Malpractice Cases
EHRs and Audit Trails

Summary: This is Part 1 of a 2-part article relating to Electronic Health Records and corresponding EHR audit trails. In today's healthcare environment, the EHR audit trail is the source of all clinical activity tracking. Basically, the rule is: If it's not documented, it never happened. Additionally, it is important to know if clinical data has been modified, who modified the data, when the data was modified, and what was modified. Same with the initial entry of clinical data. The audit trail will indicate when the data was entered and by whom. In legal cases, it is especially important to know when the data was entered – was the data entered within 15 minutes of the clinical event or 4 hours later. In some cases, it is important to know where the person was located when they enter the clinical data. Knowing what question to ask during the Discovery period is imperative.

Electronic Health Records:

Electronic medical records (EMR) electronic health records (EHR) (hereinafter EHR) have largely replaced paper medical records since the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. Previously, when alterations were made to a medical paper record, the same health care provider that made the original entry would cross out the altered entry with a single line, add a correction, and initial the change with the date and time of the alteration. The change made was generally legible. Both the initials and handwriting aided a reviewer in identifying the individual. Some alterations were "late entries" where a health care provider would document an entry into the record as a "late entry," identifying the date and time of the entry, the identification of the individual making the entry, and that the entry was made after the fact. Generally, alterations that were made to a patient's medical record were made where the medical chart was kept during the course of care.

Thus, with a paper record, the identification of who accessed the record, where that access took place, the date and time the record was accessed, and what information was altered remained transparent and preserved for any subsequent users or reviewers of that record. Importantly, this method also discouraged unauthorized alterations to the medical record. The authenticity, completeness, reliability, and admissibility of the medical record were preserved for the health care providers, the patient, and any subsequent reviewer. These types of alterations to the record were integral to the record's usefulness as a business record and made with the intent to aid the users and/or reviewers of the record in understanding the medical care provided and clinical decisions that were made during the course of care. In the context of a lawsuit or other investigation, these alterations were not redacted from the paper record prior to production. In fact, these types of authorized and transparent alterations were considered a testament to the medical record's accuracy, freedom from unauthorized alterations, and completeness.

Enter the age of EHR. Now, health care providers often take the position that EHRs have a "legal electronic health record" definition whereby the provider decides internally what information constitutes the official business record for evidentiary purposes. This definition often does not include the critical information about alterations to the medical record that had previously been preserved on the paper medical record. Unlike paper records, detection of any alterations by a simple inspection of printouts of electronic records is impossible. It is not that this information is no longer available in the context of EHR. Rather, health care providers exploit an EHR system's ability to filter out documentation of who made alterations, what was altered, and where and when these alterations to the medical record occurred, effectively compromising everyone else's ability to authenticate the record or fully understand the clinical events that transpired.

Further, alterations to a medical chart can now occur at any time and from various user-EHR interfaces (computer terminal in the emergency department; nurse's station on an obstetrical floor; tablet in a doctor's office. EHR users may or may not have taken part in the medical care documented in the record; and these users may not be medical professionals at all (billing personnel; medical records personnel). An EHR user is anyone with system access and designated EHR rights. These issues now make the EHR vulnerable to access and alterations that misrepresent or change the documentation of the medical

care provided and jeopardize both the actual provision of medical care; and the admissibility of the medical record as a business record that accurately reflects the course of care at issue.

The HIPAA security rule includes two provisions that require organizations to perform security audits. They are:

- Section 164.308(a)(1)(ii)(c), Information system activity review (required), which 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 164.312(1)(b), Audit controls (required), which states organizations must "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

EHR Audit logs:

Starting in 2005, the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) required all healthcare organizations to “implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” Electronic health record (EHR) access and audit logs record behaviors of providers as they navigate the EHR. These data can be used to better understand provider responses to EHR-based clinical decision support (CDS), shedding light on whether and why CDS are effective.

