GALEN HEALTHCARE SOLUTIONS

# ACCESSIBILITY

MUCH MORE THAN I.T.

# LEGAL CONSIDERATIONS FOR HEALTHCARE DATA ARCHIVING

Authors:

**Matt Fisher**

Partner, Mirick O'Connell DeMallie & Lougee, LLP

**Robert Downey**

Vice President, Galen Healthcare

**For more information visit www.galenhealthcare.com**

# TABLE OF CONTENTS

# SUMMARY

There are many legal considerations to evaluate when navigating the complex data structure and data sets, legal and compliance requirements, and continuity of care requirements that characterize effective healthcare legacy application retirement. Successful and risk-minimized healthcare data archiving requires the preservation of not only the organization defined legal medical record, but also data sets such as contextual audit trails, referenced data in ancillary systems, data change and version history, and even database metadata.

**Key Takeaways:**

**Preserve the Integrity of the Complete Record**
An organization's ability to preserve the integrity and completeness of the original record, especially the ability to recreate a copy of the record as it existed at the relevant time in question, may be compromised when EMRs are replaced.

**Don't Overlook Version History**
The version history for individual clinical items is a major data set often overlooked in data archiving.

**Retain Audit Trails**
Ensuring that a robust audit trail is retained and archived is essential for capturing the precise sequence of events, provides evidence that justifies and/or explains what actions have occurred, and is also vital to satisfy e-Discovery requests.

**Purging Archived Data Has Significant Legal Risk**
When it comes to purging of archived data, the ambiguity around retention guidelines at the state and federal levels have resulted in organizations putting themselves in considerable legal risk.

**Didn't get your questions answered in this paper, or have feedback for us?**

Let us know at www.galenhealthcare.com/ArchiveWhitePaperQuestions/

# BACKGROUND

Usage of Electronic Medical Records ("EMR") across care settings is now nearly universal. As a management tool, EMRs are intended to facilitate standardized care, provide access to complete patient records, and gain acceptance of policies, procedures and care protocols. However, EMRs also contain information potentially relevant to litigation, such as medical malpractice claims, regulatory investigations, False Claims Act allegations, HIPAA-related claims, and billing audits.

*In 2006, the Federal Rules of Civil Procedure acknowledged the advent of e-Discovery for the first time. The amendments to Rules 16, 26, 33, and 34 govern the disclosure and production of relevant electronically stored information in federal courts. For example, Rule 26(a)(1) obliges a party to disclose all electronically stored information in its "possession, custody or control" that it "may use to support its claims or defenses." Rule 26(f) requires a party to devise a discovery plan for how to produce this data.*

A clinician's use of an EMR is an increasingly significant factor in malpractice complaints. Indeed, individual clinicians are not the only ones at risk. Most healthcare delivery organizations are also at risk. All must show that the care they provided was consistent with acceptable medical standards of care at the time and was reasonable under the circumstances.

Furthermore, as organizations replace their EMRs and retire outdated legacy systems, they jeopardize data retention and access. An organization's ability to preserve the integrity and completeness of the original record, especially the ability to recreate a copy of the record as it existed at the relevant time in question, may be compromised when EMRs are replaced. This is particularly challenging because litigation and investigations can span several years, requiring a search for data contained in multiple EMR and/or legacy systems.

**85%** of healthcare provider organizations who have retired legacy IT systems and opted for health data archiving report positive financial impacts, according to KLAS research.

EMRs are a treasure trove of information, containing rich and deep data including patient demographics, symptoms, vital signs, medical diagnoses, treatments, progress notes, medications, immunizations, past medical history, laboratory data, care plans, and more. As such, the data contained in the EMR can reveal the standard of care and demonstrate consistency (or inconsistency) in treatment and policy application.

The challenge to organizations is exacerbated by the fact that not all healthcare data archiving solutions are designed to manage the rigors of e-Discovery and may lack critical capabilities and controls to reduce risk.

