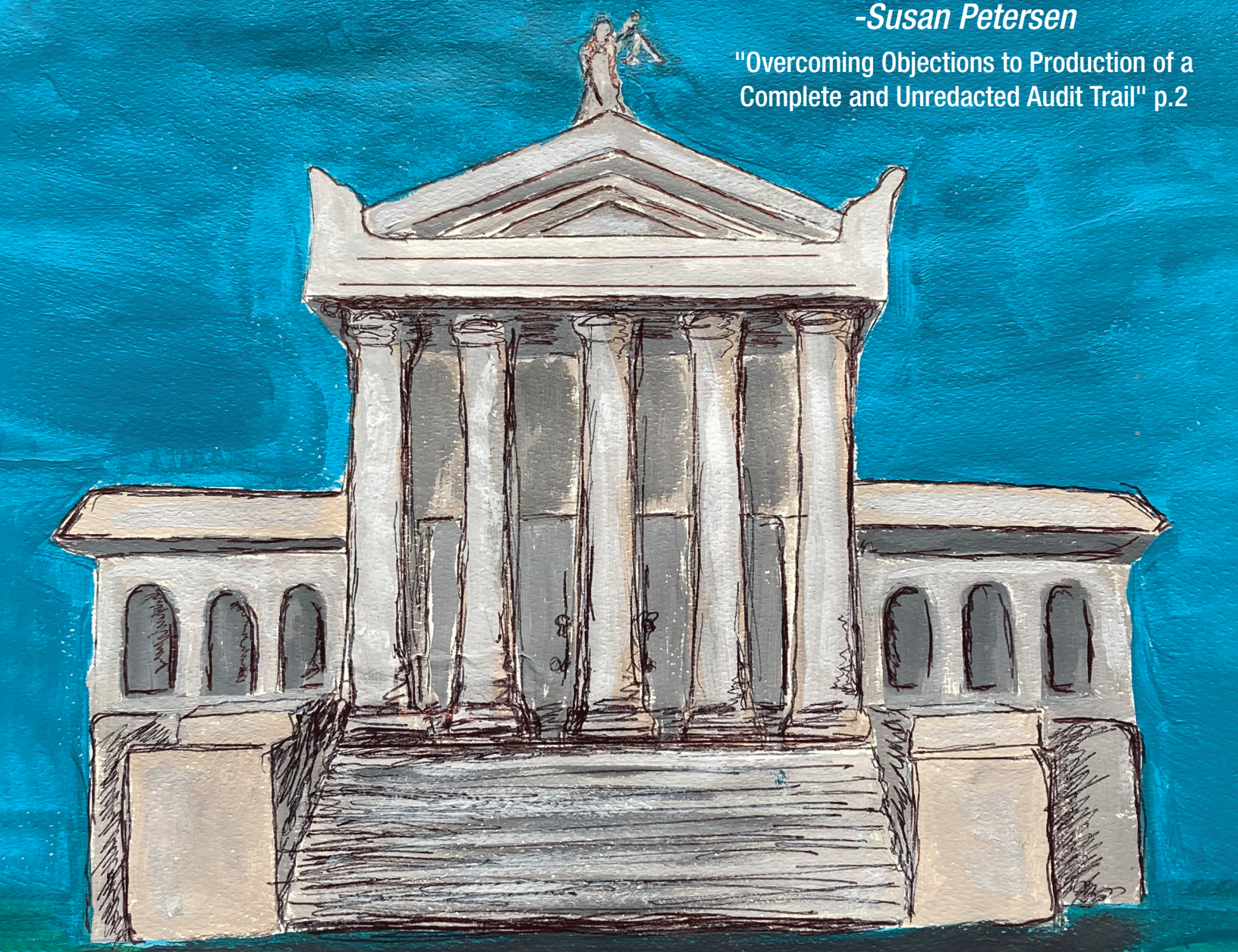
CATA
CLEVELAND ACADEMY OF TRIAL ATTORNEYS
Spring 2023
News

"Know the Law. Know Your Client's Rights. Work Hard to Protect Both."

-Susan Petersen

"Overcoming Objections to Production of a Complete and Unredacted Audit Trail" p.2



Also in this issue:

Susan E. Petersen is a principal at Petersen & Petersen. She can be reached at 440.279.4480 or SEP@petersenlegal.com.