The second stage of the Meaningful Use regulations, released in 2014, further clarified that certified EHRs must maintain audit logs adhering to the ASTM E2147 standard for tracking health information technology (HIT) use. Due to these regulations, virtually all EHRs in the United States (including eClinicalWorks) now track at least 4 pieces of information about every episode of patient record access including who accessed which patient record at what time and the action they performed in that record such as adding, deleting, or copying information (Table 1). Depending on the vendor, EHR audit logs may track additional information about the computer, user, or record involved in each action, track those actions at different levels of granularity, and give them different names.

Table 1. Example EHR audit log

TIME	USER	RECORD	ACTION	Section	Workstation
05/12/2019 13: 04: 35	SMITHJANE	104738297	Edit	Note Section	MED2938
05/12/2019 13: 04: 37	SMITHJANE	104738297	Pend	Note	MED2938
05/12/2019 13: 04: 42	SMITHJANE	104738297	Sign	Note	MED2938
05/12/2019 13: 04: 52	DOEJOHN	105837489	View	Problem List	MED1238
05/12/2019 13: 05: 02	DOEJOHN	105837489	View	Note	MED1238
05/12/2019 13: 05: 04	DOEJOHN	105837489	View	Note	MED1238
05/12/2019 13: 05: 32	SMITHJANE	107483726	View	Patient Summary	MED2938
05/12/2019 13: 13: 32	SMITHJANE	107483726	View	Patient Summary	MED2938

The Audit Log of actions related to Electronic Health Information (EPHI) that supports the forensic reconstruction of the sequence of changes to a patient’s chart was required for all EHRs certified to qualify for the Medicare and Medicaid

Electronic Health Records (EHR) Incentive Programs. The Stage 1 of certification criteria for meaningful use, Section 170.302 ®, Audit log, requires entities to record actions related to electronic health information and generate an audit log1. The EHR system audit log should always be operational, should be stored as long as clinical records, and should never be altered.

Further under the certification criterion at § 170.315(d)(10) may be required as part of the 2015 Edition privacy and security approach for the certification criteria at § 170.315(g)(7), (g)(9), and (g)(10). A developer may choose to demonstrate either § 170.315(d)(2) or § 170.315(d)(10) as part of the 2015 Edition privacy & security approach for § 170.315(g)(7), (g)(8), and (g)(9). If the developer chooses to demonstrate § 170.315(d)(10) for § 170.315(g)(7), (g)(9), and/or (g)(10), this criterion at § 170.315(d)(10) only needs to be demonstrated once as part of the overall scope of the certificate sought.

According to the 2015 Edition §170.315(d)(3) Audit Report(s) Testing Components: Health IT developer self-declaration to the testing outcomes Test Procedure Version 1.3 – Last Updated 09/21/17 Please consult the Final Rule entitled: 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications for a detailed description of the certification criterion with which these testing steps are associated. We also encourage developers to consult the Certification Companion Guide in tandem with the test procedure as they provide clarifications that may be useful for product development and testing. Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place. The Required Tests include::

§170.315(d)(3) Audit report(s). Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in §170.210(e) by Recording actions related to electronic health information, audit log status, and encryption of end-user devices.

- The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standards specified at § 170.210(h) and changes to user privileges when EHR technology is in use.
- The date and time must be recorded in accordance with the standard specified at § 170.210(g). (2)(i) The audit log must record the information specified in sections 7.2 and 7.4 of the standards specified at § 170.210(h) when the audit log status is changed.
- The date and time each action occurs in accordance with the standard specified at § 170.210(g).
- The audit log must record the information specified in sections 7.2 and 7.4 of the standards specified at § 170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at § 170.210(g).

The 2015 ONC Cures Act Final Rule included the requirement for Health IT Modules to support 7.1.3 Duration of Access in the ASTM E2147-18 standard. The ONC Cures Act Final Rule included the requirement for Health IT Modules to support an updates to audit logging and has incorporated by reference the standards, as amended effective June 30 2020, § 170.299(1) ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1 2018, IBR approved for § 170.210(h).

