I. ELECTRONIC RECORDS AND AUDIT TRAILS

In medical malpractice cases there are issues about what the doctors and nurses did to a patient at what time and why, including what they knew or should have known at the time. Traditionally, the cornerstone of these actions was the “chart". However, the electronic age is now well upon us. With electronic records there is an opportunity to more accurately track exactly what happens in a given patient encounter. But it must always be kept in mind that electronic health records are NOT medical records typewriters. Instead, they should be thought of as experimental medical devices which have the ability to affect patient care[1]. These medical devices, for which there is no uniformity and which have not suffered the benefit of clinical trials, bring with them many new issues which need to be kept in mind. Issues include data collection, compilation, manipulation and display. To complicate the matter, one must keep in mind that the use of this device is as a result of a contract with a commercial vendor, typically fraught with indemnity and nondisclosure clauses, as well as provisions for maintenance and remediation of problems with the system[2]. Moreover, these systems are often designed by “computer guys" without a clue as to what is really important in terms of taking care of a patient. Issues arise as to the use of templates, drop-down menus, and the habit of “drag and clicking” patient data to populate the electronic chart, oftentimes with volumes of meaningless data and print. Accordingly, there are issues as to portals, i.e., what data was actually available on a given computer screen, and what did the doctor or nurse have to do in order to pull it up. One should always question what the use of this experimental device did to cause or contribute to the patient's harm.[3]

In broad simple terms, electronic records are simply a compilation of data in a digital or other non-paper format. There are a number of categories of data that are collected, manipulated and stored in a healthcare setting. These include what are generally referred to as “medical records” and includes the “patient's chart”, “radiographic information”, “laboratory results”, and “monitoring records” and other data. Collectively, these data are known as the Electronic Health Record or

[1] Shuren testimony to HHS Health Information Technology H-IT Plicy Committee, http://healthIT.hhs.gov/portal/server.pt/gateway/PTARGS0116739107170018/3, Shuren Testimony 022510, pdf: see also HC renewal 109 http://herenewal.blogspot.com/2011/04/dfa-decides-regulating-implantable.html

[2] Health IT and Patient Safety. Building Safer Systems for Better Care, Institute of Medicine of the National Academies, 2012

[3] Chesanow, Neil, 8 Malpractice Dangers in Your EHR, www.medscape.com, August 26, 2014

"EHR". But in the healthcare setting, there are a lot of other pertinent data that are also collected in an electronic format. For example, many hospitals have security cameras in a variety of areas from hallways to the cafeteria to the garage. Likewise, many secure areas of hospitals, doctors' offices and parking garages are controlled by card key or other digital access of which an electronic record is maintained. Moreover, many personal encounters in a healthcare setting are electronic, rather than "in person". These include communications by cell phones, hospital phones, texting and other means of digital communication. To be sure, healthcare organizations, including hospitals and doctors' offices, are sophisticated users of electronic data. Information is collected, manipulated and maintained for many purposes ranging from keeping track of a patient's healthcare status to billing and the prevention of (or perpetration of) fraud.[4]

As can be expected, every time electronic data is generated, whether it be to enter a parking garage, take a patient history, perform a CT scan or record a change in a patient's condition, there is an electronic record of who input the data, when it was input, who accessed or reviewed the data, who manipulated or altered the data and when and from where such activities took place. The compilation of these entries into an electronic record is referred to as an audit trail.

In the context of litigation and discovery, technical but usable definitions are important. Keep in mind that with respect to the production of medical records, the request is not simply directed to the Medical Records Department, but also to the Information Technology Department. Dr. Scott Silverstein, M.D., a medical informatics expert, suggests the following definitions:

> "Electronic Health Record" (EHR) "EHR" refers to electronic information systems and/or computerized devices containing electronic records of patient data captured in any care delivery setting within [Hospital]. Records include but are not limited to patient demographics, histories and physicals, progress notes, clinician orders, lab tests, diagnostic imagines, graphical data such as EKG tracings, physiological data such as blood pressure, pulse, respiratory rate and temperature, automated decision support-generated alerts and reminders, and any other

[4] Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology, Department of Health and Human Services, Office of Inspector General, http://oig.hhs.gov, December 2013