Overcoming Objections to Production of a Complete and Unredacted Audit Trail

by Susan E. Petersen

At this point, you have read about "A Patient's Right to Access and Inspect their Electronic medical records."[1] You know that amongst the "10 Things You Must Request in Every Medical Malpractice Case" is the audit trail/log.[2] Yet, in response to these discovery requests in your case, opposing counsel gives you nothing but objections. Now what?

This article will arm you with practical advice and lessons learned to overcome the frequent objections raised by hospitals and their attorneys to production of your client's electronic medical record ("EMR") and audit trails/logs.

1. Know The Federal Laws Regarding EMR Audit Trails:

The process of defeating the typical objections to production of an audit trail/log begins with knowledge of the statutory requirements of a hospital's EMR and corresponding audit trails/logs. These laws are your first line of defense. You must educate opposing counsel and your trial court that a patient's right to inspect and obtain copies of their EMR and audit trail/logs is protected by federal law. Arm yourself with an understanding of the list of federal regulations established by the US government to protect the privacy and security of patients' electronic health information. Federal laws and agencies that protect your right of access include the Health Information Technology for Economic and Clinical Health (HITECH) Act, the 21st Century Cures Act, the Office of the National Coordinator for Health Information Technology (ONC), the Health Insurance Portability and Accountability Act (HIPAA), and the federally adopted standard, ASTM E2147-18.

HITECH ACT

As part of a national effort relative to EMRs, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. The goal of the HITECH Act was aimed at promoting the widespread adoption of EMRs in the US healthcare system. The HITECH Act also established regulations for privacy and security of electronic health information, including the requirement for healthcare providers to comply with the Health Insurance Portability and Accountability Act (HIPAA).[3]

HIPAA

HIPAA, enacted in 1996, sets national standards for the privacy and security of patients' health information. The HITECH Act amended HIPAA to strengthen its protections and to establish breach notification requirements for covered entities and their business associates.[4] The HIPAA Security Rule requires covered entities to implement procedures to regularly review and audit access to EMRs. Covered entities are defined as healthcare providers, health plans, or healthcare clearinghouses that transmit any health information in electronic form. This includes doctors' offices, hospitals, clinics, health insurance companies, and healthcare billing companies.[5]

Under 45 CFR §164.530, a section of the HIPAA Privacy Rule, covered entities and business associates are required to implement policies and procedures to document and track certain actions related to EMRs. This includes actions such as who accessed the information, when it was accessed, the user ID of the person accessing, and the actions performed on that information, such as viewing, modifying, or deleting.[6] Covered entities must maintain the audit trail for at least six years from the date of creation.[7]

ONC

The HITECH Act also established the Office of the National Coordinator for Health Information Technology (ONC) as the primary agency responsible for promoting the adoption and meaningful use of health information technology in the US healthcare system.[8] Under the ONC's regulations, covered entities are required to provide patients with access to their health information, including EMRs and audit trails/logs, in a timely manner and in a format that is convenient and accessible to the patient. Since its establishment, the ONC has continued to play a critical role in shaping the direction of health IT in the US. This has included the development of standards and policies for EMRs, the promotion of patient access to health information, and efforts to address privacy and security concerns related to the use of health IT.

CURES ACT

The 21st Century Cures Act, enacted in 2016, built upon the HITECH Act's provisions for patient access to health information by expanding patients' rights to access their health information electronically.[9] As part of the Cures Act, Congress mandated audit controls of a patient's EMR to "record and examine activity in information systems that contain or use electronic protected health information . . in order to protect the integrity of such information." This included the use of audit trails and edit histories as a necessary security measure to safeguard and protect electronic health information from improper alteration or destruction. [10, 11]

ASTM E2147-18

In 2018, the US government codified standards for recording and maintaining EMR audit trails/logs via 45 CFR §170.299. The purpose of this regulation was to establish a standardized way for healthcare providers and organizations to maintain audit logs and track disclosures of patients' health information, as required by the HIPAA Privacy Rule. Specifically, this regulation codified ASTM E2147-18, developed by the American Society for Testing and Materials (ASTM), which is the "Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems."