# THE "STATE" OF LEGACY DATA STORED IN AN ARCHIVING SYSTEM

There are generally three distinct "states" in which legacy data is stored in an archive system – *active*, in which data can be modified, *static*, that is "view only" data, and *cold storage*, which is infrequently accessed data retained to satisfy legal requirements. *Active* and *static* states are quickly accessible, while *cold storage* may not be accessible without additional effort.

To limit cost and effort, some organizations will archive legacy data in a *cold storage* state to be compliant with legal requirements, or they will archive portions of the data in a *cold storage* state, based on the level of activity, and frequency or necessity of producing online access to the data. But this type of fragmented archiving approach increases risk for the organization by inhibiting the ability to satisfy release of information requests within an allotted window of time, which may increase the risk of e-Discovery liability.

**75%**

Healthcare industry experts say that legacy systems consume 75% of hospital IT staff time and cost more money in annual licensing costs than hopitals pay in IT staff wages.

A best-practice, risk averse approach is to provide the same level of access for all archived systems and data sets. SaaS-native healthcare data archiving platforms designed from the ground up for the cloud are well suited to a cost-effective approach to the storage of legacy data without compromising accessibility or risking liability.

**Distinct States of Legacy Data Storage**

| | | |
|---|---|---|
| 1 | **Active** | Actively modified data |
| 2 | **Static** | View only data |
| 3 | **Cold Storage** | Infrequently accessed data |

# PURGING OF DATA

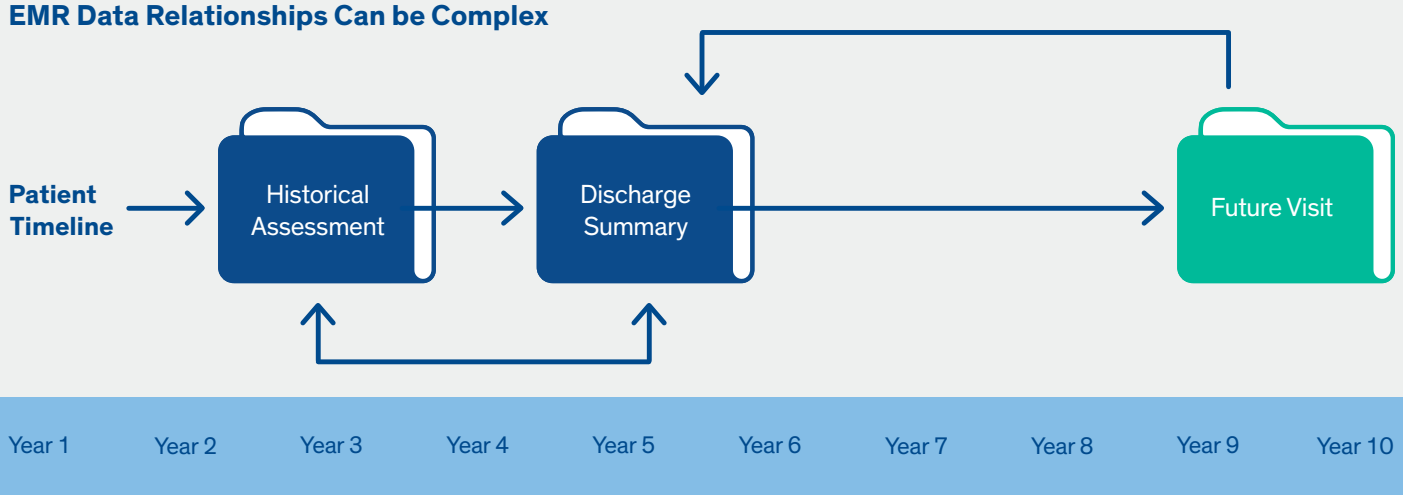
The ambiguity around retention guidelines at the state and federal levels have resulted in organizations putting themselves in considerable legal risk. Some organizations treat EMR systems as completely isolated repositories of information, and they start the retention clock ticking when activity in the EMR ceases. For example, when an organization migrates from one EMR to another, the activity in the legacy EMR winds down fairly rapidly. It's common for that system to be put in a read-only mode within weeks or months, and eventually that system's data may be moved into an archival solution. An organization may mistakenly "start the clock" for data within that system based on looking at activity only within the legacy system itself. Since that system is read only or archived, there will of course be no new encounters or data entry. This does

not mean, however, that the patient hasn't been seen in the go-forward EMR. Instead, organizations must use a global EMPI to track activity throughout all systems to accurately know when a patient's records can be purged without risk.

