Electronic Data Discovery and the New Federal Rules: Health Industry Organizations at Particular Risk

By Christopher A. Myers, William F. Hamilton And Suzanne M. Foster Holland & Knight LLP

Introduction

On December 1, 2006, significant changes to the Federal Rules of Civil Procedure (FRCP) specifically directed to discovery of electronic data (E-Discovery) went into effect. Compliance with the new rules may be particularly complicated for health industry organizations, because of the ongoing conversions to paperless record keeping and healthcare organizations’ unique need to document and keep secure virtually every aspect of their business and treatment processes. It is crucial for entities involved in the health industry to swiftly incorporate the FRCP changes into comprehensive records management systems. If they wait until the first lawsuit or investigation hits, it may be too late. Compliance with the new rules will become even more important, if, as expected in the near future, state court litigation, such as medical malpractice, begins to follow the federal model for e-discovery.

The federal rules were amended to deal with the explosion of electronically stored information (ESI) by providing directions for dealing with the preservation, exchange and production of ESI. Over the past several years, the healthcare industry has seen its own explosion in ESI, as most healthcare organizations are quickly replacing paper medical records, research data, sales and marketing information and other paper documents with electronic health record (EHR) systems and diverse kinds of electronic information systems. As clarified by the new FRCP changes, the contents of the EHR and other electronic systems are subject to discovery and production requirements. A major challenge for healthcare organizations will be to comply with e-discovery requirements while also following privacy and security laws that protect patient health information. Healthcare entities need to prepare in advance in order to avoid the penalties, sanctions and litigation costs other industries have experienced as a result of antiquated records management systems.1

A further complication for health industry players is the proliferation of government audits and investigations. Each audit or investigation brings with it immediate obligations to preserve potentially relevant hard copy and electronic records. While a failure to preserve records in the normal litigation process can result in sanctions and penalties, failure to preserve records in the context of government audits and investigations can also result in criminal investigations for

---
Obstruction of Justice [is there a specific reason for initial caps? If not, let’s use lower case. I used them because this the formal name of the statute. It is not a generic violation, but a specific one.] and related offenses.

Although the detailed standards for the production of health industry ESI will play out in litigation and government investigations over the next several years, healthcare organizations should not use this as an excuse for procrastination on records management programs and procedures for dealing with electronic information. This article will: [but earlier it says what this article will do. Please remove the redundancy. That will also make the intro shorter, which it should be (Done)] highlight risk areas that legal and compliance professionals in the health and life sciences industries should consider in advance of having to deal with e-discovery demands; provide a three step plan for dealing with e-discovery once a request is received; and discuss the importance of implementing a records management program as part of a comprehensive compliance and ethics program. For ease of discussion, we will focus our attention on the kinds of electronic records that are, or will be, maintained by hospitals and other health care provider organizations. These principles, however, are equally applicable to pharmaceutical manufacturers, pharmaceutical distributors, pharmacy benefits managers, pharmacies and other health industry organizations.

**Preparing for E-Discovery**

In most organizations, the legal, compliance and information technology departments typically lead the preparation of electronic and other forms of discovery. In healthcare organizations it is critical to also include representatives from the Health Information Management (HIM) or medical records team, grants or research departments and any other department which creates, uses or maintains electronic information. Document requests in litigation or government investigations almost always demand production of information that includes patient health information; therefore, the persons that will be responsible for preserving, accessing, gathering and producing the information from the EHR must thoroughly understand the issues addressed below. Furthermore, in preparing for e-discovery these departments should work together to: 1) develop a comprehensive knowledge of their electronic information systems; 2) develop and implement a records management plan; 3) learn where, and in what formats electronic information is stored, including the kinds of metadata are contained in them; and 4) maintain only information required to be preserved, or with an important business or legal use.