The purpose of ASTM E2147-18 is expressly defined within the standard:

> 1.2 The first purpose of this specification is to define the nature, purpose, and function of system access audit logs and their use in health information systems as a technical and procedural tool to help provide privacy and security oversight and produce a self-authenticating record that would, when maintained together with its audit logs, speak to and confirm its own integrity and accuracy of the medical and other data within the record. Moreover, in concert with organizational confidentiality and security policies and procedures, permanent audit logs can clearly identify all system application users who accessed and acted on patient identifiable information or both, and identify the location of the user, identify patient information accessed, and maintain a permanent record of actions taken by the user. . . Full transparency of modifications or deletions or both is mandatory. For example, record changes shall not obscure previously recorded information. . . **Audit logs and healthcare information shall be provided when specifically requested by** authorized healthcare providers; **the patient, his personal representative,** advocate, and/or designee; researchers; quality control personnel; and organizational managers or administrators or both; and other persons authorized to have access to patient records or patient-identifiable information or both in any form.
>
> 1.4 The second purpose of this specification is 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. Security management of health information requires a comprehensive framework that incorporates both mandates and criteria for disclosing patient health information found in federal and state laws and rules and regulations and ethical statements of professional conduct. **Accountability for such a framework shall be established through a set of standard principles that are applicable to all healthcare settings and health information systems.**[12]

Significantly, ASTM E2147-18 4.3 explains why audit trails/logs are not privileged documents, stating:

> A patient has a right to know who has accessed their patient information and what occurred during such access. Access by any means (viewing or any other action) regarding the patient record and/or audit log or the data

contained therein by attorneys, risk management, or similar individuals or entities are not privileged actions and must also be fully transparent and disclosed.

By standardizing the way in which audit and disclosure logs are maintained and tracked, the federal government sought to promote greater transparency and accountability in the use of patients' health information, including the prevention of unauthorized access or disclosure of sensitive health information.

2. Practice Advice/ Lessons Learned on Overcoming Objections:

Defending against objections to the discovery of your client's audit trails/ logs will depend on the specific circumstances of the case and the available evidence. However, here are some approaches to overcome some of the objections we typically see:

"We do not have an Audit Trail. It does not exist."

If the defendant is claiming that it does not have an audit trail, you need to challenge this assertion by requesting further information or evidence. For example, you can:

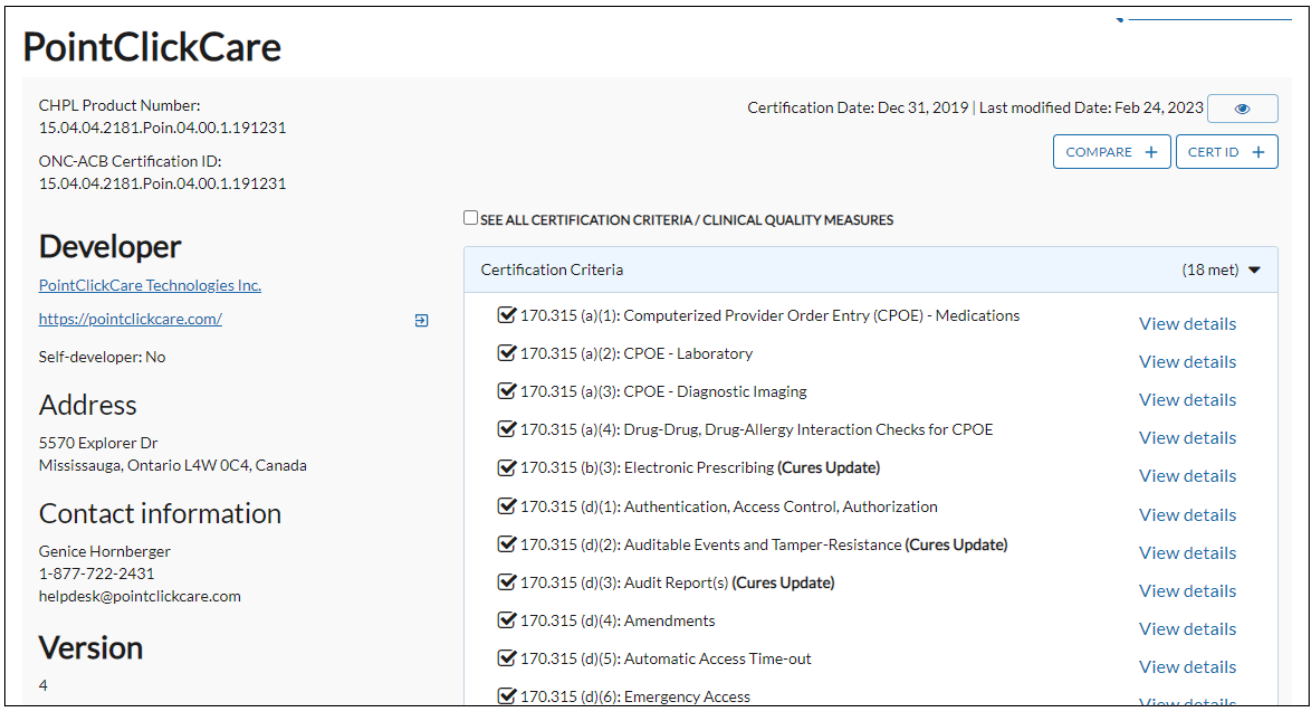
- Request that the defendant provide documentation or testimony from their EMR vendor or IT department to support their claim that no audit trail exists.
- Request the name of the defendant's EMR Software Vendor, product, and version and go to the ONC website.