In order to realize cost benefit and risk aversion with regard to a patient's record not being retained beyond a period of time that would pose legal risk, organizations pursue purging of data within a record based on the age of the data itself. For example, a patient's record may have visit notes or other data points recorded decades ago, and the organization views this data as outside the retention window despite the fact the patient may have activity that's much more recent. Most legislation refers to the "patient record", with the usage implying an atomic quality to patient data. Thus, while individual pieces of documentation may be far older than retention requirements might indicate, it's not the age of the documentation that starts the clock. It's the most recent activity for the patient as a whole, in any system. This is further complicated by the fact that data within a typical EMR has complex relationships. A visit entry may reference an historical problem assessment,

which may itself be referenced by discharge summaries, for example. It is often not possible to delete an individual piece of documentation because of downstream dependencies in the system, causing unintended issues and potentially cascading deletions. While this scenario may have been common in the world of paper documents, an EMR is usually not structured to allow for selective purging of pieces of clinical documentation, with most only offering the ability to mark the information as "Entered in Error."

**EMR Data Relationships Can be Complex**




To lose or destroy data after litigation is reasonably anticipated and/or commenced can lead to dire consequences. Courts can, and do, punish parties, including healthcare providers, that engage in intentional or negligent spoliation of evidence, the legal term for the loss, alteration, withholding, or destruction of documents or other relevant information. Sanctions for spoliation may include payment of the other party's attorneys' fees and costs, dismissal of defenses or claims, and/or jury instructions that damage a defense.

# PRODUCTION OF RECORDS

Federal Rule of Civil Procedure 34(b)(2)(E)(i) provides that a party responding to a discovery request for electronically stored information "must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms." As reasonable as this rule may appear, it presents many difficulties stemming primarily from the fact that EMRs were not designed for purposes of litigation or legal discovery. Formatting patient records for discovery must meet varying levels and breadths of detail that will likely need to be comprehensive and capable of supporting underlying requirements for all potential data requests, ranging from clinical to audit-based. Record detail for virtually any shape of data, regardless of the patient modality (ambulatory/inpatient), must be captured to ensure a full and complete legal medical record. The detail fields displayed in the data archiving solution must be data source-specific, allowing archive details to expand and contract according to any source system and its associated data elements.

# VERSION HISTORY

The version history for individual clinical items is a major data set often overlooked in data archiving. For example, consider visit notes. Most note workflows include multiple edits to a visit note. Perhaps a nurse starts the note at the beginning of a visit, a doctor adds some relevant content during the face to face with the patient, and another clinical staff member adds additional content after hours. Each time the note is saved, it is usually a copy that is saved.

There is a good reason for such a process — it shows who made which changes, and what information was present in the EMR at a given point in time. From a clinical perspective, the most relevant data is usually the most recent, although there are certainly exceptions to this. From the legal perspective, having the capability to produce a "point in time" view is frequently critical.

**90%** of hospitals continue to run old applications to preserve data after an application has been replaced or retired

That is one big reason why virtually all EMRs include this type of versioning or change history for almost all-important clinical documentation. It is also why organizations should not ignore this data during retirement of a system. It is possible, perhaps even likely, that such data will never be needed, but, as the sophistication of clinical documentation has increased, so too have the legal requests for information in litigation, administrative hearings, and other venues for legal disputes.

