

# EHRs and Audit Trail Discovery Requests

## A. Overview:

1. EHRs (computerized electronic medical record systems) have largely replaced handwritten paper records in hospitals. Medical records produced from EHRs are not inherently trustworthy as complete and accurate depictions of clinical events. Because of significant risks of medical information manipulation in computerized hospital environments, especially after a bad outcome or initiation of litigation, printouts from EHR systems are untrustworthy unless proper safeguards are in place such that absence of tampering, previously seen via inspection of handwritten paper but invisible on electronic media (such as disk), can be proven.
2. In recognition of the vulnerability of electronic medical records to tampering, increasingly detailed regulations were passed by the U.S. Department of Health and Human Services (HHS) over the years to provide safeguards that permitted tampering to be detected. These safeguards included automatically recorded audit trails, with original content preserved if changes were made.
3. Those regulations include:
  - i. 1997 - 21 CFR Part 11 “Electronic records, electronic signatures”, Subpart B—Electronic Records 2003 - 45 CFR Part 164 Subpart C “Security Standards for the Protection of Electronic Protected Health Information”,
  - ii. 45 CFR §164.306 “Security standards: General rules”, 45 CFR §164.308 “Administrative safeguards”, 45 CFR § 164.312 “Technical safeguards”
  - iii. 2010 - 45 CFR Part 170 “Standards for health information technology to protect electronic health information created, maintained, and exchanged”, 45 CFR §170.210 “Standards for health information technology to protect electronic health information created, maintained, and exchanged”.
  - iv. 2012, 2015 and 2020 revisions to 45 CFR §170.210 (e) and (h) that specified ASTM E2147 as a national audit trail standard.
4. Further, CMS Pub 100-08 Medicare Program Integrity rules Ch. 3: Sec. 3.3.2.5 – “**Amendments, Corrections and Delayed** Entries in Medical Documentation” of 2013 and later versions called for any amendment, correction or delayed entry to be clearly identified, and original content to be shown, for both paper and electronic records.
5. The ASTM E2147 standard called for EHR audit trails to include Date and time of event. Patient identification, user identification. type of user action (such as **additions, deletions, changes**, queries, print, copy), original content if changes or deletions made, and identification of the patient data that was accessed.
6. Per the ASTM E2147 audit trail standard, audit data in audit trails is integral to authentication and trustworthiness of patient information in medical records. Authentication is a process of confirmation that a record is what it purports to be, an accurate depiction of a patient’s medical care and data; the act of establishing a record, or other document, as genuine, trustworthy and official; the provision of such assurance of the record’s authenticity is possible only because of the audit log and data associated therewith.

## EHRs and Audit Trail Discovery Requests

7. Authentication of the electronic medical record is possible only when the associated audit data relating to the record is made an indispensable part of the medical record and provided along with the records themselves for review. Authentication requires comparing the records and audit trails for discrepancies or lack thereof, **along with note modifications, deletions and original content.**
8. 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.
9. This definition often does not include 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.
10. 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 summary, whenever an EHR is produced, it should be mandated that it be produced with the audit log and revision history.

### **B. Name(s) of the EHR Vendor and their Product Name**

1. One challenge is that Hospitals were only required to install “modular” EHR software applications. Therefore, you could have a separate EHR software product from different companies, different EHR software products and then you would need to review different audit trails. When requesting medical records, ask if there are different EHR software vendors for any of these departments:
  - a. Emergency Room
  - b. Surgery Department
  - c. Labor and Delivery
  - d. Vital Monitoring Newborn
  - e. Outpatient Clinics
  - f. Inpatient Setting for Acute Care
  - g. Inpatient Setting for Behavioral Health
  - h. Laboratory
  - i. Pharmacy
  - j. Radiology
  - k. Cardiology
  - l. Other Departments

## EHRs and Audit Trail Discovery Requests

2. 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."

