



Rashbaum Associates, LLC

# Electronic Health Information Management: Risk and Cost Controls in Litigation Discovery



## Electronic Health Information Management: Risk and Cost Controls in Litigation Discovery

### **Executive Summary:**

Health care entities have been moving in the direction of increased digitization of information for some time, with caregivers increasingly communicating with each other and with patients by email; laboratory results and radiology images primarily stored and disseminated electronically; and claims and reimbursements long ago having given up the pencil and pad. This transition picked up considerable speed with monetary grants to expedite the transition to electronic health records in the American Reinvestment and Recovery Act of 2009 (colloquially known as “The Stimulus Package”).

The increase in the amount of digitized medical information means that health Electronically Stored Information (“ESI”) will increasingly become the predominant form of evidence in regulatory proceedings and litigation. Cost-efficient management of that information – preservation, identification, collection (access), and production – takes on concomitantly greater significance than at any time since medical information first migrated from paper to electronic formats.

As a balance to the significant increase in the universe of ESI generated and maintained by health care organizations, the privacy and security Rules of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) have been revised and expanded as the potential vulnerability of ESI to breaches of privacy and security have become front-page news. Health care entities thus face increased exposure to enforcement proceedings by regulatory agencies at the federal and state level, as well as surveys (such as those by the Joint Commission on Accreditation of Health Care Organizations) and external or internal audits. Pursuant to the expanded HIPAA provisions, state attorneys general will now have jurisdiction to pursue violations of the HIPAA Privacy and Security Rules, a significant increasing in the potential for enforcement.

Health care organizations wanting to reduce the risks and costs associated with the increased legal and regulatory exposure should consider implementation of a Health ESI Risk Mitigation Program. Components of such a program can include Discovery Readiness Assessment, Information Governance Assessment, ESI Content Mapping and Legal Hold Management protocols.

## Introduction

The primary forms of information sought in regulatory proceedings, audits, surveys and litigation is, increasingly, ESI such as lab data, radiology images, caregivers' notes and emails between caregivers. Electronic health information requires careful management in order to meet these demands for ESI, and well-honed response mechanisms when it must be produced. The responding entity must know how its electronic health information is created, where it is stored within the enterprise, how best to access the data for collection, how it is backed up, and all relevant retention policies and schedules applicable to the data in order to respond to requests for health ESI production. All potentially relevant electronic health information must be identified and preserved, often on very short timelines, to avoid potential penalties and sanctions from regulating entities and courts. In the event some potentially relevant data cannot be produced, which will occur since no system is perfect, well-designed protocols for preservation and management must be documented so that the system of data preservation can be defended and the risk of penalties and sanctions mitigated.

This White Paper discusses trends in the evolving legal and regulatory environment relating to health ESI. The author also outlines a program designed to reduce the risks and costs involved in producing health ESI in response to demands.

## The Landscape: Regulations and Case Law

ESI in the health care environment poses unique challenges in preservation, identification, collection and disclosure. HIPAA mandates, for covered entities (health care provider, health plans and clearinghouses<sup>1</sup>), preservation of data used for treatment, payment or hospital operations in a secure environment, and governs access to and disclosure of Protected Health Information ("PHI"), which is defined as "individually identifiable health information".<sup>2</sup> The Privacy and Security Rules of HIPAA were expanded and supplemented by the American Recovery and Reinvestment Act of 2009 ("ARRA"). Among other things, this provision increased the exposure of covered entities to regulatory scrutiny by requiring periodic audits of covered entities by the Office of Civil Rights of the U.S. Department of Health and Human Services<sup>3</sup> and expanding HIPAA enforcement jurisdiction, previously confined exclusively to the U.S. Department of Health and Human Services, to state attorneys general.<sup>4</sup> This last provision is currently

---

<sup>1</sup> 45 C.F.R. §160.102

<sup>2</sup> 45 C.F.R. §164.501

<sup>3</sup> §13411

<sup>4</sup> §13410(d)

in effect. New and costly procedures are mandated for notification of patients in the event of a breach of confidentiality.<sup>5</sup>