**Metadata**

Metadata is the information in an electronic document that tells the knowing reader when and in what manner the document was created, changed, and accessed. Metadata is not present in the management or production of paper documents. Events and information about who knew what and when are often critical to healthcare cases, especially malpractice actions and fraud investigations. Thus, requests for metadata will likely increase significantly once litigants begin to fully understand its worth. Indeed, several courts already have required that metadata be included when reproducing electronic documents.² EHR metadata, for example, provides

---

information about every person who viewed or entered data in the patient's record. It provides a
good starting point for identifying key witnesses and issues.

Recently, the University of Miami/Jackson Medical Center settled a malpractice case when an e-
discovery request revealed that the surgery's electronic anesthesia record showed ninety minutes
of undocumented vital signs and that the attending anesthesiologist recorded his attendance for
the entire surgery just minutes after it began. These facts emerged through a hidden electronic
time stamp embedded in the electronic anesthesia record. As a result, the hospital settled notwithstanding that the anesthesiologist apparently did stay for the entire surgery and the
undocumented vitals probably did not lead to the adverse outcome.

We can expect an increase in specific e-discovery requests for metadata in light of the significant
information the metadata provides about the record's integrity and reliability. Indeed, every time
a document is accessed, its metadata changes. Healthcare organizations and their lawyers need
to know how to preserve and access metadata to respond to e-discovery requests and manage
both favorable and potentially damaging information. It simply must be a part of risk assessment
and case analysis. In addition, healthcare organizations should develop policies and procedures
that address retention and destruction of metadata and electronic documentation protocols for
their clinicians. Courts are increasingly strident in awarding sanctions where there is a lack of
diligence in preserving electronic data locations. [needs substantiation in footnote (Done)]

**Trends, Statistical Data, and Related Information**

Healthcare organizations must also be concerned about the increasing ease of aggregating and
searching large collections of data files to extract statistical data and patterns. In the paper
world such analyses were often too onerous and time consuming to be feasible. Now, large
amounts of data contained in EHRs can easily be extrapolated to identify legally relevant
information. For example, in the context of a government investigation, information about how
often a particular doctor codes a certain procedure can be easily determined and is likely relevant
to an investigation of that doctor's billing habits. Or, in the case of a malpractice action, it may
be relevant to know how many patients with the same diagnosis had a similar outcome.
Although this kind of information can prove extremely useful to healthcare organizations' internal quality and safety personnel, it may or may not always be helpful in the context of litigation or an investigation if it might support a finding of negligence or improper coding.

**Prompts and Alerts**

Healthcare organizations should know whether their EHR or other prescribing software produce prompts or alerts. This information is conveyed through interruptive alerts which require a
recorded override to move forward, or a recorded disabling of that same override. These alerts
are sometimes referred to as a "break the glass" notifications. For example, if someone without
appropriate access tries to view a particular patient's EHR, a break the glass alert would pop up
and require an affirmative keystroke by the person before access was allowed. Other alerts may

---

4 See Zubalake and Morgan Stanley, supra n.1.
relate to clinical decision-making and require an additional acknowledgement or disabling before a physician proceeds with entering a prescription for a certain drug or orders something that is different from the standard treatment protocol. Admissibility and relevance of this type of evidence in courts has yet to be determined; however, healthcare organizations should preemptively develop policies controlling whether, how and for how long they store prompt and alert information and discuss the relevance of these alerts before turning them on or off in their EHRs.

