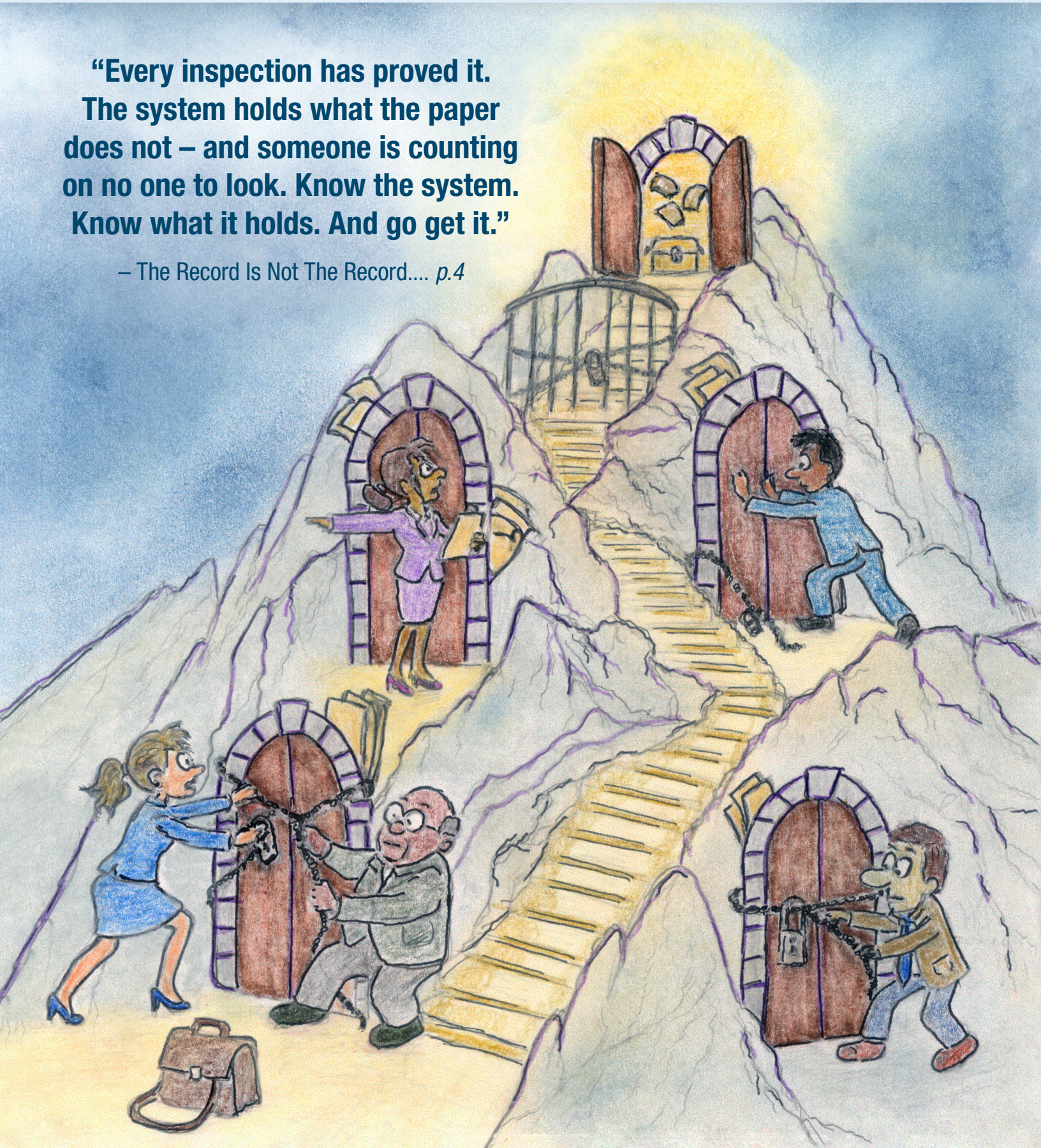
CATA
CLEVELAND ACADEMY OF TRIAL ATTORNEYS
News
Spring 2026

"Every inspection has proved it. The system holds what the paper does not – and someone is counting on no one to look. Know the system. Know what it holds. And go get it."

– The Record Is Not The Record.... *p.4*



The Record Is Not The Record:

EHR Inspections, Hidden Data, and Ten Lessons for Finding What Was Never Produced

by Susan E. Petersen, Esq.