> clinical data used in monitoring and providing medical care to a patient.
>
> "Metadata." Metadata, commonly described as "data about data," is an automatically generated computer record, including but not limited to audit trails, order and results "detail" sheets, and other data that certify how, when, where and by whom electronic documents (e-documents) and other computer-based information have been reviewed, manipulated or otherwise accessed.[5]

In healthcare liability claims, the metadata or audit trail is highly relevant evidence as to who accessed what in the record, what entries were made and/or changed, by whom and when. Frankly, the audit trail is an integral part of the medical record. It is the metadata about the medical record that cannot be separated from the record itself. And it will show important information about care provided in any given case. For example it will show when the various assessments of a patient occurred and were documented in a medical record. It is important to know if all of the critical assessments documented were entered into the chart from a remote location two days after the patient died or by someone who had never seen the patient.

II. DUTIES

The duty of a healthcare provider to create and maintain accurate records, including electronic health records and audit trails stems from a variety of sources. To be sure, pursuant to the Nurse Practice Act,[6] common law and most hospitals' policies and procedures, nurses have an obligation to accurately evaluate a patient, make a nursing diagnosis, create and evaluate a plan of care, and assess a patient's response to therapy or treatment and to document. But the duty to create and maintain accurate records, electronic or otherwise, stems from a number of other

[5] Silverstein, Scot M., M.D., A Primer on Healthcare IT Myths, Realities, Risks, and Practical Implications for Trial Lawyers. See also Atherton, Jim, M.D., Development of the Electronic Health Record, Virtual Mentor, March 2011, Vol. 13, No. 3, pgs 186-189. See also Electronic Health Records Overview, National Institutes of Health, National Center for Research Resources, April 2006

[6] Sec eg 217 Tex. Adm. Code §217.11(1)(D)

sources as well. For example, the Joint Commission has "IM standards"[7], and Medicare and Medicaid, together with the federal Conditions for Participation[8], have strict recordkeeping requirements. HIPAA and its progeny provide further requirements, including keeping timely and accurate records for purposes of patient care and establishing "medical necessity" and other information for billing and other purposes.[9] By the same token, an audit trail is not just an accidental byproduct of the electronic age. It is instead a heavily regulated necessity. For a variety of reasons, healthcare organizations must perform security audits using audit trails that offer a back end view of system use. The federal government and many other payors require an audit trail for billing and other purposes. Some of the obvious reasons for the necessity of an audit trail include:

- Authenticating a medical record for payment purposes;
- Establishing a culture of responsibility and accountability;
- Reducing the risk associated with inappropriate access;
- Providing forensic evidence during investigations of suspected known security incidents and breaches to private safety;
- Tracking disclosures of protected health information;
- Responding to patient privacy concerns regarding unauthorized access;
- Evaluating the overall effectiveness of the organization's appropriate access and use of patient information;
- Detecting new threats and intrusion attempts;
- Identifying potential problems;

[7] Sec eg 2014 HAS@IM standards
[8] Sec eg 42 CFR 482
[9] Sec eg Health Information Privacy, U.S. Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/index.html

- Addressing compliance with regulatory and accreditation requirements.[10]

Additionally, and obviously, such data is important in terms of trying to figure out what happened to a given patient and why.

III. REGULATORY REQUIREMENTS.

There are many regulatory requirements, providing how and why security audits are conducted and maintained. Most hospitals have healthcare information management professionals who are well aware of these requirements and are responsible for the institution's compliance. In addition to the Joint Commission standards, Conditions for Participation, policies and procedures and various state law requirements, HIPAA provides various security rules. For example the HIPAA security rule includes two provisions that require healthcare organizations to perform security audits:

> Section 164.308(a1)(I)(c) provides that information system activity must be reviewed. It states organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
>
> Section 164.132(1)(b) provides that audit controls are required. Organizations must "implement hardware, software and procedural mechanisms that record and examine activity and information systems that contain or use electronic protected health information."