Regarding the granularity of the information, this should be consistent with the guidance in Section 7.1.9 of ASTM E2147-18, which states the "granularity should be specific enough to clearly determine if data designated by federal or state law as requiring special confidentiality protection has been accessed." And more to the point, Section 7.1.9 goes on to state that "[s]pecific category of data content, such as demographics, pharmacy data, test results, and transcribed notes type, should be identified." For example, the ability of the audit log to record that the user accessed a patient's medication list would be sufficient for certification, and the audit log would not need to also record the specific medication. [see also 77 FR 54234]

The certification criterion requires actions initiated by the user from within the health IT interface to be tracked in the audit log. The copy and paste functions of Microsoft Windows originate outside of the health IT environment and are thus outside the scope of

certification. Copy actions originating from within the health IT interface (e.g., exporting or downloading a copy of electronic health information from the health IT) are required to be tracked in the audit log.

Information related to the required actions (e.g., additions, deletions, changes, queries, print, and copy) must be recorded in the audit log, however the certification criterion is not prescriptive to the method by which this is achieved and does not place limitations on the format in which this information is presented in the audit log. Developers may design systems to place content in the audit log as long as the audit logs can be used to identify the information before and after change. A "pointer to original data state" is a means of identifying original information that has been changed by a user. Similarly, a "pointer to deleted information" is a means of identifying information prior to deletion. A description of a change or deletion is acceptable as long as the type of action is specified, and both the original and modified data states are able to be identified. For example, an audit log could include a link to an original document and provide a description of the modified state. Conversely, it could include a description of the original data state and provide a link to the modified document.

Audit logs may not, however, save the actual content of the record that was changed, i.e., what the record said before and after the change. Thus, a *revision history* is needed to evaluate changes made over time (comparable to the Microsoft Word “track changes” feature). In other words, it is a chronological listing of document versions or data versions showing the changes over time. Without a duty to disclose the audit logs and the revision history, an EHR can be altered with impunity. Timelines can be changed, information can be altered or deleted, or “new” information entered. Importantly, these changes may or may not reflect falsification of a medical record; these changes may reflect the actual care, but it is impossible to know without an audit log and revision history to authenticate the changes.

In sum, when an attorney wants an expert to look at clinical data, the attorney should request a complete audit log and a medical record with revision history. The applicable statutes, regulations and/or the Practice Book should be modified in this regard and brought to the age of the EHR Audit Trail. Stage 1 (2011) of certification criteria for meaningful use requires healthcare entities to:

1. Record actions related to electronic health information in accordance with the standard specified in §170.210(a to h). Specifically, the regulations state:

Section (e) ***Record actions related to electronic health information, audit log status, and encryption of end-user devices.***

(1) EHR Access

(i) The audit log must record the information specified in sections 7.1.1 and 7.1.2 and 7.1.6 through 7.1.9 of the standard specified in § 170.210(h) and changes to user privileges when health IT is in use.

(ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).

(2) EHR changes/Modifications

(i) The audit log must record the information specified in sections 7.1.1 and 7.1.7 of the standard specified at § 170.210(h) when the audit log status is changed.

(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g).

(3) Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at §170.210(e)

- The audit trail displays every time a person logged into and accessed the EHR, which patient chart they accessed, the date and time and what workstation they were using, and what part of the EHR program they accessed. Each EHR has a standard Audit Trail output format that can be sorted by:

    1. Patient ID or name
    2. Staff person Name and ID number

3. Date and time of activity
4. Workstation ID
5. Event (add, changed, print, viewed, deleted)

Technically, every electronic health record system after 2009 should have an audit log detailing entry, views, and the associated users. Within a visit/encounter/progress note, that most resembles a paper chart, that log is usually quite robust. Every Electronic Health Record (EHR), which was mandated in 2009 by the federal government, is required to have an electronic Audit trail that shows every ***Add, View, Delete, Print, and Change*** that was made within the EHR.