In March 2026, a defense law firm wrote a check to my office for $221,937.98.

This was not discretionary. It was an agreed-upon sanctions payment entered after a court-ordered forensic inspection of the hospital's live electronic health record ("EHR") system uncovered 845 pages of medical records that had never been produced. Seven months earlier, defense counsel had certified that the complete electronic medical record—including audit trails and note revision histories—had been fully produced. The court found otherwise.

The Sanctions Order, issued in October 2025, made the basis for cost-shifting explicit. The court concluded that defendants had failed to comply with their prior discovery order and that no circumstances justified withholding the records. As the court explained, "[t]he fact that Plaintiffs were forced to proceed with a multiple day, virtual, live EMR inspection to obtain additional documents that should have been produced in discovery demonstrates that the Summa Defendants failed to comply with this Court's January 29, 2025 Order and with the general principles of discovery."[1]

The sanction was not imposed for delay in the abstract. It was imposed because the inspection proved what the production did not—those responsive records existed within the system and had not been produced. The court ordered defendants to pay all reasonable fees and expenses associated with the inspection pursuant to Ohio Civ.R. 37(B)(3). The defendants contested the amount. The parties reached agreement in February 2026, and final payment was ordered by March 6.[2]

The check arrived.

Eight hundred forty-five pages of the patient's own protected health information—inside the hospital's EHR system the entire time. Available to any authorized user. Never produced. Never disclosed.

This is the argument. You cannot litigate what you cannot see; until you go inside the system—not the printed chart, but the live database—you do not know what it contains. What you receive reflects the limits of the query, the filters applied, and the assumptions built into the system.

> *Risk management does not print your client's chart. It runs a query. And whoever sets the parameters of that query decides what you get.*

I have been conducting EHR inspections for many years, including prior to a 2023 article I published in this journal.[3] That article catalogued the standard objections raised when plaintiffs seek audit trail data and live access to EHR systems, and it described a single case in which those objections were overcome through targeted discovery and inspection. Since that publication, I have conducted additional inspections of live EHR systems. The lessons have been consistent.

When a hospital produces the medical record, it is not opening a drawer and handing you the contents. It is running a query against a database—and that query was almost certainly not designed with your case in mind. It was designed for billing. For rounds. For the nursing supervisor. For risk management's routine chart reviews. The filters built into that query determine what surfaces in the report. Everything else stays in the system. The chart you receive with the title "Legal Medical Record" is not the record. The redacted audit trail that comes as a non-sortable PDF that ends on a date that the patient died or was discharged is not the record.

In an increasingly AI-integrated clinical environment, the terrain continues to shift. The medical record is no longer confined to the hospital's certified system. It may also reside within the retention policies of third-party scribe vendors, in the space between what an AI system generated and what a physician ultimately reviewed and signed, and in underlying

data layers that existing audit trail standards do not yet require to be preserved.

What follows is a field guide to getting inside the system—and to understanding what happens when the record has already left it entirely.

I. The Live Virtual Inspection: What It Is and How to Get One

The answer to a curated production is not another document request. It is access to the system that generated it. You need an agreed-upon or court-ordered, real-time examination of the live system that generated it. Not a deposition or a request for additional documents. An inspection of the system itself.

Using a secure remote connection — e.g., Zoom— the defendant's IT staff connects your qualified forensic expert to a live session of the hospital's EHR. The session runs under a court-approved or agreed-upon protective protocol: inspection is confined to the patient's clinical records, the defendant controls the remote session, and the expert's access is supervised at all times. No data leaves the system except through authenticated export under defense counsel's supervision. The session is videotaped; screenshots are captured throughout the inspection and uploaded to a shared cloud folder accessible to the parties pursuant to the protocol's terms.

This framework addresses the confidentiality concerns defendants typically raise and does so comprehensively. The safeguards are sufficiently robust that courts have not identified a legitimate basis for objection, and the litigation record reflects that result: where inspection has been ordered, those objections have failed. The same pattern holds on appeal, where the Ohio Eighth District Court of Appeals has repeatedly dismissed interlocutory challenges to inspection orders for lack of a final, appealable order.[4] Inspection reveals context that a printed chart cannot—how records relate, what was visible to the user, how the system functioned at the time of care, and which systems were involved.