## Scenario #1:

**Change Matters** — The following data set demonstrates how data can change in legally and clinically relevant ways, and which data are not typically captured by data archiving:

| Version | Problem Diagnosis Database Record | |
|---|---|---|
| 3 (Latest) | { "Created": "2006-12-28T09:13:49", "Updated": "2009-04-05T10:04:12", Updated ← "LastUpdatedBy": "MD Howell, Chris", Updated ← "Recorded": "2006-12-29T09:13:49", "OnsetDate": "2009-03-22", Updated ← "Diagnosis": " Myocardial Infaction (lateral wall)", "DiagnosisCode": "121.29", "View": "Chronic" } | "Unsafe" Change |
| 2 | { "Created": "2006-12-28T09:13:49", "Updated": "2006-12-28T09:13:49", Updated ← "LastUpdatedBy": "MD Smith, John", Updated ← "Recorded": "2006-12-28T09:13:49", "OnsetDate": "2006-11-14", "Diagnosis": " Myocardial Infaction (lateral wall)", "DiagnosisCode": "121.29", "View": "Chronic" Updated ← } | "Safe" Change |
| 1 (First) | { "Created": "2006-12-28T09:13:49", "Updated": "2006-12-28T09:13:49", "LastUpdatedBy": "MD Levine, Elizabeth", "Recorded": "2006-12-29T09:13:49", "OnsetDate": "2006-11-14", "Diagnosis": " Myocardial Infaction (lateral wall)", "DiagnosisCode": "121.29", "View": "Active" } | Initial Data Entry |

In the above example, which has been simplified for clarity, we have a patient who was diagnosed in December of 2006 (version 1) with a myocardial infarction. This version represents the initial data entry into the EMR by Dr. Elizabeth Levine. Note that the onset date was documented as November 14, 2006. In version 2, Dr. John Smith modified the diagnosis to change the view. This change is probably not clinically or legally relevant, so the loss of this information during a data archiving is unlikely to be a serious issue. Version 3 (updated on April 5, 2009), however, shows that Dr. Chris Howell changed the onset date for the diagnosis to March 22, 2009. The probable explanation for this date change is that the patient had a second heart attack, and the provider decided to update the first heart attack diagnosis with the date of the most recent incident.

Unfortunately, the change reflects an improper usage of the EMR. The diagnosis should have been resolved or put in a past medical history category, and a new diagnosis should have been recorded. For whatever reason, that did not occur. This change has significant clinical implications, as each heart attack a person suffers increases the risk of subsequent heart attacks and may require modifications in treatment plans. The loss of this information represents a gap in this organization's defenses against litigation as well as its ability to ensure patient safety. Beyond the clinical complications, the inaccurate change of the date of diagnosis could create a false impression of liability. If each subsequent heart attack increases the risk to a patient, not seeing the proper diagnosis history could influence clinical treatment decisions, which errors would be determinable by reviewing the version history.

# REFERENCED DATA IN ANCILLARY SYSTEMS

Healthcare delivery organizations have historically designated their Health Information Management ("HIM") departments as the official "custodians of medical records." Most HIM departments process and respond to subpoenas from courts, attorneys, and other sources. As such, it is critical to incorporate consideration of commonly missed data sets, as well as those in ancillary systems, into a healthcare organization's approach to information governance, including the establishment of policies to guide responses to discovery requests.

**Scenario #2:**

**Surgical Equipment Recall** — A device manufacturer issues a recall of equipment used for surgeries. The hospital must determine which patients may have been affected by the faulty equipment. In archiving, the review can be facilitated by linking the serial number stored in the materials management system to the patient's records in the legacy EMR. An inability to identify and subsequently notify patients of the recall could have drastic consequences for the patient's health, which in turn could create liability. Accordingly, organizations will not want to unnecessarily create risk.

**Scenario #3:**

**OIG Audit** — Healthcare clinicians and organizations are increasingly receiving funding from various government sponsored initiatives, which will not be given without the possibility of an audit of sensitive EMR data. This audit process could be triggered by:

1. **Subpoena**, a civil investigative demand, or a letter notifying the recipient of an intent to audit. Such a request would stipulate the need for access to all relevant records, reports, and previous audits (including potential legislative inquiries) and could be triggered by a report of suspected wrongdoing.

2. **Meaningful Use** incentive payment appraisals demanding verification that providers receiving Medicare and/or Medicaid Meaningful Use incentive payments were entitled to them.