**Privacy and Security Considerations in E-Discovery**

The FRCP definition of "relevant" information\(^5\) is extremely broad. It includes all documents "reasonably calculated to lead to the discovery of admissible evidence." \(^{Id.}\) Traditionally when a request for a patient's medical record is made, HIM professionals are trained, and obligated by the Health Insurance Portability and Accountability Act of 1966 (HIPAA)\(^6\), to produce only those records that are related to the reason for the request. For example, if a patient's record was subpoenaed for a case related to a car accident in which the patient broke his leg, only those records related to the broken leg would be copied and produced. In other words, it would not be appropriate under HIPAA to include that patient's prior substance abuse or mental health treatment (unless these issues were material to the case). With electronic records from multiple and integrated sources, it will be more important than ever that the organization has professionals that are trained in discerning which information is relevant and which is, or is not protected. With the volume of electronic information rapidly increasing, and the ease of transmitting it by mistake, inadvertent production of protected information is a greater risk than ever before. Moreover, federal and state laws require added caution for HIV, mental health, substance abuse, genetic testing results and certain other sensitive health information. Special records management guidelines should be instituted, and if this information must be produced, privacy requirements need to be a high priority concern.

Another difficulty most healthcare organizations will have in responding to e-discovery requests will be determining how to freeze the record to produce a snapshot for any relevant point in time. With paper records a complete copy can be made and filed away for future reference. This is not usually the case for most EHRs. A patient's EHR may be accessed from a variety of locations and once information is inputted it may automatically change related information within the EHR, even information related to a prior date.

**What to Do When an E-Discovery Request is Received**

Given the almost unthinkable volume and volatility of ESI managed by healthcare organizations, corporate counsel (and compliance officials) are now under tremendous pressure to quickly issue preservation/litigation hold orders of the appropriate scope and to make sure they are enforced. Further, counsel must, in very short order, determine how to accomplish searches for potentially relevant information, and then review and produce responsive data. Under the new amendments, counsel is now required to make a series of nearly immediate judgment calls that may

\(^5\) FRCP 26(b)(1). "Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."

\(^6\) Pub. L. 104-191, 110 Stat. 1936; 45 CFR Parts 160 and 164,
subsequently be questioned by the courts, opposing counsel or the government. Worse, because of the transitory nature of electronic documents and EHRs, there is likely no chance for a "do-over" if a judgment call is later questioned.

In the context of government investigations, such as those under the False Claims Act\(^7\), the stakes are higher. If ESI that the government believes might be relevant is not preserved, the company and its officials could be investigated for Obstruction of Justice, False Statements [again, if there's no reason for initial caps, let's not use them; see previous comment] or other offenses based solely on the failure to preserve records, or making inaccurate statements regarding the existence of certain records. Law enforcement agencies and prosecutors may impose their own version of an adverse inference by concluding, based on the failure to preserve records, that the scienter, or intent element of the charges they are investigating, is supported by this failure.

The risk of future untoward consequences such as sanctions and adverse inferences can be minimized by following the procedures contemplated in the FRCP amendments, and by incorporating them into a comprehensive records management program. The three key procedures under the Amendments are as follows. First, as soon as the litigation or investigation begins, or as soon as the duty to preserve records is otherwise triggered, conduct a thorough ESI self-analysis. Second, based on the ESI self-analysis, make prompt preservation decisions, communicate those decisions to all necessary individuals, and make sure those decisions are properly implemented. Third, analyze any privacy and security concerns related to patient health information, examine the cost and expense of both your document preservation and the required search of your ESI locations for relevant data. Promptly schedule the Rule 26(f) conference (or a meeting with government investigators) and disclose your concerns, analysis and decisions. If the opposing side agrees, you will have a strong response if ESI evidence has been lost or can only be recovered at great expense. If the opposing side does not agree with your preservation, search and production decisions, you have an early opportunity to seek guidance from the court, or to negotiate a common understanding with the government investigators.

**Step 1: The Initial Self-Analysis**

When litigation or an investigation is "reasonably foreseeable,"\(^8\) a duty to preserve potentially relevant records, including electronic records, is triggered. It is very easy to underestimate the scope of the documents the opposition, or the government, will request and which may be relevant to claims or defenses in the case. A good exercise is to assign one member of the attorney team to step into the role of the other side in the matter, and assign him or her the task of developing a list of categories of all documents the other side may request, or which might be relevant. Depending on available resources, this task should be attacked by a team, at minimum, composed of a lawyer and employees at the core of the matter. Also, be careful not to confuse "custodians" with "witnesses." A secretary may be a likely custodian, but not a likely witness.