That distinction is particularly significant in multi-system hospital environments. As recognized by the IEEE Standards Association—an international body that develops widely adopted technical standards—the ICAID Workgroup on Data Quality Standards of Electronic Health Records has identified that EHR systems vary across facilities and implementations, often resulting in inconsistencies in how records are generated and interpreted.[5] A single patient's care may span multiple platforms—EPIC for inpatient care, Cerner for outpatient services, Oracle for imaging, and Soarian for surgical documentation—each generating its own data, each maintaining its own audit trail, and each requiring its own query.[6] A standard production typically runs against one system. An inspection can reach them all.

The following example, drawn from a recent inspection, demonstrates how revision histories for physician progress notes are accessible within the EPIC electronic medical record. Once inside the chart, the reviewer navigates to the "Notes" tab, clears any default filters to ensure all entries are visible, and selects the progress note of interest.

After opening the note, navigating to the bottom of the screen reveals whether the entry has been revised. Where revisions exist, EPIC provides a clearly identifiable link to the note's revision history. Selecting that link opens a view displaying all prior versions of the note, each accessible for review. Reviewing these iterations reveals when changes were made and what changed. This process moves beyond the static version of a note typically produced in discovery and exposes the full history of the entry—an embedded audit trail reflecting its evolution over time.

The Procedural Vehicle

A live virtual inspection may be obtained through three procedural avenues: agreement of the parties, a request for production under Rule 34 that specifically identifies the live EHR system as the subject of inspection, or motion practice. Ohio Civ.R. 34(A) expressly authorizes a party to compel the production and inspection of electronically stored information, including access to the systems in which that information resides, when within the possession, custody, or control of another party.

In recent cases, this request has been incorporated at the outset of litigation, including within the joint discovery plan and initial discovery requests, often accompanied by a proposed protective protocol. Framed in this manner, the request places the issue squarely before the parties from the first scheduling conference. In a number of matters, that early framing has resulted in agreement without the need for motion practice.

> **LESSON 1** *A virtual inspection is the only mechanism by which the completeness of an electronic health record can be independently verified and should be requested at the outset of the case, in the initial joint discovery plan, as a primary remedy rather than a fallback. When defendants object, the case law supports the request, and when they pursue interlocutory appeal, Eighth District precedent supports dismissal for lack of a final, appealable order.*

The cases that follow illustrate why inspections are truth magnets.

II. The Exemplars — What Each Case Established

Matter One: The Care Plan That Did Not Exist

The facility entered litigation with confidence. It produced what appeared to be a complete and contemporaneous Fall Risk Care Plan—dated, formatted, and authenticated with nursing signatures. On its face, the document reflected compliance.

It was not contemporaneous.

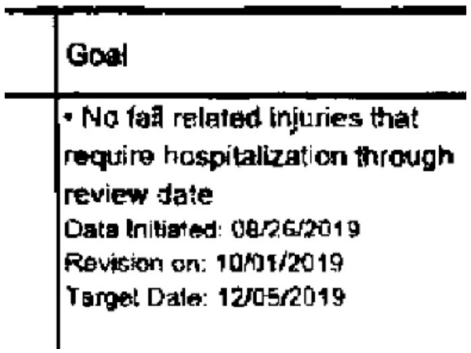
The care plan had been generated only after the resident's discharge and subsequent death. The discrepancy was not immediately visible because the EHR system had been configured to suppress a critical metadata field—the "Created On" timestamp—from all printed outputs. This was not a redaction. The field was systematically excluded. What remained was a curated record reflecting only a "Date Initiated," thereby conveying the false appearance of contemporaneity.[7]

The defense offered shifting explanations—first denying the audit trail existed, then attributing it to a third-party vendor, and ultimately claiming it was not preserved in the ordinary course of business. The trial court rejected these representations. It found that the defendants maintained an accessible electronic audit trail—one that could be produced "by clicking a few buttons"—and imposed coercive contempt sanctions of $1,000 per day, escalating to $5,000 per day, until compliance was achieved. Quickly, the facility produced 1,145 pages of audit trail logs.[8] The production confirmed what the printed records had concealed.