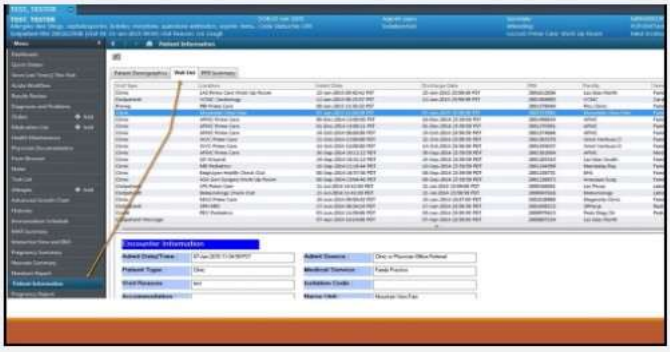
Hospitals and physicians started installing EHRs in 2000 and 95% were completed by 2015. Prior to 2009, only 17% of healthcare organizations had installed an EHR. Therefore, between 2009 and 2015, the majority of the healthcare organizations (98% of hospitals and 87% of Physicians) had installed and implemented an EHR and therefore, they should be able to provide an electronic copy of the patient's chart and a thorough electronic audit trail.

Health IT developers that participate in the ONC Health IT Certification Program are subject to Condition and Maintenance of Certification requirements as part of the 2015 Edition Cures Update. Included in these requirements is the Assurances Maintenance of Certification which requires Certified Health IT that electronically stores Electronic Health Information (EHI) to certify to the Cures Update § 170.315(b)(10) EHI Export criterion. Health IT developers certifying this criterion must provide their customers with the capability to efficiently export single and multi-patient EHI in a secure and timely manner. The Direct Review process promotes accountability, ensuring Certified Health IT conforms to Certification Program requirements when it is implemented and used in real world settings.

Electronic Health Information (EHI) refers to "electronic protected health information" (ePHI) to the extent that it would be included in a designated record set as defined in 45 CFR 164.501. EHI does not include psychotherapy notes as defined in 45 CFR 164.501 or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. The EHI definition represents the same ePHI that an individual would have the right to access under the HIPAA Privacy Rule.

What we need to know:

1. When looking for an Audit Log/Trail, we usually look to the EHR Audit Log for clinical entries, adding, viewing, and printing and we look for the Registration Audit log for demographics information enter by clerical staff before the patient is admitted to the clinical floor or Emergency Room and last for the Billing Audit Log if we are looking for billing related data.



2. The EHR audit trail will not have billing data or registration data audit trails unless someone changed the data after registration. When entered by the clerical staff, the registration and insurance information is passed along to the EHR software through an interface. Therefore, registration or insurance data date of entry or who entered the data will not be in the EHR audit trail. The EHR audit Trail starts when the nurses and the physicians start recording the patient's clinical data, and that cannot start until after the patient is registered.

3. There could be multiple EHR products used within one healthcare organization. We will need the audit trail from every clinical documentation software application. Sometimes there is only one EHR audit trail for the entire healthcare system. Other times there may be one major EHR software application and a few separate departmental EHR applications:

    a. The Registration Audit Trail if the question is related to Demographics or Insurance Information
    b. The Billing Audit Trail if the questions are related to billing and payments.
    c. The EHR Audit Trail for the Nursing Floors and physician interactions
    d. The EHR Audit Trail for the Emergency Room
    e. Usually, there is a separate EHR software in Surgery.
    f. If the patient goes to Rehab or Home Health, there is a separate EHR software.

g. Many times, we need to look at the Lab Information System (LIS) or the Radiology Information System (RIS) audit trail if we want to know who performed the test and when the test was completed. The EHR audit trail will indicate when someone viewed the lab results or the radiology report, but not when the result was available. For example, the results were available in the patient's chart at 10:00 AM CT but the provider did not view the results until 6:00 PM CT, 8 hours later.