### C. EHR Audit Trails

1. **ASTM E2147** states that Audit reports designed for system access provide a precise capability for healthcare providers, organizations, patients, patient representatives, and advocates to see who has accessed and/or ***manipulated patient information***. Because of the significant risk of medical information manipulation in computing environments by authorized and unauthorized users, the audit report is an important management tool to monitor access and any such manipulation retrospectively.
2. **ASTM E2147** specifies how an EHR audit log records all activities impacting a medical record, for example, creating a new record, entering data into a record, changing or deleting an existing record, and all additional user access data (for example, identification, location, and date and time) to patient-identifiable information maintained in computer systems. Such audit logs should track not only data entry and modifications, but also simple access and viewing of the patient record, and whether any modifications are made during that access.
3. **ASTM E2147** creates a trustworthy record thus requires the use of secure, automatic, computer-generated, time-stamped audit logs, which shall be used to independently record the identity of the user as well as the date, time, and location of user access, and also record all entries and actions that create, change, or delete electronic records or other patient information. Full transparency of modifications or deletions or both is mandatory. For example, record changes shall not obscure **previously recorded information**.
4. The federal government has mandated that health care providers utilize EHR systems that record information about access to an EHR. See, 45 C.F.R. 170.210, referencing **ASTM E2147-01**, 7.2 through 7.4, 7.6 and 7.7; 45 C.F.R. 164.308; and 45 C.F.R. 164.312. This information is preserved by way of audit logs.
5. **In ASTM E2147-01** (2009, 2013, and 2018 revisions) section 7.6 states all actions (additions, deletions, changes, queries, print, copy) specifies inquiry, any changes made (with pointer to ***original data state***), and a delete specification (with a pointer to deleted information).
6. **ASTM E2147-18** is a **Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems**. This standard outlines the requirements for audit logs that record access and changes to health information, ensuring accountability and compliance in health IT systems. It was approved on **May 1, 2018**, and is referenced in various health IT regulations, including the ONC Cures Act Final Rule. For more detailed information, you can access the full standard on the ASTM International.
7. This specification also responds to the need for a standard addressing privacy and confidentiality as noted in Public Law 104–191 (2), or the Health Insurance Portability and Accountability Act of 1996, and the

## EHRs and Audit Trail Discovery Requests

need for a self-authenticating record that will verify accuracy and integrity. This specification describes the security requirements involved in the development and implementation of audit and disclosure logs used in health information systems. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems, and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of confidential health care information to external users for use in manual and computer systems. This specification provides for two main purposes, namely: to define the nature, role, and function of system access audit logs and their use in health information systems as a technical and procedural tool to help provide security oversight; and to identify principles for establishing a permanent record of disclosure of health information to external users and the data to be recorded in maintaining it.

8. This specification is for the development and implementation of secure audit data and logs for electronically stored health information. It specifies how to design the audit log to record all activities impacting a medical record, for example, creating a new record, entering data into a record, changing or deleting an existing record, and all additional user access data (for example, identification, location, and date and time) to patient-identifiable information maintained in computer systems. Such audit logs shall track not only data entry and modifications, but also simple access and viewing of the patient record, and whether any modifications are made during that access.
9. There is a major difference between EHR “Access Logs” and Audit Trails. Many times, a hospital may only provide a list of who logged into a patient’s record (known as an access log) since they may interrupt your request for “who accessed a patient’s chart”. In reality, we need to know who accessed the chart, what part of the chart they accessed, and what activity did they performed (Viewed Added, Modified, Deleted, Printed, etc.). We need a complete copy of the EHR Audit Log and include a date range through today’s date. Even if that is a year past the incident so that we could see if anyone viewed or modified the patient’s chart.
10. An EHR audit log (sometimes called an audit trail by some EHR companies) is a security-relevant chronological record that provides documentary evidence of, among other events, who accessed an electronic medical record system, when they accessed it, from where, and exactly what they did, such as enter new data, modify or remove existing data, view a part of the chart, obtain a printout, etc.
11. 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.
12. When asking for a patient’s audit trails (plural because there is usually more than one) during the discovery phase of the case, we need to ask for the federal format related to electronic health information in accordance with the standard specified in §170.210(b). The required format includes one-line audit trail for every time someone adds, changes, deletes, prints, and views a specific “screen” in the EHR. The electronic audit trail is required to show:

# EHRs and Audit Trail Discovery Requests


- a. Username - ID of the person who accessed the EHR information.
  - b. Event Date/Time - Date and time of entry and a new line item every time a different EHR screen was accessed.
  - c. Event Action - ID of the action taken when they accessed the EHR (View, Add, Delete, Change, Print)
  - d. Status – was the specific action rejected, completed,
  - e. Participant Object Name – This is the name of the patient.
  - f. Participant Object ID – This is the patient unique ID number assigned during registration.
  - g. Location ID - ID of the workstation they used to access the patient’s information.
  - h. Description of what area in the EHR the user accesses.
13. I would ask to receive the audit trails in an electronic searchable format (MS-Excel or .CVS) so that we can search for and filter the information. If they will only give you the audit trail in PDF version, it should all be included in one line (landscape format) 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.