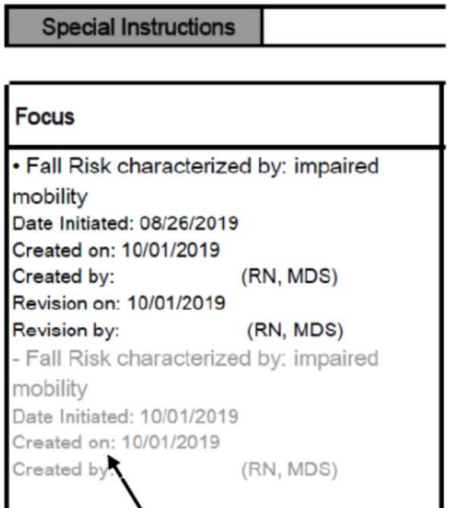
The trial court also ordered a live inspection of the EHR system.[9] The defendants sought appellate relief, first in the Eighth District Court of Appeals and then in the Supreme Court of Ohio. Both efforts failed.[10] Within days of the Supreme Court's denial of jurisdiction, additional record materials were produced. Those materials established, conclusively, that the care plan had been backdated.

The family's account was not merely plausible. It was correct. The contrast between the records produced before inspection and those produced after court intervention is shown below:

BEFORE INSPECTION:



AFTER ORDERS: [11]



LESSON 2 *If a party represents that no audit trail exists, verify that claim independently by consulting the Office of the National Coordinator for Health Information Technology's Certified Health IT Product List (CHPL) at chpl.healthit.gov, the federal repository for EHR certification standards. Search the CHPL for the defendant's EMR software by name and review whether it reflects compliance with § 170.315(d)(3) (Audit Report(s)) under the Cures Update—as it almost invariably does—because that certification provides independent, government-sourced evidence that audit trail functionality exists and is capable of production. It directly undercuts any claim that such data does not exist and should be cited in support of a motion to compel.*

Matter Two: The Report That Preceded Surgery

A second EHR inspection in another case revealed a defect not in the content of the record, but in its chronology. The timeline requires no interpretation:

12:22 p.m. *— An operative report is electronically signed by the treating surgeon. The report states the surgery has been completed. It documents clinical findings. It describes what was observed. It specifies the quantity of tissue removed from the operative site.*

12:38 p.m. *— The surgery actually begins.*[12]

As set forth in the pleadings on the public docket, the operative report was signed, finalized, and placed in the permanent medical record sixteen minutes before the first incision. The surgeon documented findings from a procedure that had not yet occurred. The timestamp was system-generated, tamper-proof, and federally certified to be accurate under 45 C.F.R. § 170.315(g)(7), which requires synchronization to Network Time Protocol standards.[13]

That timestamp alone would have been enough. But it was not the only discrepancy. The original operative report — signed at 12:22 p.m. — documented a specific quantity of tissue removed from the operative site. After surgery concluded, a different operative report was created. The revised report documented a quantity approximately forty percent smaller. Two operative reports for the same procedure: one signed before surgery began, one created after it ended, each recording a materially different account of what was done.

In discovery, the defendant health system represented to the court that its production was complete. That representation proved inaccurate. The day before the plaintiff's deposition was scheduled to begin, the court entered an order requiring production of additional records by 10:00 a.m. the following morning — with sanctions of $100 per day for noncompliance.[14] The court thereafter ordered a live inspection of the EHR. The inspection was conducted pursuant to an agreed protocol.[15]

The 12:22 operative report was not in the defendant health system's document production. It surfaced in the records of the co-defendant, complete with a fax transmission timestamp of 12:25 p.m., thirteen minutes before the surgery began. The co-defendant, for its part, did not have the second report in its production. Each defendant had produced one version. Neither had produced both.[16]

Individually, each production looked like a complete medical record — correct date, correct provider, correct format. Only the timestamp revealed when the document had actually been created. The inspection revealed that BOTH versions of the operative report existed in the hospital's EHR.

> *"Documentation created before care and treatment are provided is false documentation. In more than a thousand cases reviewed across fourteen years of forensic audit trail analysis, I have never encountered an operative report created, signed, and made part of the medical record prior to a procedure." — Expert report filed in the litigation.*[17]

LESSON 3 *In every surgical case, counsel should ask their forensic expert a simple question: what are the creation timestamps for each operative procedure entry, how do those timestamps compare to the anesthesia times, and do any entries predate the scheduled or actual start of the procedure? This question is inexpensive to pose and straightforward to answer, yet it can be outcome-determinative—here, it was. Its significance, however, would not have been fully realized without both expert analysis and a system-level inspection.*

LESSON 4 *When multiple defendants are involved, serve inspection requests on each and cross-reference every production against the others and against the live system. Discrepancies do not hide under this approach—they surface. Incomplete or selective productions become immediately apparent when measured against parallel productions and the system itself. Here, that comparison, combined with direct inspection, exposed the existence of two divergent operative reports within the hospital EHR—records that did not reconcile and would not have been identified through any single production alone.*