h. Many times, there may be questions regarding a dictated report like a surgical report, discharge summary or consult note. Since those documents are generally dictated outside of the EHR and transcribed by a third party it may be important to know what the provider actually dictated initially. What shows up in the EHR is the final version after any documented changes, known as the revision history. However, the original version is not maintained in the EHR until the document is saved. If the documented is "pended" the changes are not saved until the provider signed the document.

i. We have also seen that if a document or an order is not signed off by the provider, the document will not be saved and stored in the EHR. A provider could provide clinical findings but we c an not see the findings because the provider did not sign off on the findings. We know that when producing the EHR, administration can exclude any action if the action was not signed off by the provider by simply clicking a box when producing the EHR. When that occurs, any action by the provider for the entire patient encounter will not be produced.

j. Also, remember that all phone conversions and text messages are not part of the EHR or the Audit trail. We have often asked for internal and external phone records if any issues were identified when a phone was used. Typically, hospital policies state that the phone call or the text message should be documented in the EHR, but if the call or text is not regarding a clinical result, most providers do not document the call/text. So, if we are looking at when a provider/nurse notify someone of an event, we might need to look at the Phone/text audit trails.

k. And many times, there is a different EHR software application(s) that tracks all clinical encounters when the patient is in the Physician Office and/or an Ambulatory Surgery Center (ASC).

4. All of these healthcare organizational departments, in theory, could have different EHR products from different companies. Therefore, when requesting access to a healthcare organization's EHR and audit Trail, we must first determine what software products are used in what departments. If you just ask for access to the EHR record and audit trail, the defendant's lawyers will state "The Request as phrased is vague, overly broad and unreasonably burdensome."

5. When asking for the EHR audit log or Trail, typically the Information Technology (IT) department is the only department that knows how to produce the standard EHR audit trail that has been in all EHR since 2009. Typically, the Health Information Management Department (aka Medical Records Department) will not have the authority or even knowledge on how to run the EHR Audit trail.

6. EHR product Company Name, Product Name, and software Version during the time of care by department.

7. I would ask to receive the audit Trails in an electronic searchable version (MS-Excel) so that we can search for and re-sort the information. If they will only give you the audit trail in PDF version, then I prefer to have the audit trail in Date and Time order by patient ID or patient name for the entire patient stay to include all views, additions, changes, deletions and if anything was printed.

8. In some cases, the EHR vendor might provide a "revision History" EHR record and audit log showing all changes to the EHR over time.

9. Additionally, some of the EHRs can also provide a "Detailed Audit Report." The detailed audit report shows the same information as above plus it shows what actual specific "data" was added, changed, or deleted. This is important if we want to see what actual data was inputted or changed down to the date and second.

Patient Medical Record:

1. When asking for the Patient's Medical Records always ask for the Final Legal Record, also know as the "EHR Revision History" version if the hospital is using EPIC Healthcare EHR. It is important to not only know what data was entered for a patient but also any time the data was changed/modified or updated, who updated the information, when they updated the information, and why they updated the information.

    a. Many times, a nurse might change information in the EHR hours or even days later, but they do not indicate why the patient's data was changed. At all times, there must be a reason for changing data in a patient's EHR and if we do not know why the data was changed, this only creates issues and liabilities.

b. In some cases, data is entered into the Patient's EHR late, maybe 30 minutes to 4 hours late. This can occur especially in the Emergency Room or critical care nursing units where the life of the patient appears more important than entering data into the computer. Operationally, all patient data should be entered into the EHR prior to the shift ending or as soon as possible after the event occurred. The person entering the late information should also record why the patient data was entered late. The question that arises in legal cases is memory. How does the person who is entering the information late remember exactly what happened or what clinical numerical value was present 30 minutes to 4 hours after the event?

c. If the information was written down on a piece of paper, then the paper is part of the legal record and should be scanned into the EHR under the documents folder. If the late information was not recorded anywhere, how does the person entering the late information prove that they entered the correct information?

