should use certified or other forms of mailing that ensures the receipt of delivery. If the request for information is determined to be overly broad or unduly burdensome, this should be communicated to OCR as soon as identified, again through legal counsel. In addition, a written response to the requester should detail any information that will support the organization's position, including an explanation of any differences between what was requested and what was produced.

The contracted release of information (ROI) vendor is also involved in the process of compiling the ESI gathered from the designated record set (DRS). The vendor should be engaged through legal counsel to obtain clear direction as to who is involved in the response team and what level of response is warranted, what information is to be compiled, how it should be compiled, and when and how it is to be submitted. In addition, the ROI vendor will be responsible for including additional documentation from outside of the DRS with the ESI, if needed.

Due to the nature of the request or demand for records, every effort should be made to provide the information requested, in the manner requested, and within the timeline requested. Depending on the requesting agency, consequences for noncompliance with an information request/demand can vary widely, including exclusion from participation in the Medicare Program, implementation of a Corporate Integrity Agreement, civil monetary penalties, or escalation of the request to a higher authority.

To ensure a smooth data collection process for the regulatory response team, particularly when firm response timelines are imposed, a good information governance plan is essential. Classifying and categorizing data and information with an IAI will provide an immediate display of information assets, location, asset ID, owner of the information asset, associated interfaces, acquire and destruction dates, etc. Establishment and adherence to organizational document retention schedules will guide the response team in the smooth identification, collection, and submission of requested data. This documentation is also critical in identifying if/when data submission limitations exist for the organization.

Be Prepared for Litigation

This Practice Brief is intended as a means to inform AHIMA members about the stages of civil litigation and the roles that HIM professionals might fill throughout litigation. It is important to note that throughout the process of litigation, solid information governance practices will arm organizations to be better prepared for litigation. Through people, processes, and technologies, IG will standardize litigation processes and ensure that the appropriate data and information is captured and preserved in such ways as to comply with legal and regulatory demands.

Appendix Available Online

The following appendix to this Practice Brief can be found online at http://bok.ahima.org:

- Appendix A: Selected Reading

Note

1. Brodnik, Melanie S. et al. *Fundamentals of Law for Health Informatics and Information Management*, Third Edition. Chicago, IL: AHIMA Press, 2017.

Prepared By

Kristi Fahy, RHIA
Ron Hedges, JD
Dawn Paulson, MJ, RHIA, CHPS, CPHI
Robyn Stambaugh, MS, RHIA

Acknowledgments

Patty Buttner, MBA/HCM, RHIA, CDIP, CHDA, CPHI, CCS
Jill S. Clark, MBA, RHIA, CHDA, FAHIMA
Stephanie Helmke Costello, MS, RHIA
Julie A. Dooling, MSHI, RHIA, CHDA, FAHIMA
Margaret Foley
John J. Francis, JD, MPP
Nyssa M. Fuhreck
Elisa R. Gorton, RHIA, CHPS, CHC
Steph Luthi-Terry, MA, RHIA, CHPS, FAHIMA
Ann Meehan, RHIA
Laurie Peters, RHIA, CCS
Donna Rugg, RHIT, CDIP, CCS-P, CCS
Molly Watson
Shawn Wells, RHIT, CHDA
Kenneth J. Withers, JD, MLS
Jami Woebkenberg, MHIM, RHIA, CPHI, FAHIMA

Read More Online Column Discusses Legal Topics

https://journal.ahima.org/category/blogs/legal-e-speaking/

The *Journal of AHIMA* web-exclusive online column Legal e-Speaking discusses the legal consequences that abound at every corner in healthcare, and what impact they might have on health information management roles.

Article citation:
AHIMA. "Health Information Management and Litigation: How the Two Meet." *Journal of AHIMA* 90, no. 5 (May 2019): 38-45.