"We cannot provide what we do not have" was the objection encountered in a recent wrongful death action. This was overcome via evidence independently obtained through the ONC website at https://chpl.healthit.gov.

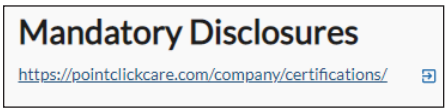
One of the ONC's main functions is to certify EMR software to ensure that it meets certain standards for functionality, security, and interoperability.[13] Specifically, EMR software vendors must undergo a certification process to receive ONC certification. The certification criteria cover areas such as privacy and security, clinical quality measures, and features to include audit reports.[14] Once an EMR software vendor receives ONC certification, the software product is listed on the Certified Health IT Product List (CHPL), which is publicly accessible through the ONC website.

The ONC website provides a searchable database of all certified EMR products, including the vendor's name, product name, certification date, and version number. In addition to the basic information about the certified EMR product, the CHPL also includes a set of mandatory disclosures that vendors must provide to include audit reports.

On the ONC website, just type the defendant's EMR software and hit search. When the EMR software product appears, a click will take you to a page of disclosures which provide detailed information about the product's capabilities and limitations. One of the items listed is whether the software meets criteria §170.315(d)(3) Audit Report(s)(Cures Update).[15] If the box is checked as evidenced by the following example, you have independent evidence that an audit trail exists and is producible from your defendant:



On the product webpage, there will also be a link to the company's mandatory disclosures as seen in the following example:



It will be impossible for a defendant to credibly maintain that an audit trail does not exist once you obtain the EMR software vendor disclosure to the government that it does.

"Audits are managed by a third party, we can't access them."

If the defendant claims that it cannot provide the audit trail because it is managed by a third party, you may need to take steps to secure evidence to compel the audit trail. For example, you could:

- Request a subpoena or court order compelling the third party to produce the audit trail.
- Argue that the defendant has a duty to ensure that third-party vendors are complying with industry standards and regulations for maintaining electronic medical records.
- Request that the Defendant produce a copy of its service agreement with the third-party vendor.

In the recent case we had, this was another objection to overcome. The defendant facility's software vendor was headquartered in Canada and not easily subject to subpoena. We got an Order to compel a copy of the EMR service agreement with the third-party vendor to establish what obligations the defendant and vendor had relative to the audit trail.[16]

"Producing the Audit Trails/Logs is unduly burdensome."

When overcoming an objection that producing an audit trail is unduly burdensome, there are a few potential strategies that can be employed:

- Challenge the claim of undue burden: The defendant has the burden of proving that producing the audit trail would be unduly burdensome, which requires showing that the cost or effort of producing the audit trail outweighs its potential value as evidence. Typically, an IT department can easily produce an audit trail/log into an excel document with a few key strokes.
- Seek a court order: If the defendant continues to object to the production of the audit trail, it may be necessary to seek a court order compelling its disclosure. This may require a motion to compel discovery, and could involve a hearing or other court proceedings.

"Audit Trails/Logs are irrelevant."

When the defendant objects that an EMR is not relevant, there are a few potential strategies to overcoming such an objection:

- Establish the relevance of the audit trail: You may need to demonstrate how it relates to the issues in the case. For example, you could argue that the audit trail is necessary to establish the authenticity of the electronic medical record, to show that certain medical decisions were made or not made, or to demonstrate the presence or absence of tampering.
- Challenge the objection on factual grounds: You may need to show that it contains information that is critical to the issues in dispute.