As a part of the American Recovery and Reinvestment Act of 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act. (HITECH). This act also includes provisions that require organizations to maintain records and conduct audits. Essentially, healthcare organizations, as well as third-party payors, are expected to monitor electronic healthcare records for breaches of protected health information from both internal and external sources. Many federal regulations require that electronic records and audit trails be maintained. For example 40 5DCFR, parts 160 and 164 include a variety of rules providing that healthcare organizations must use reasonable due

[10] Privacy and Security Audits of Electronic Health Information, AHiMA, http://library.ahima.org/xpedio

diligence by actively auditing and monitoring for protected health information breaches. Additionally, institutions and their electronic medical records vendors must be able to demonstrate that the electronic systems meet the technical safeguards in the HIPAA security rule, including audit requirements, to be able to become certified. Stage one of the certification criteria for meaningful use includes requirements for audit controls. Section 170.302(r) requires:

> – Record actions. Record actions related to electronic health information in accordance with the standards specified in section 170.210(b).
>
> – Generate audit log. Enable a user to generate an audit log for specific time period and to sort entries in the audit log according to any of the elements specified in the standard at section 170.210(b).

As indicated, a metadata or an audit trail is a mandatory log containing the identity of every individual accessing a medical record, the time and date of the record accessed, identification of the records accessed, the portion of the records accessed and any modifications to the records made. 20 1CFR part 11.

Stage II of the certification criteria for meaningful use includes section 170.314(b).

> (3) audit reports. This section requires the ability to enable a user to create an audit report for a specific time period and to sort entries in the Autoblog according to each of the data specified in the standards at section 170.210(e).

Additionally, in June 2012, the Office for Civil Rights released criteria that its auditors used to validate a healthcare organization's compliance with the HIPAA requirements.[11]

The Department of Health and Human Services HIPAA audit program protocols are available and presumably followed by all healthcare organizations.[12]

[11] Privacy and Security Audits of Electronic Health Information, AHiMA, http://library.ahima.org/xpedio. See also Dept. of Health and Human Services, HIPAA Audit Protocol, http://hss.gov/ocr/privacy/hipaa/enforcementprotocol.html.

[12] Id.

To be sure, there are numerous and wide ranging regulations concerning the creation and maintenance of electronic medical records. On the other hand, when the health information software is thought of as an experimental medical device, it is hardly regulated at all, and this is dangerous. For example according to the FDA's chair of the Center for Devices and Radiological Health, Jeffrey Shurer, M.D., J.D., "under the federal food drug and cosmetics act, health information technology software is a medical device."[13] He also stated that "to date, FDA has largely refrained from enforcing our regulatory requirements with respect to health information technology devices."[14] Frankly, these experimental devices are used on and affect patients largely without the benefit of the basic ethical considerations for such experimentation. See for example:

- 45 CFR 46 – Protection of Human Subjects;
- Guidelines for Conduct of Research Involving Human Subjects at NIH (Gray Booklet);
- The Belmont Report – Ethical Principles and Guidelines for the Protection of Human Subjects of Research;
- World Medical Association Declaration of Helsinki;
- Nuremberg Code – Directives For Human Experimentation[15]

Make no mistake: this is a real potential problem for a given patient who happens to find himself in a hospital or, for that matter, in a doctors' office.

The use of unregulated and experimental information technology in the healthcare setting brings with it a number of new and unique challenges. For example, the ECRI Institute recently published Health Devices, Top 10 Health Technology Hazards for 2010[16]. These included hazards specifically related to information technology, namely alarm hazards and data loss, system incompatibilities, and other health IT complications. The Joint Commission has included electronic technologies as a safety issue and one of its Sentinel Event

[13] Supra footnote 1, IM.02.01, and IM.02.01.03

[14] Id.

[15] See eg Silverstein, Scot M., M.D., A Primer on Healthcare IT Myths, Realities, Risks, and Practical Implications for Trial Lawyers

[16] Health Devices; Top 10 Health Technology Hazards for 2011. ECRI Institute, Vol. 39, Issue 11, pp. 386 – 398, November 2010

Alerts[17]. The alert provides in part:

> Inadequate technology planning can result in poor product selection, a solution that does not adapt well to the local clinical environment, or insufficient testing or training. Inadequacies include failing to include front – line clinicians in the planning process, to consider best practices, to consider the costs and resources needed for ongoing maintenance, or to consult product safety reviews or alerts or previous experience of others. Implementing new clinical information systems can expose latent problems or flawed processes with existing manual systems; these problems should be identified and resolved before implementing the new system. And over – reliance on vendor advice, without the oversight of an objective third party (whether internal or external), also can lead to problems.