Matter Three: Eight Hundred Forty-Five Pages Hidden in Plain Sight

Inspection Three—the matter introduced at the outset—illustrates the problem in its most concrete form. Comprehensive discovery was served at the outset: audit trails from every EHR platform and revision histories for every provider note. Defense counsel repeatedly certified production as complete after multiple rounds of supplementation. The trial court entered a stipulated order—signed by both counsel—requiring full compliance.[18]

By the time of a subsequent hearing, material components of that order remained unfulfilled.[19] As the court made clear, the issue was not what had been produced, but what had not.[20] A forensic expert was retained for a specific purpose: to analyze the EHR systems and identify the gap between what existed and what had been produced.[21] She did exactly that. Against that backdrop, the prospect of a live inspection was addressed on the record, and the defendants ultimately agreed to proceed pursuant to a defined protocol.[22]

Unlike most inspections, which are completed within a day, this inspection extended across three days. What the forensic expert located—within the defendants' own EHR systems, never reached by any prior production query—required 19.75 hours to identify and document.[23] The burden was not the inspection. The burden was the omission. Civ.R. 37(B)(3) turned that omission into accountability.

The results were not marginal. They included: Twenty-three note revision histories previously represented as non-existent; forty-five complete infusion encounter records, including associated treatment plans; a key canceled surgical imaging order that had never been disclosed; ultrasound images and screening flowsheets omitted from every encounter summary produced in discovery; and documents residing in an archived prior version of the EHR system that had not migrated to

the current instance.[24] That final category reflects a problem recognized in the technical literature: when EHR systems are upgraded, data may not transfer completely, leaving records accessible only through legacy systems.

The court's Sanctions Order found that defendants had failed to comply with the stipulated discovery order and the governing principles of discovery, and it required payment of all fees and expenses associated with the inspection pursuant to Ohio Civ.R. 37(B)(3).[25] The parties subsequently agreed upon the sanctions amount of $221,937.98.[26]

That figure answers a recurring objection: live inspection is often labeled disproportionate, burdensome, or beyond the scope of discovery. The record demonstrates otherwise.

> **LESSON 5** *"Complete production" is a subjective assertion dressed as fact. It reflects what counsel represents, not what the system contains. If a production appears thin, unusually clean, or omits records that should exist, obtain a forensic audit analysis and, if supported, promptly seek a live inspection through a motion to compel. It is not a last resort.*

Matter Four: The Audit Trail and the Envelope

The patient had died. His estate brought suit for malpractice and wrongful death. Subsequent amendments added a claim that the defendants had altered the decedent's medical records to avoid liability.[27]

Years after his death and during the course of litigation, the decedent's widow received an envelope in the mail. It had been sent from the office of one of the defendant physicians. Inside was a copy of a critical imaging study—one of the central evidentiary documents in the case. No explanation accompanied it. The significance of that party-to-party direct communication would become clear only after the audit trail was produced and analyzed, revealing who had accessed the record, and when, in the day immediately preceding the mailing.[28]

From the outset, the discovery request was direct. Plaintiff served a notice of videotaped deposition under Civ.R. 30(B)(5) together with a Civ.R. 34 request seeking inspection of the live EHR system, including remote access sufficient to view the decedent's records within the system itself.[29] The defendants moved for a protective order. They argued that real-time access to the EHR system would invade privacy and confidentiality, expose protected health information, and impose an undue and disproportionate burden.[30] The trial court rejected those arguments. It denied the protective order and ordered that defendants provide access to the decedent's electronic medical record through a virtual inspection, subject to a protective protocol and privacy safeguards to be agreed upon by the parties.[31]

The defendants pursued multiple interlocutory appeals. Each was dismissed for lack of a final, appealable order.[32] The appellate court's reasoning was direct. The inspection order did not involve privileged or confidential information within the meaning of R.C. 2505.02(B)(4) because the protocol required that defendants control the system navigation, preapprove screenshots, and submit disputed material for *in-camera* review before disclosure. Blanket assertions of privilege were insufficient. Orders providing for *in-camera* inspection are not final, appealable orders.[33]

The inspection proceeded pursuant to court order and protocol and revealed records that had not been previously produced. As set forth on the public docket, the inspection exposed the scale of the omission: 3,826 pages of medical records and 10,012,594 audit trail data points.[34] Deposition testimony established that these records were not missing or unavailable—they had remained in the defendants' systems for years and were capable of production when originally requested.[35]