2. Typically, electronic and scanning documents are in reverse chronological order. The terms medical record, health record, and medical chart are used somewhat interchangeably to describe the systematic documentation of a single patient's medical history and care across time within one particular health care provider's authority.

3. The medical record includes a variety of types of "notes" entered over time by health care professionals, recording observations and administration of drugs and therapies, orders for the administration of drugs and therapies, test results, x-rays, reports, History and Physical report, physician orders, nursing notes, lab, radiology and other procedure notes, Medication Administrative Report (MAR), daily and hourly Vital signs, operative reports, discharge summary, daily physician notes, etc.

4. The maintenance of complete and accurate medical records is a requirement of health care providers and is generally enforced as a licensing or certification prerequisite.

Text Messages:

Today, many hospitals allow staff to text and to text physicians. This is a form of clinical documentation that must be maintained if the information pertains to a specific patient where PHI is included in the text message. Testing is a form of documentation and thus must be maintained and should be stored within the EHR.

However, if you ask for a copy of the Medical Record and the audit log, typically you will not receive any information regarding texting since it is not normally considered part of the EHR. However, it is considered part of the patient's legal medical record. Just like a "Fax," all faxes should be scan in as a document and stored under the EHR document folder(s). Since Faxes are usually scan and are part of the Legal Medical Record, all text messages should fall under the same category. But to be clear, faxes and text messages are traditionally not considered part of the hospital's EHR but as a component of a document imaging/scanning solution that is interfaced or integrated with the Hospital's EHR software. In many cases, the Release of Information (ROI) department will conclude that faxes, scanned documents as well as text messages are not part of the patient's EHR but traditionally considered these types of patient data to be part of the Legal Record. Therefore, when requesting a patient's medical records, do not ask for the EHR record because they is considered only the data that was entered into the specific EHR software, and might not be consider including data outside of the EHR like scanned documents, Faxes, text messages, electronic vital signs capture by other devices, radiology exam images and in some cases, data from primary care physicians or specialist prior to the patient's admission into the hospital.

End-of-shift Nursing Report - Emergency Room and Nursing Floor:

1. A proper end-of-shift report is a compilation of details recorded by a patient's nurse.

2. Written or printed from the EHR by nurses who are wrapping up their shifts and provided to those nurses beginning the next shift, these details include a patient's current medical status, along with his or her medical history, individual medication needs, allergies, a record of the patient's pain levels and a pain management plan, as well as any discharge instructions.

3. Without these details, a nurse could potentially endanger a patient's life.

4. The different needs of individual patients are best met when the nursing staff understands their current medical situation. An end-of-shift report allows nurses to understand where their patients stand in regard to recovery by providing a picture of a patient's improvement or decline over the last several hours.

5. By knowing what has previously occurred in a patient's treatment plan, nurses can proceed with the right steps to contribute to positive outcomes.

6. Typically, the end of shift report is not stored in the patient's chart because the report typically has multiple patients on the report since the typical nurse has 3-5 patients during their shift.

7. Nursing is required to maintain the Nursing end-of-shift reports, typically on the nursing unit, or stored in Nursing Administration if any notes are charted on the report. Basically, because it includes patient data, and documents must be saved if any information is written on the report. Now, if the report comes from the EHR and nothing is noted on the report, the report might not be saved since we can reproduce the report from the EHR at any time.

Author: Mark R. Anderson has been a healthcare executive over the past 50 years and has worked for or consulted for over 350 hospitals and with over 26,000 physicians on healthcare policy and procedures; Clinical, Operational, and financial concerns; finance, billing, and collections; staffing based on acuity levels; as well as all aspects of technology. Since the late 1990's Mr. Anderson has been involved with Clinical Information Systems and later with Electronic Medical/Health record systems (EHR) and has assisted numerous law firms with their Malpractice cases where they need an expert to evaluate the federal mandated EHR audit logs and compare those audit logs to the actual legally binding EHR patient medical records. Mr. Anderson is a life fellow with HIMSS and is a Certified professional in Healthcare information systems (CPHIMS).