"Audit Trails are not kept in the ordinary course of business."

If the defendant argues that audit trails are not kept in the ordinary course of business, you need to disprove this proposition. For example, you could:

- Take the deposition of the IT Manager for the facility about its EMR record keeping and audit trails/logs.
- Present testimony from experts in the field of electronic medical records who can attest to the importance of maintaining audit trails and how they are typically managed.

In our recent case, the defense pivoted to this objection after the Court compelled the defendant facility to tender its audit trails "to the extent that Defendants maintain such documents in the ordinary course of business." In response to the Judgment Entry, the Defendants produced nothing. Following a hearing on Plaintiff's Motion to Show Cause, the trial court issued the following Sanctions Order:

> "The Court is not persuaded by Defendants' interpretation that the Court's order does not apply to them because they do not maintain audit trail information in the ordinary course of business. The evidence showed that Defendants maintained facility level audit trail information electronically and that it could provide the information in printed form to Plaintiff's counsel by clicking a few buttons. . . . The Court finds Defendants . . . in contempt and imposes the following: $1,000 for each day after June 28, 2021 for the first five days and $5,000 a day thereafter for Defendants failure to provide audit trail information as requested in Plaintiff's Request for Production

Nos. 46, 47, and 57. Defendant may purge this Order at any time."[17]

As set forth on the docket in subsequent briefing, the Defendant facility thereafter tendered 1,145 pages of its audit trail/logs on June 28, 2021.[18]

"Audit Report Data is privileged/ work product."

When the defense objects to production of complete audit trail/logs based upon a privilege claim, you must fight back and educate your trial court. Audit trails and logs are not privileged documents per the federally adopted standard for Audit and Disclosure Logs for Use in Health Information Systems. Section 4.3 of ASTM E2147-18, "Significance and Use" expressly states:

> 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. In addition, the access and disclosure logs become powerful support documents for disciplinary and legal actions. Moreover, audit reports are essential components to comprehensive security programs in healthcare and vital for the privacy rights of the individual. **A patient has a right to know who has accessed their patient information and what occurred during such access. Access by any means (viewing or any other action) regarding the patient record and/or audit log or the data contained therein by attorneys, risk management, or similar individuals or entities are not privileged actions and must also be fully transparent and disclosed.**[19]

Here are the arguments to overcome any "privilege" objection:

- Audit trail entries are not privileged per 45 CFR §170.299 and ASTM E2147-18. Under Ohio law, the attorney-client privilege and work-product doctrine protect only certain types of communications or materials, and only if certain requirements are met. In Ohio, the attorney-client privilege protects communications made in confidence between an attorney and a client for the purpose of obtaining legal advice or assistance. The work-product doctrine protects materials prepared in anticipation of litigation. As stated in ASTM E2147-18 4.3, neither of these privileges are applicable.
- Consider a protective order: If the defendant expresses confidentiality concerns, you may be able to reach a compromise by agreeing to limit the scope of the audit trail production or by seeking a protective order.

"Audit trail data after the date of the patient's discharge or death is not discoverable."

There is a good chance that if you get an audit trail/log, the defendants will have limited the data to a premature end date. This is despite the fact that EMRs can be accessed, changed, and/ or modified after a patient is discharged or dies. The terminology section of ASTM E2147-18 is extremely helpful to explaining why a partial production is unacceptable and contrary to law:

3.1.2 *access report*—record that is a subset of the "clinical audit report" documenting the following information about each access of patient medical information: user identification (the person accessing the record); the date and time of the access (documenting both start and exit times spent on each record accessed); total duration of access; specific terminal, hardware, or location from which the access occurred; type of action (for example, copy, print, addition, modification, and deletion to the record, and when any access has been made, even when the user makes no entry or change); specific patient data accessed.

3.1.2.1 *Discussion*—The above access information is an indispensable part of the medical record because it is clinically relevant and does not appear in certain iterations of the record. All accesses shall be recorded, and the entire access record shall be provided when an access record is requested.

3.1.4.1 *Discussion* — Authentication of the record is possible only when the associated audit data relating to the record is made an indispensable part of the medical record.

3.1.17 *integrity*—as it relates to health information, it means that the information/record is accurate, complete, and immutable in that all actions taken with respect to the record are transparent.

3.1.19.1 *Discussion*—Audit data is integral to self-authentication and trustworthiness of patient information including the medical record and billing record.