The audit trail further identified who had accessed the decedent's record on the dates that mattered. The defendant physician had done so, as had a member of the care team who had not previously been central to the litigation. Deposition testimony established that this access occurred in the presence of outside defense counsel—the same counsel who had argued, both in the trial court and across three appellate proceedings, that plaintiff counsel's access of a hospital's EHR system posed an unacceptable risk to security and confidentiality.[36]

ASTM E2147-18 is explicit and leaves no room for ambiguity: access to a patient's record "by any means"—including access by attorneys, risk management, or similar personnel—is not privileged and must be "fully transparent and disclosed." The standard further requires that audit logs capture and preserve a complete, time-stamped record of all such access as part of the permanent medical record itself. Against that backdrop, three rounds of appellate litigation were undertaken to prevent disclosure of precisely that information. All three were dismissed.[37]

> **LESSON 6** *In every hospital case, demand the master IT integration map in your first request for production. It is the table of contents for the discovery you should be conducting; without it, you are searching for documents in rooms you do not know exist. A hospital may operate multiple software systems for a single patient's care—each with its own data, its own audit trail, and each requiring its own demand. The integration map tells you what to ask for.*

Matter Five: The Florida Court Order — The Third-Party Scribe

The fifth matter in this article is not an EHR inspection. The records at issue never resided within the hospital's EHR in the first place.

In this case, the subsequent treating physician recorded patient encounters in full on her cell phone. The patient was aware that the visits were being recorded. What was not disclosed was where those recordings went. The audio was not retained by the physician or the health system. It was transmitted to a third-party vendor—ScribeAmerica—where it was processed outside the hospital's electronic health record environment.[38]

The documentation process operated entirely off system. Once recorded, the audio was uploaded to ScribeAmerica's platform, where a remote scribe—working from the recording rather than from presence in the room—generated a clinical note and transmitted it back to the physician for review and editing before it was signed into the medical record. The version that entered the permanent record was the edited version.[39]

In discovery, a critical progress note reflected that it had been amended. After much digging, we learned the underlying materials—the audio recording and the contemporaneous transcription from which the note was created—were no longer available. ScribeAmerica's corporate representative testified that audio recordings and transcripts are deleted within seventy-two hours after completion of the note, and that audit logs are automatically deleted after approximately 400 days.[40] A preservation letter was sent to the defendant health system specifically requesting preservation of encounter recordings. ScribeAmerica did not receive that request until April 2025—well after the relevant encounters—and by that time, any audio, transcripts, and audit logs had already been deleted pursuant to standard retention protocols.[41]

Because ScribeAmerica is a Florida-based entity, an Ohio subpoena could not compel testimony. A Florida court order was required. After hearing argument, the Circuit Court for Palm Beach County denied ScribeAmerica's motion to quash and permitted a limited corporate deposition directed to three issues: what records existed, when they ceased to exist, and when ScribeAmerica became aware of the underlying Ohio litigation.[42]

That deposition confirmed the practical effect of the retention policy. By the time ScribeAmerica was asked to search for records, it had no audio recordings, no transcripts, and no audit logs from the relevant encounters.[43] The witness further testified that once deleted, those materials cannot be recovered.[44] What remained was the amended note—the final version entered into the medical record. What was lost was the most contemporaneous account of the encounter: the physician's recorded words, the verbatim transcription, and any system-level record of how the note was created or changed.

The record never remained where the law assumed it would be—and then it was gone.

> **LESSON 7** *On every intake call, identify whether any third-party documentation was used during clinical encounters, including human scribes and recorded interactions. Ask by name—ScribeAmerica, Aquity Solutions, iScribe, PhysAssist, ProScribe, Scribe-X, and similar vendors—and determine whether any portion of the clinical record was created or stored outside the hospital's EHR. The contemporaneous record of what was said and done in the exam room may not reside within the hospital's production at all. It may instead be maintained by a third-party vendor, subject to separate retention policies, and require independent legal process to obtain.*

> **LESSON 8** *Ohio Civ. R. 45 does not reach an out-of-state entity. The Uniform Interstate Depositions and Discovery Act, adopted in Ohio at R.C. § 2319.09, provides the mechanism for third-party discovery across state lines, but it requires additional procedural steps and, critically, time. That delay carries risk: a scribe vendor's retention policies continue to run while counsel determines the proper vehicle for enforcement. Third-party vendor discovery must therefore be built into the case strategy from the outset, not after gaps in production are identified.*