Indeed, the Department of health and human services has even categorized health information technology safety issues:[18]

H-IT Safety Issues-General Categories

Category	**Description**
Errors of Commission (EOC)	Events such as accessing the wrong patient's record or overwriting one patient's information with another's .
Errors of Omission or Transmission (EOT)	Events such as the loss or corruption of vital patient data
Errors in Data Analysis (EDA)	Includes medication dosing errors of several orders of magnitude
Incompatibility between Multi-Vendor Software Applications or Systems (ISMA)	Incompatibilities which can lead to any of the above.

Recently, the Institute of Medicine of the National Academies weighed in

[17] "Safety implementing health information and converging technologies", The Joint Commission Sentinel Event Alert, Issue 42, December 11, 2008

[18] Memo: H-IT Safety Issues, Department of Health & Human Services, February 23, 2010

on the problems. In 2012, the Institute of Medicine published Health IT and Patient Safety, Building Safer Systems for Better Care. Salient points from their study include:

- While some studies suggest improvements in patient safety can be made, others have found no effect. Instances of health IT-associated harm have been reported. However, little published evidence could be found quantifying the magnitude of the risk.
- Several reasons health IT-related safety data are lacking include the absence of measures and a central repository (or linkages among decentralized repositories).
- Another impediment to gathering safety data is contractual barriers (e.g., nondisclosure, confidentiality clauses).
- Some vendors include language in their sales contracts and escape responsibility for errors or defects in their software (i.e., "**hold harmless clauses**").
- Contractual restrictions limit transparency, which significantly contributes to the gaps in knowledge of health IT-related patient safety risks. These barriers to generating evidence pose unacceptable risks to safety.[19]

When these problems are identified, the solution often falls solely to the remediation or repair clause in information technology vendor contracts. Healthcare information technology vendors often enjoy a contractual and legal arrangement to attempt to make themselves liability free and held harmless. These contractual provisions often shift the liability and remedial burden of defective systems to physicians, nurses, hospitals, and clinics, even when these practitioners are strictly following vendor instructions[20]. One must question whether hospital executives signing such contracts are violating Joint Commission Standards, as well as their fiduciary obligations to patients.

IV.RECORDS COMPONENTS.

With the numerous issues that surround information technology, one must keep in mind that electronic healthcare records contain a number of key

[19] Health IT and Patient Safety. Building Safer Systems for Better Care, Institute of Medicine of the National Academies, 2012

components. Most electronic health records are designed to include and combine data from large ancillary services, such as pharmacy, laboratory, radiology, and clinical care (including nursing care plans, medication administration and physician orders). Most commercial electronic health records have at least the following components

– Administrative system components,

– Laboratory system components,

– Radiology system components,

– Pharmacy system components,

– Computerized physician order entry components,

– Clinical documentation components.[21]

Medical devices can also be integrated into the flow of clinical information. These various components do not always play well together. Integration is often a problem, one that can lead directly to patient harm.[22]

V. DISCOVERY:

A. AUDIT TRAIL PRODUCTION The production of the metadata or audit trail is certainly not burdensome. Indeed, healthcare organizations have sophisticated information technology personnel whose job it is to provide such data. It is important to keep in mind that various personnel have different levels of security access to the electronic data. Accordingly, when

[20] Sec eg Chesanow, Neil, 8 Malpractice Dangers in Your EHR, www.medscape.com, August 26, 2014
[21] Electronic Health Records Overview, National Institutes of Health, National Center for Research Resources, April 2006
[22] Health Care Renewal – FDA on Health IT risk: reckless, or another GM-like political coverup? http://hcrenewal.blogspot.com/2014/04/fda-on-health-it-risk-reckless-or.html; Integrity of the Healthcare Record: Best Practices for EHR Documentation, AHiMA

requesting production of an audit trail, be sure that the persons generating the metadata have sufficient security clearance to access the entire electronic record. Moreover, the data you receive will be entirely dependent on what query the IT personnel makes to generate it.