Yet HIPAA, even as expanded and supplemented, remains a floor for medical confidentiality. States laws may be, and frequently are, more demanding in their restrictions on disclosures of patient information. One of those requirements is documentation of a protocol for records retention (which includes such responsibilities as disclosure and deletion). In *Randi v. Long Island Surgi-Center*<sup>6</sup>, a New York intermediate appellate court upheld a \$300,000 punitive damages award for violation of a patient's privacy instructions (the case was brought under New York's Public Health Law) on the ground, among others, that the facility had no written privacy policy or procedure and no training protocol for implementing the putative privacy practices.

The federal government, even before the enhancement of HIPAA in the ARRA provisions, had begun ramping up HIPAA enforcement. In July, 2008 Seattle-based Providence Health and Services resolved a HIPAA proceeding brought by the Office of Civil Rights of the U.S. Department of Health and Human Services with a Resolution Agreement and Correction Plan. Providence had failed to safeguard patient information stored on a variety of portable and backup media. The resolution entailed a \$100,000 civil monetary penalty and a detailed (and, no doubt, costly) Corrective Plan to protect electronic information against loss. In addition, Providence must submit compliance reports, indicating that it is implementing appropriate safeguards and training its workforce on those safeguards, for three years.<sup>7</sup>

The lack of an assessment for readiness to produce ESI when demanded by an audit, survey, investigation or litigation, and a failure to have in place a plan for doing so can have disastrous consequences. In *Keithley v. The Home Store, Inc.*<sup>8</sup>, the failure to have a documented plan to produce ESI when required, and the lack of a written plan to issue and implement a legal hold (suspension of automatic deletion of emails and requirement for preservation and safeguarding of ESI in reasonable anticipation of litigation) was, according to Judge LaPorte, "gross negligence."<sup>9</sup> The court imposed attorney's fees and costs of almost \$150,000, and recommended an adverse inference jury instruction (advising that jury that it may infer that the lost emails, if produced, would have been adverse to the producing party).

---

<sup>5</sup> §13402

<sup>6</sup> 46 A.D.3d 74, 842 N.Y.S.2d 558 (2d Dept. 2007). Verdict was reversed on other grounds (flawed jury instructions)

<sup>7</sup> <http://www.hhs.gov/news/pres/2008pres/07/200807179.html>

<sup>8</sup> 2008 WL 383384 (N.D. Cal. August 12, 2008)

<sup>9</sup> *Id.* at \*12.

## Emerging Themes

**Health ESI is proliferating.** As the health care industry relies more extensively on electronic communications and records, the quantum of data such as emails between caregivers and between caregivers and patients, and digitized chart entries and test results, is increasing at an exponential rate. Management of this data in an efficient manner, including access for surveys, audits, investigations and litigation, is critical to effective cost controls.

**Most evidence in health care proceedings is digital.** Health ESI is becoming the predominant form of evidence requested by investigatory agencies and courts. Laboratory reports, radiology images, chart notes and, of course, emails are among the first items demanded when a proceeding is commenced.

**The risks are real.** Technical and administrative safeguards for health ESI are mandatory pursuant to HIPAA and state laws. The penalties for failure to draft and implement these protections are severe and federal and state agencies will conduct compliance audits. Failure to produce health ESI in litigation can result in monetary sanctions, adverse inference instructions (which can result in adverse court decisions) or default judgments.

### **Components of a Health ESI Risk & Cost Mitigation Program**

To minimize cost and risk, the enterprise must be fully prepared to meet the demands of producing health ESI in an audit, survey, governmental investigation or litigation. This process of responding to a request for ESI is known as electronic discovery, or “E-discovery.” A health care provider’s ability to efficiently manage E-discovery is a direct consequence of the time and effort put into preparation. Deadlines to respond to demands for health ESI from a state or federal are typically very short. Requests for Production in litigation and third-party subpoenas require detailed compliance which is subject to court review. Further, courts may look more favorably upon applications to shift the costs of large data productions to the requesting party if the enterprise has documented the details of the costs and effort required to meet the demands of discovery.