4.6 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 need for a self-authenticating record that will verify accuracy and integrity.

By reviewing the audit trail up to the date of production of the EMR, a plaintiff can ensure that their medical records accurately reflect their medical history and the care that they received. If the plaintiff suspects that their records were altered or modified after the date of their discharge, the audit trail can help them identify any such changes and potentially provide evidence to support their claims.

3. Be wary once you receive the Audit Trail:

Although federal law prohibits editing the audit trail in the EMR system, the information can be altered once it is exported to a spreadsheet. More importantly, key items might be deleted or changed or eliminated from the production of the audit trial in discovery. Insist on the unedited, original electronic format of the document (e.g., "EXCEL"), and have a forensic expert examine it to ensure no one tampered with it. Do not accept other formats, such as a PDF document. Be sure to obtain the Search Header as part of its production. The Header will provide you with the search parameters in producing the audit trail which provide a window as to certain data being excluded.

Question audit records that lack evidence of any EMR access from the lab, radiology, pharmacy, or other departments within a hospital. Many of the EMR platforms are "closed systems," which means they cannot be integrated with other systems in the hospital. The documentation systems other departments use may not show up on an audit inquiry of the main clinical documentation system. Each database that is not directly connected to the main clinical charting system must be queried as part of a records search and will have its own audit trail/log which has to be produced.

Audit logs often include additional elements. ASTM Standard E2147-01 suggests that audit logs also should include data identifying the access device—the terminal, work station, or device from which the user obtained access—and the reason for access. Request a log of the terminal, work station, and device locations as part of your discovery requests to know where the access occurred.

4. If the Defendants' EMR and/or Audit Trails/Logs Production Appears Altered or Incomplete, Consider Asserting Your Client's Right to Inspect the EMR:

As part of the HITECH Act, the US Department of Health and Human Services requires that "an individual has a right of access to inspect and obtain a copy of Protected Health Information about the individual..." 45 CFR §164.524(a)(l). In a section entitled "Empowering Patients and Improving Patient Access to Their Electronic Health Information, Section 4006 of the Cures Act amends the HITECH Act to further require that patients have direct access to their protected health Information, providing:

> [I]f the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual.[20]

Given the recent federal mandates, the dearth of case law on requests for inspections is not surprising. Where defendant-medical providers have nonetheless ignored these clear legislative mandates, Courts have ordered them to allow patients to conduct inspections required pursuant to the Civil Rules. *Borum v. Smith MD et al.*, Dist. Court, WD Kentucky (July 14, 2017); *Picco v. Glenn*, D. Colo. No. 12-CV-02858-RM-MJW, 2015 WL 2128486 (May 5, 2015); *Kirt v. Bozeman Deaconess Health Services*, Mont. 18th Dist. Ct. No. DV-10-209CX (Aug. 8, 2014).

In our recent case referenced in this article, we had enough doubt about the authenticity of the decedent's EMR that we pressed for a deeper dive. The trial court granted our motion to compel a virtual inspection of the EMR to be conducted and recorded via "Zoom" with our EMR expert using a court approved protective protocol and/or privacy agreement.[21] The defendants objected and appealed all the way to the Ohio Supreme Court, claiming an inspection would jeopardize confidential and privileged material.[22]

In the Eighth District Court of Appeals, there are two Judgment Entries which will be helpful to your cause should the need for a virtual inspection arise:

> Motion by appellee to dismiss appeal for lack of a final appealable order is granted. Discovery orders not involving the discovery of confidential or privileged information are not final appealable orders under R.C.2505.02(B)(4). *Myers v. Toledo*, 110 Ohio St.3d 218, 2006-Ohio 4353. The trial

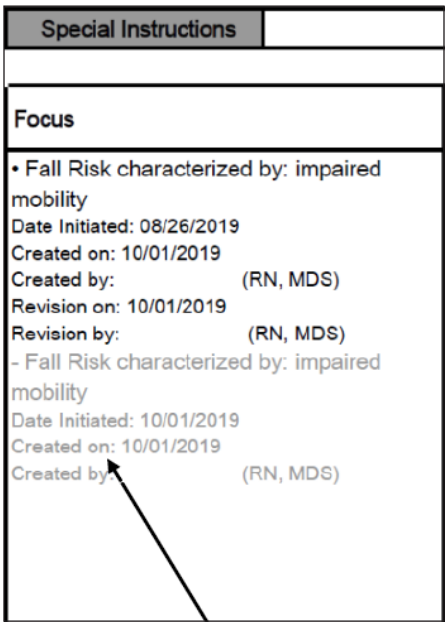
court's order allowing the estate of the decedent to view the decedent's electronic medical records maintained by the appellants does not involve privileged or confidential information. Appellants are concerned that other privileged or confidential documents would be viewable. However, the court approved a protected protocol and privacy agreement, which provides in part "the parties presently agree that the inspection shall be confined to the resident's clinical records only and shall not include any facility level reports or other patient data." Additionally, under the approved protocol, the appellants would control the remote viewing of the electronic documents.[23]