Next, the IT and HIM departments must be involved. The possible locations for ESI for each custodian must be considered and documented. They may include: laptops, servers,

---

\(^7\) 31 U.S.C. §§ 3729-3733 (Civil False Claims Act); 18 U.S.C. § 287 (Criminal False Claims Act).

Blackberries, home computers, network file servers, Exchange, or other email servers, flash drives, discs in drawers, back-up tapes, etc. The IT department's active cooperation is crucial for an understanding, search and preservation of these various sources. Each custodian must also be questioned regarding possible locations of ESI (as well as traditional paper documents).

**Step 2: The Initial Preservation Decisions**

The next step is both critical and difficult in light of the need to anticipate what paths an investigation or litigation may take, and the severe sanctions possible if the other parties or the court disagrees with the decisions made: What data of each custodian must be promptly preserved and by what method. First, a few basic rules: the hard drives of all core witnesses and custodians should be immediately preserved bit by bit. This requires capturing all of the "active" data on the drive, plus the deleted matter that has not been written over. Don't forget the email and file servers. Make sure to take a full snapshot of the server to prevent the inadvertent loss of any relevant data. Issue litigation, or document destruction "holds" to all custodians and make sure that the IT department suspends any automatic delete functions of the system. In addition, all back-up tapes that have captured data from the core custodians should be preserved. At a minimum, a temporary hold should be placed on the rotation of back-up tapes that may have captured relevant data.

The next question is how much data beyond the core custodians must be preserved. This decision depends on several factors, including the potential value of the case, the locations of the data, the number of custodians, the potential relevance of any metadata to the case, and the cost of preservation and retrieval. The key in minimizing potential sanctions is to document your decisions. The risk of sanctions and criminal charges is dramatically reduced if your decisions are based on an informed, reasonable assessment of the value, or potential value of the data and the expense of preservation and production. As will be seen, if these decisions are made pursuant to a carefully designed records management program that has been implemented in good faith, and which are documented in a way that can be followed by the opposing party and the court, the basis for sanctions will be difficult to establish. The compliance and ethics officer and staff can help with this process and with the periodic follow-up which will be required. This will be discussed in more detail below.

**Step 3. The Rule 26(f) Meeting and Disclosures**

The biggest safety net for a company and its counsel in this complex process is the Rule 26(f) conference. The conference is the principle disclosure point, and through disclosure comes the maximum protection and risk reduction.

The Rule 26(f) conference must be the subject of thorough preparation. At a minimum, counsel must be prepared to discuss the following E-Discovery topics:

1. All locations of ESI, (including the EHR and other information systems, back-up tapes);
2. The kinds of ESI (medical devices, emails, spreadsheets, digital voice, etc.);
3. The accessibility of ESI;
4. The cost of retrieving ESI;
5. The methods and searches for retrieving ESI;
6. The materiality and relevance of the various locations of ESI;
7. What ESI should be preserved in its original form;
8. The costs of preservation of ESI (the cost of forensic images and back-up tapes);
9. The form of ESI production.

The Rule 26(f) conference should be undertaken as early as possible in the litigation. Why? Because these disclosures and procedures provide the company and its counsel with a safety net. If the opposition accepts proposals and decisions regarding ESI, then the potential for future sanctions related to deleted, lost or otherwise destroyed information is dramatically reduced, if not eliminated. On the other hand, if the opposition does not agree with your proposals, the initial decisions can be modified promptly, sometimes at the cost of the opposition. In addition, early discussion gives you the opportunity to take disagreements to the court.