Accordingly, the first stage of a Discovery Readiness Assessment (“DRA”) is devoted to a comprehensive assessment of the enterprise’s overall readiness to meet legal or regulatory disclosure requirements. Current practices in the identification, preservation, collection, processing, review, and production [here you list several phases of the EDRM model, while in other sections you only talk about identification, preservation

and collection] of health ESI for disclosure to governmental entities, courts or adversary counsel will be analyzed and documented.

The analysis will include:

- **Assessment** of current policies, practices, people, and technologies associated with the organization's existing electronic discovery response process
- **Identification** of gaps between current practices and best practices, and
- **Recommendations** detailing how the organization can close the identified gaps and improve its ability to respond to e-discovery obligations

This methodology begins by forming an inter-disciplinary group of key representatives from divisions or departments regularly involved in production of ESI, such as Risk/Compliance Management, Medical Records, Legal and IT. Existing disclosure and discovery processes would then be analyzed relative to best practice.

### Information Governance Assessment

Crucial to the enterprise is ascertaining how health ESI is accessed, utilized and disclosed within the organization and to outside entities. This will be a critical area of inquiry in the coming period of heightened privacy scrutiny pursuant to the expansion of enforcement of the revised HIPAA Privacy and Security Rules.

The foundation for the Information Governance Assessment and Gap Analysis process is a review of the organization's current Information Governance practices. There are five key goals when it comes to implementing governance practices and managing ESI for information confidentiality/security, regulatory compliance, and litigation response: acquire less, replicate less, organize it better, improve access, and dispose as soon as practical. In order to accomplish these goals, the enterprise's IT owners and managers (administrative personnel as well as "front-line" users) would be interviewed to determine how systems are managed, the rules applicable to these systems and who's ultimately in charge of the pertinent ESI. Some of the questions which may be asked include:

- What do employees know about applicable usage guidelines? Do they follow the guidelines?
- Are the users aware of restrictions applied to data storage?
- How is the data organized?

- How is the data secured?

By answering these and other questions, a clear view into policies and actual practices of how ESI is managed will be gained by all involved in the Information Governance effort.

Establishing an understanding of the organization's security/regulatory/litigation portfolio and risk tolerance will also provide a baseline upon which to evaluate the Information Governance practices.

Based on the Information Governance Assessment, specific, detailed and actionable recommendations can be prepared for ensuring that repeatable and defensible policies and practices are in place for the implementation of confidentiality and security controls, and response regulatory and litigation obligations. These recommendations would include specific information about the people, process and technology needed to build and implement effective solutions, including metrics and management controls, and will offer the framework, tools and templates to accomplish the tasks.

### ESI Content Mapping

In most primary care systems, such as hospitals, digitization of medical information has been an incremental process. Laboratories, radiology departments, clinical departments, faculty practices and administrative departments adopted electronic communications and record-keeping at differing levels of implementation, and at different times. Accordingly, jurisdiction over and responsibility for the spectrum of health ESI may be fragmented. Medical Records may be a repository for the formal hospital chart, but individual departments and services often have their own ESI modules which may or may not be updated regularly to the formal record. In many instances emails are not centrally categorized (i.e., Risk Management, NICU, Obstetrics and Gynecology, etc.), and thus difficult to identify and collect in the event of a time-sensitive regulatory, survey, audit or litigation demand.

ESI Content Mapping provides the framework for an enterprise-wide inventory of the most relevant data repositories for legal and regulatory proceedings faced by the organization. An issue mapping exercise, as part of the content mapping process, identifies the type and scope of data most frequently demanded. The results of this exercise provide a rational framework for narrowing the scope of systems that must be documented in the ESI Content Map. These data types then become the basis for confirming the key content repositories and applications that represent the greatest cost, bur-

den and legal risk to the organization. The key content repositories and applications are then inventoried in the ESI Content Map.