It is important to keep in mind that hospitals are commercial enterprises in many respects, not unlike banks, insurance companies and other organizations that maintain electronic records. The records system is provided by a commercial vendor. Accordingly, there will be typically a detailed contract between the two entities involved. Usually the contract will provide for maintenance and changes to the electronic record-keeping system. Typically the vendors will have a number of documents that they provide to the hospital. Accordingly, in addition to the hospital's own policies and procedures, there usually will exist an owners' manual, a user's guide, recommended electronic recordkeeping policies and procedures and often education materials regarding the use of the electronic record, inasmuch as audit trails are a federally mandated requirement.[23] These materials from the vendor will provide useful information about not only how to enter comments and manipulate and store data in the healthcare record, but also how to provide an audit trail. These manuals will also provide the toll-free number to the customer service representative as well as to technical support. Oftentimes, the vendor is able to easily provide the audit trail from their location, thousands of miles away.

B. OTHER DISCOVERY CONSIDERATIONS:

When drafting discovery requests to a hospital for specific healthcare records, in addition to requesting the complete chart and the metadata or audit trail, you must tailor the discovery to your case. Dr. Silverstein, suggests the following template, for example, with respect to metadata:[24]

[23] See generally Privacy and Security Audits of Electronic Health Information, AHiMA, http://library.ahima.org/xpedio

[24] Silverstein, Scot M., M.D., A Primer on Healthcare IT Myths, Realities, Risks, and Practical Implications for Trial Lawyers

1. For the pre-operative to return-to-ICU time period [X-Y] for Plaintiff: identify the vendor and specific EHR application(s), including LIS (lab information systems), PACS, CPOE (computerized order entry systems), computerized anesthesiology or operating room systems and apparatuses, computerized medication dispensing machines, etc. that clinicians who cared for Plaintiff used or interacted with for treatment, data entry, and data review, and that stored clinical data and/or metadata.

By way of example, "PICIS Pulsecheck ED EHR", "Cerner Millennium Powerchart EHR", "Stentor iSite PACS", and "Pyxis MedStation computerized medication dispensing cabinet" illustrate the form of responses sought**. (Note – IT technical/executive personnel and/or the CMIO(S) have this information.)**

(a) Indicate names and addresses of all persons who have knowledge of, and will testify to same.

2. State the retention policies, procedures, and schedules in effect regarding the complete medical record in effect during Plaintiff's stay at [Hospital].

3. Besides medical data that is part of the complete medical record produced per request of DD/MM/YYYY, identify the **metadata** that exists in all EHRs or computer-based medical devices identified in interrogatory #1, from the time of Plaintiff's pre-op preparations on DD/MM/YYYY up to and including his return to the ICU. This specifically includes but is not limited to computer-based medication orders, orders for therapy, instrumentation and interventions, and physiologic data such as BP, pulse, temperature, etc. automatically measured or otherwise obtained.

4. Produce the metadata identified in response to interrogatory #3, including but not limited to all orders and results "detail sheets", problem lists, problem histories, alerts and reminders, and other metadata for the time period specified, in the form of charts, tables…

- May want to ask for **chronological, monolithic sorting**, or for data in an Excel format – recent report sorted alphabetically by "events", in multiple seemingly random event sets.

The metadata should include date and time of EHR access, EHR section/tab/function accessed, user name performing the access, user position/role, computer workstation name or other identification, action(s) performed, and any other metadata stored by [Hospital's] EHRs.

5. Indicate if any changes/upgrades that have occurred in [Hospital's] EHRs since Plaintiff's surgical or post-surgical period that could affect or change the clinical data or metadata as reproduced in response to these requests in any way.

As a final note, keep in mind some of the following considerations:

You should also consider the possibility of the electronic health record causing or contributing to malpractice and harm to the patient. You need to discover all of the information systems that in any way “touched" the patient's care throughout a hospitalization. Additionally, you need to consider potential corporate negligence issues with respect to the use of an electronic system, the remediation of problems, as well as the policies and procedures that govern the use of such systems. You should consider, for example, who the information technology people are, as well as what are their qualifications to be involved in clinical affairs. Always be aware of the potential for evidence spoliation and who could be involved. This includes not only clinical practitioners, but also the information technology staff and others who have access to the electronic data.[25]

[25] See generally Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology, Department of Health and Human Services, Office of Inspector General, http://oig.hhs.gov, December 2013