# DATA RETENTION & E-DISCOVERY

Electronic Discovery, or e-Discovery, is a modern component of the traditional pre-trial process during which the parties to a lawsuit request that the opposing party turn over copies of documents that may contain valuable evidence or lead to admissible evidence. Once a lawsuit begins, parties in e-Discovery may be asked to produce answers and/or documentation about alerts (bypassed?), notes (who wrote it? who has reviewed it? when was it written? when was it signed? was it changed?), medication ordering, lab review, and many other data points. The scope of the searches related to e-discovery includes nearly anything electronic, though the specific areas to search are influenced by the wording of the discovery request. From that perspective, an organization likely does not want to volunteer information, which means paying particular attention to the exact wording of a request. Legacy and antiquated EMRs, and consequently the archival systems that replace these systems, are attractive targets for e-Discovery because the systems contain so much potentially useful information, including patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. Danger can arise if archival systems used to protect this data in accordance with applicable federal and/or state requirements are not capturing all of the data needed to render a complete view of the circumstances surrounding patient care.

**Scenario #4:**

**Legal Requests for Records** — A request for medical records is submitted to the HIM department regarding a pending legal matter involving a patient. The request for records may include the following data elements and challenges:

1. **Multiple encounters with multiple providers** across multiple data sources.

2. **All preserved chart data** within a particular range.

3. **Clinical instance data**, plus patient and user audit data specific to the data source.

The elements sought in the request can be problematic if comprehensive and well-thought out archiving plans are not put into place. While archiving plans will necessarily focus on operational and clinical considerations, healthcare organizations would be well served to add legal to the list as well. Legal requirements may slightly differ and could have a direct impact on an organization's ability to fully defend itself.

Healthcare delivery organizations are required to retain data from two years to twenty-five years after the last date of service to a patient. That period can be slightly different when the patient is a minor, as retention requirements are typically the longer of a stated period or until the patient turns 18 (or 21 in some instances). While the period in which a lawsuit can be initiated may be limited by statutes of limitation, the interval between an event and a lawsuit could still be significant and longer than anticipated.

The legal foundation for record requests rests upon rules of procedure at both the federal and state level. The particular set of procedural rules applicable to a case will depend upon the court in which the action was filed, namely federal court or state court. Interpretation of how the procedural rules will be applied can and does vary state by state on both levels. While it may be expected that all federal courts will interpret the federal rules in the same way, there can be splits among or between the circuits. However, the area of difference is more likely to arise on the state level. The differences underscore the importance of being well aware of the laws in the state where an organization is located, or where a particular facility is located, if an organization is spread across multiple jurisdictions.

An example of how one state interprets discovery is *Griffith v Aultman Hospital*, a decision by the Ohio Supreme Court. In *Griffith*, this court deemed that a patient's medical record is not limited to data solely in one location determined by the healthcare organization, often identified as the medical records department. This case centered around the plaintiff's request for the "medical record." When the record was produced, cardiac monitoring strips were not included since those were not in the record held by the records department. The Court expanded the organization's obligation of where to look for information constituting the record, determining that physical location of information is not determinative. Instead, the issue is whether a healthcare

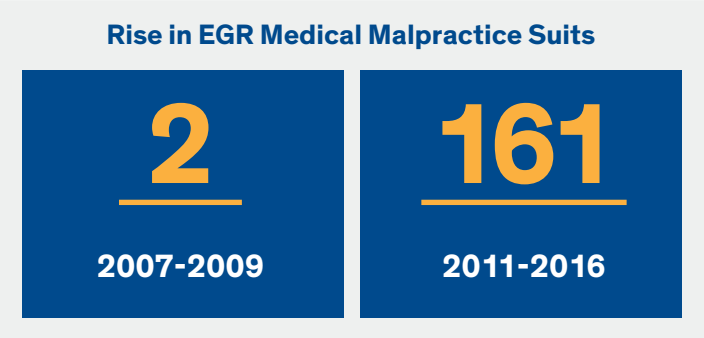
provider decided to keep data generated in the process of providing care and that that information pertained to diagnosis, treatment, history, or other use in the process. The decision means that in Ohio at least, any number of areas could contain information constituting the medical record, not the least of which are many folders in the EMR.