* * *

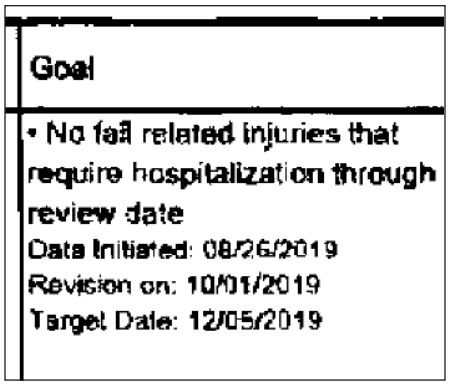
Application by appellants for reconsideration is denied. By the terms of the protective order, discovery is limited to the appellee-decedent's electronic clinical records. Pursuant to the discovery protocol, the appellants are given control over what is actually viewed by the appellee during the remote viewing of the electronic medical records. Even if the appellants' emails to the trial court's staff attorney properly raised the concern that the remote viewing may result in the appellee viewing documents that are outside the scope of discovery, the trial court's order restricts the viewing to the decedent's clinical records and does not allow for the release of privileged documents. *Smith v. Chen*,142 OhioSt.3d 411, 2015-0hio-1480.[24]

What occurred thereafter epitomizes why the battle to preserve the federally protected right to a complete EMR and audit trails/logs is so critical to truth and justice. The following comes directly from Plaintiff's Trial Brief on the publicly available docket:

> On August 17, 2021 – just over a month before trial – the Defendants lost their appeal to the Ohio Supreme Court to avoid this Court's order of a virtual inspection of Plaintiff's decedent's electronic medical record. Three days later, on August 20th, they turned over a complete copy of [the patient's] Fall Risk Care Plan, knowing that Plaintiff would soon discover it via the court ordered virtual inspection. As it turns out, [the patient's] Fall Risk Care Plan was NOT initiated on 8/28 afterall as the medical records previously led Plaintiff to believe. In fact, it was not initiated on any date that [X] was a patient of [the attending physician]. It was faked. The Defendants made it appear as if it existed during her residency by excluding the "Created On" date from the print job. The August 20th production finally included the data Plaintiff had been requesting for months and months as seen in the following snippet:



> The arrows point to the finally disclosed time stamped "Created On" date which revealed that the Defendants created this Fall Risk Care Plan AFTER [X]'s discharge and death. The Fall Risk care plan was not just below standard, it was backdated to make it look as though it was in place during her residency! . . . Not only did it fail to include all the needed interventions to keep her safe (e.g., bedside tables with wheels locked), it failed to include ANY interventions <u>because it didn't exist.</u>
>
> . . . The Fall Risk Care Plan provided pre-suit and in discovery in this case would lead anyone to believe that it existed during her residency. The following is a snippet of that version of the medical record provided which conveniently excluded from its print job the "Created Date:"



25

Conclusion

When it comes to these frequent objections to production of a complete and unredacted EMR and audit trail, it is imperative that legal professionals prioritize transparency and accountability. This discovery can provide crucial insights and evidence to determining the facts of a case. By overcoming objections and following the federal statutes, codes, and regulations for EMRs and Audit Trails/Logs, we can uphold the principles of integrity and truth. Know the law. Know your client's rights. Work hard to protect both. ■