## D. Best Practice Alerts

1. If the hospital is using EPIC Healthcare EHR, it’s also important to view all the “**Best Practice Alerts**” (“BPA”) were displayed when a provider was accessing the patient’s medical chart. BPAs are a central tool in the Epic Healthcare EHR decision support system that serve as reminders or warnings to clinicians during their workflows (also known as **Our Practice Advisories** (OPAs). BPAs are pop-up alerts, based upon the information entered the EHR, designed to guide the end user’s actions, offering reminders about possible diagnoses, suggestions regarding possible treatments, and warnings against contraindications. The EHR BPA portion of the audit trail would indicate what “action” the user performed when the BPA was displayed. Did the user just cancel out the alert or did the user follow the prescribed plan of action that is displayed with the alert? For example:

2/6/25, 8:05 PM

Zayad, Zakaria Mahmoud (MRN: 5318191) DOB: 2/28/1963

<span>?</span> <b>BestPractice Advisories for 11/2/21 Imaging Services</b>				
<b>Screenings</b>				Inactive
Date	User	Actions Taken	Triggers	Comment
11/07/21 2120	Safeblade, David E [B03110]	None 	General BPA section • Rule: ADMG CI PRE DIABETES SCREEN BPA [4904472]	None

# EHRs and Audit Trail Discovery Requests

## E. Patient Medical Records

1. Always request the “**revision history**” version of the Patient’s Medical Records, not the legal version or the final or complete medical records. The legal or final version is limited to the complete patient record after all the changes have been made. We need to see everything that was entered, when it was entered, who entered the information and if any of the information was modified or changed. That version is usually known as the “Revision History” which indicates all information captured or changed/modified.
2. When the administrative staff is producing the patient’s chart there is an option of not including any records or orders that have not been signed off on by the provider. If the event were not signed off, there would be no record of the event even though the information was in the chart and may be pending sign-off. Request that all records be provided and include all records even if the document has not been signed off by the provider.

## F. 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 about 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 document 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.

# EHRs and Audit Trail Discovery Requests

## G. Cell Phone:

1. Cell phone communications are quite common today. The phones might communicate via a cellular connection through AT&T, Verizon, etc. In that case, the phone carrier will have a log of every single call with whom they called and who they called with length of time.
2. There is also internal phone software like RingRX, Vecna and others that appear to be a cellular phone but only communicate within the building and only use Wi-Fi connections. But even those systems have a complete audit log of all calls showing when and who called, who they called, and how long they talked. Some of these systems track all calls and pictures or documents that were sent. Just like our cell phones, they track all calls, pictures, and in healthcare – clinical results.
3. If the issue could be related to telephone communications, always ask for the Cell phone or internal phone records which will indicate the date and time of a call, the call duration, calling from and calling to information.

## H. Sticky Notes

1. EPIC has a communication platform known as Sticky Notes. This serves as an instant messaging mode of communication between healthcare workers discussing a specific patient. EPIC lacks a report that can allow easy printing or export of these notes. This creates a common misperception among health providers that these notes are not part of the legal discoverable record. In fact, there are other ways to access these sticky notes, which are an important part of documenting the patient care provided. An in-person inspection of the EHR using a camera to record the user's screen can allow for obtaining these important communications. These sticky notes are part of the EHR and are subject to preservation by HIPPA.

## I. EPIC In-Basket

1. In Basket is Epic's communication hub. It is a secure, message-based task system within the UH Epic electronic health record (EHR) that streamlines communication and coordinates care. Users can send and receive messages about patient accounts, charts, orders, and billing needs.
2. If there are any questions regarding communications, you may need to ask for a complete listing of all in-basket communications between certain providers and nurses.

# EHRs and Audit Trail Discovery Requests

## J. List of care Providers

1. **Request a list of all care providers who care for the patient during the period of \_\_\_\_\_ and \_\_\_\_\_ including the care provider's name, credentials, years of experience within the organization, and department they work in.**
  - a. Every hospital is required to maintain a list of all care providers that interact with the patient during their clinical stay.
  - b. Normally, we can get that information from the EHR audit trails, but in certain areas, the hospital staff may not be using the same EHRs.
  - c. For example, the physical therapists may be using a paper-based system for charting their care, and thus, they would not be listed under any electronic EHR audit report.
  - d. Given that the care might have been provided years ago, the request might be considered overly broad and unreasonably burdensome, but a quick review of the patient's legal medical record would provide a source of the staff's name.

## E. Policies and Procedures:

1. Request for any and all written documents relating to policies and procedures regarding the requirements for the completeness and timing of the patient history and physical examination and clinical documentation, including a listing of the minimum contents to be included in the medical record for each EHR listed in Item B#3 for the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Once again, every EHR product and HIM department maintains written policies and procedures on how they handle the protection of medical record information for each EHR maintained and used within the healthcare system. The policies and procedures are required to be updated annually based on Federal Joint Commission Mandates.
  - b. One issue might be the timing of the care. The health system may not retain old policies and procedures. Usually, they maintain current written policies and procedures, but it is always good to ask for information based on the actual time period of care.
  - c. If they cannot provide the actual materials during the time period, we would accept the oldest written policies and procedures for each separate EHR software product that they would have available.
  - d. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.
  - e. The information is necessary to determine the actual processes for insuring that the patient's medical records are complete and meet minimal document requirements established by the healthcare institution.