In addition, state laws can now frequently address issues relating to e-Discovery: *VA 32.1-127.1:03:* "Health record" means any written, printed or electronically recorded material maintained by a health care entity in the course of providing health services to an individual concerning the individual and the services provided. Embedded metadata, such as notes revisions and versioning are generally hidden, but they are an integral part of electronic stored information and include features such as "track changes" or "comments.

# ARCHIVING OF TELEMETRY DATA AND METADATA

The archiving of clinical data is the primary process that enables system retirement, but audit data sets must also be considered. For instance, the laboratory information system must satisfy the auditing requirements of hospital accreditation agencies, HIPAA, and other clinical medical practitioners. Ensuring that a robust audit trail is retained and archived is essential for capturing the precise sequence of events; this trail provides evidence that justifies and/or explains what actions have occurred. It is also vital to satisfy e-Discovery requests.

Attorneys and judges have been grappling with the terms metadata and audit trails as EHRs and, more generally, electronically stored information, have more frequently become the subject of discovery requests and legal motions. The Doctors Company, the nation's largest physician-owned medical malpractice insurer, published a study in October of 2017, highlighting




the rise of EHR-related malpractice suits. The study revealed that claims in which EHRs are a factor increased from just two between 2007 and 2009 to 161 from 2011 to December 2016. This is directly material to clinical data archival, as it is expected that the archival solution will have stored the same data as the legacy EHR it replaced.

# CONCLUSION

There are many legal considerations to evaluate when navigating the complex data structure and data sets, legal and compliance requirements, and continuity of care requirements that characterize effective healthcare legacy application retirement.

Given these considerations, Galen Healthcare Solutions designed a data archiving solution, VitalCenter Online Archival, that takes the most risk-averse approach to data preservation, retention and archival, but also does so in a cost-effective manner through a SaaS-native solution. VitalCenter Online Archival facilitates not only archival of the legal medical record, but also designated record sets, that is, data not directly related to patient care, including contextual audit trails, referenced data in ancillary systems, data change and version history, and infrequently used and invisible fields.

As a result, VitalCenter Online Archiving preserves records with high fidelity to limit liability, enabling rapid retrieval of records for both clinical continuity and legal scenarios and reduction of costs associated with maintaining legacy systems and data.

# ABOUT MATT FISHER

Matt is a partner, the chair of the Mirick O'Connell Health Law Group and a member of the firm's Business Group. Matt focuses his practice on healthcare regulatory and corporate matters.

Matt's health law practice is wide-ranging and includes advising clients with regulatory, privacy, security, fraud, abuse, and compliance issues. Matt advises clients to ensure that contracts, affiliation and coordination agreements, and other business arrangements meet both federal and state statutory and regulatory requirements. Matt's regulatory advice focuses on complying with the requirements of HIPAA, the Stark Law, Anti-Kickback Statute, fraud and abuse regulations, licensing requirements, the Medicare and Medicaid programs, and the Sunshine Act. Matt also advises clients on compliance policies to develop appropriate monitoring and oversight of operations.

Matt works with all types of providers within the healthcare system, including hospitals, physician groups, skilled nursing facilities, home health agencies and any other type of provider. Matt also advises health information technology companies from start-ups to mature companies.

Matt is a Council Member-at-Large of the American Bar Association's Health Law Section, co-chair of the Emerging Issues in Health Law Conference Planning Committee, chair of the Marketing Committee, and a vice-chair of the Programs Executive Committee. Matt is also actively involved with the Health Information Management Systems Society in North America and chairs the Advocacy Committee of the New England Chapter of HIMSS.

# ABOUT ROBERT DOWNEY

Robert is Vice President, Product Development, at Galen Healthcare Solutions. He has nearly 10 years of healthcare IT experience and over 20 years in Software Engineering. Robert is responsible for design and development of Galen's products and supporting technology, including the VitalCenter Online Archival solution. He is an expert in healthcare IT and software development, as well as cloud based solutions delivery. He is author of the "Healthcare Archival Strategy" whitepaper, has written about the difference between migrated and archived data, and has presented on topics including connected care, and health IT security.

Robert holds a B.S. in Information Technology from Rochester Institute of Technology.