End Notes

1. Mellino, Calder & Lewallen, Meghan, "A Patient's Right to Access & Inspect Their Electronic Medical Record," CATA NEWS, Spring 2022, pgs. 8 – 11.
2. Herman, Dustin, "10 Things You Must Request in Every Medical Malpractice Case," CATA NEWS, Spring 2022, pg. 12 -15.
3. Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, 123 Stat. 115 (2009). Section 13401 of the HITECH Act amends the privacy and security provisions of HIPAA to extend their application to business associates of covered entities and to increase penalties for noncompliance.
4. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, 42, and 50 U.S.C.).
5. 45 CFR §160.103 and is available at the following link: https://www.ecfr.gov/cgi-bin/text-idx?SID=605210909db327f7bb8b0d13112f95a1&mc=true&node=pt45.1.160&rgn=div5#se45.1.160_1103.
6. HIPAA Security Rule, 45 CFR §164.312(b) and is available at the following link: https://www.ecfr.gov/cgi-bin/text-idx?SID=e53724509c83f7c57d50d14c7ec90faa&mc=true&node=se45.1.164_1312&rgn=div8.
7. 45 CFR §164.316(b)(1) - Policies and procedures and documentation requirements and is available online at the following link: https://www.govinfo.gov/content/pkg/CFR-2013-title45-vol1/xml/CFR-2013-title45-vol1-sec164-316.xml.
8. Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, 123 Stat. 115 (2009).
9. 45 CFR §164.312(b).
10. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).
11. 45 CFR §164.312(c).
12. ASTM International. (2018). ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems. Retrieved from https://www.astm.org/Standards/E2147.htm (emphasis added).
13. 45 CFR §170.304, which outlines the requirements for the certification of electronic health record (EHR) technology. This regulation was issued by the Office of the National Coordinator for Health Information Technology (ONC) and is available online at the following link: https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=3ca9b11ba8d1f6b1dc7a0c334a126d8d&mc=true&r=SECTION&n=se45.1.170_1304.
14. 45 CFR §170.302, which outlines the requirements for the certification of electronic health record (EHR) technology. This regulation was issued by the Office of the National Coordinator for Health Information Technology (ONC) and is available online at the following link: https://www.ecfr.gov/cgi-bin/text-idx?SID=d6f21917a3d55a7e3e0c1b14700eae48&mc=true&node=se45.1.170_1302&rgn=div8.
15. 45 CFR §170.315(d)(3) which outlines the certification criteria for the "Audit Report(s)" capability in electronic health record (EHR) technology. This regulation was issued by the Office of the National Coordinator for Health Information Technology (ONC) and is available online at the following link: https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=3ca9b11ba8d1f6b1dc7a0c334a126d8d&mc=true&r=SECTION&n=se45.1.170_1315.
16. *Michelle Bolaney, etc., et al. v. Mapleview Operating Company, LLC, etc., et al.*, Cuyahoga Cty. Case No. CV-20-934555, Judgment Entry 6/29/21 ("The Court, in having conducted an in-camera review of Defendant's service agreement with electronic medical records service vendor, determines that the agreement is discoverable. Defendants shall provide the agreement to Plaintiffs' counsel who shall maintain it confidentially, for counsel's eyes only, unless otherwise ordered by this Court. Defendants may redact any pricing information before tendering it to Plaintiffs' counsel.").
17. *Michelle Bolaney, etc., et al. v. Mapleview Operating Company, LLC, etc., et al.*, Cuyahoga Cty. Case No. CV-20-934555, Judgment Entry, 7/25/21.
18. *Michelle Bolaney, etc., et al. v. Mapleview Operating Company, LLC, etc., et al.*, Cuyahoga Cty. Case No. CV-20-934555, Plaintiff's Final Pretrial Statement, filed on August 24, 2021.
19. ASTM International. (2018). ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems. Retrieved from https://www.astm.org/Standards/E2147.htm.
20. 42 U.S.C. § 300jj-52, Section 4006 of the Cures Act.
21. *Michelle Bolaney, etc., et al. v. Mapleview Operating Company, LLC, etc., et al.*, Cuyahoga Cty. Case No. CV-20-934555, Judgment Entry, 7/25/21.
22. 2021-0780 *Bolaney v. Mapleview Operating Co., L.L.C.*, Cuyahoga App. No. 110373.
23. *Bolaney v. Mapleview Operating Company, LLC, et al.*, Eighth District Court of Appeals, No. 110373, Judgment Entry, April 14, 2021.
24. *Bolaney v. Mapleview Operating Company, LLC, et al.*, Eighth District Court of Appeals, No. 110373, Judgment Entry, May 5, 2021.
25. *Bolaney v. Mapleview Operating Company, LLC, et al.*, Cuyahoga County Case No. CV 20-934555, Plaintiff's Trial Brief, filed on September 21, 2021.