## EHRs and Audit Trail Discovery Requests

2. Request for any and all documents relating to the written policies and procedures regarding specifications for **verbal orders**, including who may give verbal orders, who may receive them, and how soon they must be verified or countersigned in writing for each EHR listed in Item #1 for the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Once again, every EHR product and HIM department maintains written policies and procedures on how they handle verbal orders for each EHR maintained and used within the healthcare system. The policies and procedures are required to be updated annually based on Federal Joint Commission Mandates.
  - b. One issue might be the timing of the care. The health system may not retain old policies and procedures. Usually, they maintain current written policies and procedures, but it is always good to ask for information based on the actual time period of care.
  - c. If they cannot provide the actual materials during the time period, we would accept the oldest written policies and procedures for each separate EHR software product that they would have available.
  - d. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.
  - e. The information is necessary to determine the actual processes for handling physician “Verbal Orders” and to meet minimal document requirements established by the healthcare institution.
3. Request for any and all documents relating to the written policies and procedures regarding the **scope of practice, supervision**, and record keeping requirements of licensed physician assistants (PAs) or Nurse practitioner (NPs), including their role and responsibility during the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Once again, every EHR product and HIM department maintains written policies and procedures on what responsibility and controls the hospital maintains for all PAs and NPs used within the healthcare system. The policies and procedures are required to be updated annually based on Federal Joint Commission Mandates.
  - b. If they cannot provide the actual materials during the time period, we would accept the oldest written policies and procedures for each separate EHR software product that they would have available.
  - c. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.
  - d. The information is necessary to determine the actual processes and controls over PAs and NPs to meet minimal document requirements established by the healthcare institution.

## EHRs and Audit Trail Discovery Requests

4. Request for any and all documents relating to the written policies and procedures regarding Criteria for admission to and discharge and transfer from the unit during the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Once again, every EHR product and HIM department maintains written policies and procedures on what responsibly and controls the hospital maintains for all PAs and NPs used within the healthcare system. The policies and procures are required to be updated annually based on Federal Joint Commission Mandates.
  - b. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.
  - c. The information is necessary to determine the level of care an NP or PA can provide and what supervision they are under established by the healthcare institution.
5. Request for any and all documents relating to the written policies and procedures regarding Protocols for **transfer and transport of patients** within the hospital or from the hospital to another facility during the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Only add this request if the patient was transferred within the hospital or from the hospital to another facility.
  - b. Once again, every HIM department maintains written policies and procedures on what protocols are used for transfer and transport of patients within the hospital or from the hospital to another facility. The policies and procures are required to be updated annually based on Federal Joint Commission Mandates.
  - c. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.
  - d. The information is necessary to determine if the right policies and procedures are followed if the patient is transferred and transported within the hospital or from the hospital to another facility established by the healthcare institution.
6. Request for any and all documents relating to the written policies and procedures regarding Protocols that define the physician, specialist and consulting physician to be called for patient emergencies, including a response time for physicians to respond to patient emergencies during the time-period of \_\_\_\_\_ to \_\_\_\_\_ or written policies and procedures near the time period, or the oldest written materials available after the time period.
  - a. Once again, every HIM department maintains written policies and procedures on what protocols are used for transfer and transport of patients within the hospital or from the hospital to another facility. The policies and procures are required to be updated annually based on Federal Joint Commission Mandates.
  - b. Therefore, the request is NOT vague, overly broad, and unreasonably burdensome.

## EHRs and Audit Trail Discovery Requests

- c. The information is necessary to determine if the right policies and procedures are followed if an emergency or life-threatening event occurs during the care of the patient as established by the hospital.
7. Request for a list of all electronic patient monitoring devices connected to the Plaintiff's during the time-period of \_\_\_\_\_ to \_\_\_\_\_ and if the patient monitoring devices were electronically connected and automatically transfers the monitoring device clinical data directly to the EHRs listed in Request #1 or if the electronic patient monitoring device clinical data must be manually re-entered by the Hospitals staff.
    - a. Once again, every Hospital maintains a list of electronic patient monitoring devices that are used within every room or care delivery area within the hospital.
    - b. Since we are requesting the data for specific dates and based on the care of patients, the request is NOT vague, overly broad, and unreasonably burdensome.
    - c. The information is necessary to determine how patient clinical information from electronic patient monitoring devices is placed into the EHR, either manually, or through electronic transfer.



**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 (LFHIMSS) and is a Certified professional in healthcare information systems (CPHIMS).