This is also true in the context of a government investigation. Although there is no Rule 26(f) conference in a criminal or civil fraud investigation, if preservation decisions and parameters are proposed to and agreed to by the government investigating agency, or the Department of Justice, it would be difficult for them to later argue that you have obstructed the investigation. It is particularly important in criminal cases to document any agreements with the government on this issue. Sometimes investigations can continue over a period of years. Lead prosecutors and agents frequently change. Without good documentation, it can be difficult to confirm, or provide evidence of preservation agreements that happen at the beginning of an investigation.

**The Importance of a Comprehensive Records Management Program**

As can be seen from the recommendations above, healthcare organizations must be in a position to take action virtually immediately once they have reasonable anticipation of litigation or investigation. The initial self-analysis and the preservation decisions must be undertaken quickly and efficiently. Employees must receive guidance, and procedures need to be in place for establishing, enforcing and documenting the litigation hold activities. In order to prepare for and attend the Rule 26(f) conference, or to meet with prosecutors or regulatory agents in a criminal or civil investigation, you need to quickly analyze and propose preservation and production parameters. You need to be in a position to present and argue cost issues to protect from potentially massive discovery costs, potential sanctions, and, even criminal liability.

The best way to accomplish all of these things in an efficient, cost effective manner is to have a fully implemented, comprehensive records management program in place. Such a program should be communicated by senior management through policies and procedures tailored to the business methods of the company. These procedures would then be incorporated into the company's culture and operations by training employees and monitoring for compliance.

Good records management programs can save companies hundreds of thousands of dollars. They establish processes to keep records that the company needs or is required to maintain and to destroy documents the company no longer needs. In today's electronic world, reduction of records storage costs can be a tremendous benefit to the bottom line. Thus, for example, many companies are choosing to delete, or overwrite emails that are more than thirty days old. This
can be an appropriate cost saving decision. As another example, many companies are now evaluating the need to retain disaster recovery back-up tapes for periods beyond reasonable usefulness. The low cost of storing electronic data often fails to trigger an IT budgetary review. As a result, some companies awake after years of slumber to find themselves burdened with terabytes of data, worthless for any business purpose. Unfortunately, what was perceived as a minor IT budget item may become a massive litigation expense if the stored data must be restored, processed, and reviewed. Failure to confront data storage results in a de facto decision to keep the data. This de facto default decision is often the wrong decision. Equally important, your company must have procedures in place for reacting promptly to possible lawsuits or investigations and to stop any destruction of relevant records.

The Role of the Compliance and Ethics Program

All of these complex analyses and decisions should not simply be left to the IT Department, as is currently the case in many companies. These activities are best overseen in the context of a company's compliance and ethics program. The program should include records management, retention, and preservation issues in its annual risk assessment. The compliance officer should meet with representatives of the various legal, operational and management departments to discuss and help in the process of devising a records management system which will work in the context of the organization's size and business activities. In light of the risks of a compliance breakdown, records management should be one of the priorities of the compliance and ethics program until a functioning system is in place.

The compliance department, whether it is independent, part of the legal department, part of a risk management department, or is organized in some other way, is in the best position to understand the processes needed to implement a records management program and integrate it into the organization's operations. These requirements follow the elements of an effective compliance and ethics program, and include: risk assessments; written standards; designated compliance personnel; training and communication, auditing and monitoring; incentives and discipline; remedial action and periodic revisions. Compliance professionals understand these elements and can help make them work effectively in the context of a records management system. The compliance team should collaborate closely with the legal team and the business personnel to address this new, and growing compliance risk area.

Conclusion

E-Discovery and the new rules that govern it present the specter of formidable costs and significantly increased litigation and investigation risks. But, both the costs and risks of E-Discovery can be dramatically reduced through a comprehensive records management program combined with the hard work of self-analysis, reasoned preservation of relevant records; and appropriate disclosure, either under Rule26(f) or in the context of an investigation.

Christopher Myers can be contacted at chris.myers@hklaw.com. William Hamilton can be contacted at william.hamilton@hklaw.com. Suzanne Foster can be contacted at suzanne.foster@hklaw.com.