There are several benefits to an ESI Content Map, and they lend themselves to a cogent value proposition and potential return on investment. Quick access to information on potentially relevant ESI for a proceeding can greatly reduce the cost of attorney and staff time in discovery. An ESI Content Map also provides baseline measures for estimating the cost of the matter. Further, the ESI Content Map cost-effectively aids business processes, in that it can be shared by many departments and divisions, thus providing a common knowledge base for improved information governance and discovery response practices. Risks associated with proceedings are reduced as well because a consistently applied and systematic process for identifying, preserving and collecting potentially relevant sources of health ESI can mitigate the risk of missing relevant data sources. Omissions of relevant data sources can result in damaging sanctions for failure to produce requested ESI.

### Legal Hold Management

Management of legal holds is one of the primary means by which a health care organization protects itself when faced with investigations, audits, surveys or litigation. Mitigation of risk and cost lie in being able to move quickly to identify and preserve relevant health ESI when legal hold obligations arise. When such obligations arise, organizations must suspend routine deletion/destruction of pertinent data and issue legal hold notices to all custodians of relevant data once an obligation to preserve arises. “Custodians” are the primary owners of such data. For example, a physician who saves a chart entry or email about a patient’s treatment on his or her local hard drive is the Custodian of that data.

Legal hold management may intersect several departments or divisions, and integrally involves Legal, IT, Risk Management/Compliance and IT. The same commitment to quality assurance is required as the organization devotes to its business and clinical practices, in that failure to preserve relevant data pursuant to a legal hold protocol can result in sanctions up to and including loss of the proceeding or law suit. In the context of the Electronic Discovery Reference Model<sup>10</sup>, relied upon by courts in considering the sufficiency of health ESI production, legal holds are central to the preservation stage.

---

<sup>10</sup> [www.edrm.net](http://www.edrm.net)

Legal hold management is a process, not a policy. As such it can, if not planned and implemented properly, devolve into an administrative quagmire as requirements of custodians, system processes and requirements of the pertinent matter overlap. To avoid this, the four steps to a successful legal hold management plan include:

- Determination of the trigger for a legal hold
- Identification of health ESI to be preserved (including identification of custodians, data stewards and persons of specialized data knowledge, and determination of the relevant data attributes and repositories)
- Establishment of a plan to preserve that ESI
- Implementation and management of preservation and the legal hold process

The trigger for the legal hold obligation is “reasonable anticipation of litigation.” This may vary by such factors as depth of knowledge of the imminence and credibility of a claim, and the risk of losing relevant health ESI without a hold in place. Once the ESI relevant to that claim has been identified, often with the aid of an ESI Content Map, the appropriate custodians should be identified and sent a legal hold notice. A system to implement the legal hold notice, including tracking of the distribution of the legal hold notices and compliance, is also required so that the organization can defend its compliance with its preservation obligations.

There is no single standard governing how the preservation obligation should be implemented. Preservation strategies may include preserving in place (preserving ESI in its native repository); quarantining files (confiscating the physical media where the files are stored); or “copying files to preserve,” in which copies are made of the files or images taken of entire disk drives, and the copies or images are stored in a protected repository while metadata (data about the data and its creation) is carefully preserved.

Similarly, a health care organization has options for implementation of the legal hold. For example, there are systems which can manage the legal hold process and systems that are capable of applying a legal hold on the data stored within a given repository. Regardless of which technology is selected to manage the legal hold process, the litigation/regulatory proceeding workflow and management process must be addressed first.

## **Conclusion**

Health care organizations face increasing cost and time pressures as the quantity of health ESI increases in near-lockstep with regulatory and legal demands for that information. Control over these demands on finances and personnel requires management of the flows of health ESI as a mission-critical process, so the organization can focus on the business of patient care.

When a health care enterprise thoroughly understands its obligations for identification, preservation, collection and disclosure of health ESI, it will be in a much better position to mitigate the risks and costs associated with regulatory and legal demands for ESI. At the same time, tools such as ESI Content Mapping and Information Governance Assessments can be leveraged by the entire enterprise to create efficiencies in managing the expanding quantity of health ESI.

«Organization»