III. What Comes Next: The AI in the Room

The scribe problem—critical documentation existing outside the EHR, governed by private retention policies, and invisible to standard discovery—is about to become more complex. Human scribes are being replaced by software. Ambient AI documentation tools are already in widespread clinical use. These systems operate outside the EHR, generating and refining documentation before a finalized note is entered into the record. The underlying data—audio, drafts, edits, and system interactions—remains with the vendor, subject to private retention policies and often outside existing audit frameworks.

The IEEE has identified this gap with precision. In a November 2025 Industry Connections workgroup analysis addressing audit trail and audit data standards, the group concluded that existing frameworks no longer reflect the realities of modern, AI-integrated healthcare systems. The analysis specifically calls for updated audit standards capable of capturing "AI access, inference, decision outputs, and interactions with clinical workflows," emphasizing that auditability must apply regardless of whether the system is rule-based or data-driven. It further recognizes a critical structural omission: patient care information is increasingly generated and exchanged through messaging platforms, collaborative tools, and external systems, yet "existing audit trail specifications and standards do not cover these ephemeral messaging platforms in the healthcare context."[45] As of this writing, no federal certification requirement governs ambient or AI-assisted documentation tools, no comprehensive audit mandate extends to external or ephemeral systems, and no uniform retention requirement applies to the data they generate. The consequence is structural: the modern clinical record is increasingly created outside the certified EHR, beyond existing audit frameworks, and subject to private control. In the cases presented here, the missing record is not an anomaly—it is the predictable product of systems not designed to preserve what they create.

The same problem exists within the EHR itself. Clinical decisions are often communicated through integrated messaging systems that do not retain the underlying exchange. The instruction may be documented. The reasoning is not. In some systems, messages can be configured to auto-delete after they are read—ephemeral communications embedded within certified EHR infrastructure. These exchanges are not captured in standard productions and are recoverable only if identified and preserved before deletion.

At present, no comprehensive, enforceable standard governs how EHR-integrated messaging is created, retained, audited, or produced. The result is structural: critical components of clinical decision-making may occur within certified EHR systems and yet remain outside any durable, auditable, or discoverable record. In practice, this means the most contemporaneous version of the clinical encounter may never enter the medical record at all.

> *The gap between what the AI generated and what the physician signed is where the truth lives.*

> **LESSON 9** *In every new case, before serving your first records request, determine whether any ambient AI documentation system was used during clinical encounters. Ask by name—Nuance DAX, DAX Copilot, Abridge, Suki, Nabla, DeepScribe, Augmedix—and do not rely on the facility to volunteer the information. These systems generate clinical documentation from recorded encounters and often operate outside the hospital's certified EHR, with data stored in separate vendor environments. The inquiry must be directed beyond written discovery: ask the treating physician in deposition and the hospital's IT administrator directly. The existence of such a system may define the scope of discoverable evidence and, in many cases, may be the most consequential fact identified in the early stages of litigation.*

> **LESSON 10** *Send a preservation letter to the AI vendor the day its use is identified and concurrently notify the hospital of its obligation to preserve all third-party documentation within its possession, custody, or control, including data maintained by vendors acting on its behalf. The hospital's EHR operates under retention policies shaped by federal regulation; the AI vendor's retention policy does not. Whatever its terms, the clock is already running. Unless the vendor receives a litigation hold before that period expires, the underlying data—often including the original audio or source inputs—may be automatically and permanently deleted. Once lost, it cannot be reconstructed.*

IV. The Expert You Need

I will be direct about this, because the wrong expert will undermine the work you have done to get inside the system.

Medical record review is a common skill. Forensic audit trail analysis is not. The right expert has specific, demonstrable experience with EHR audit data—not records generally. She must know how EPIC generates timestamp data differently from Cerner. How PointClickCare structures its audit logs relative to Soarian. What a copy-forward event looks like in the raw audit data versus an original entry. How the system records a note that was auto populated from a template versus one that was typed. How to read a workstation identifier and understand from which terminal and location a given action originated. Ask specifically: How many EHR platforms have you worked with? Which ones? How many live inspections

have you conducted? Have you identified pre-documentation — entries timestamped before the events they describe? Have you worked with post-death access data? With copy-forward analysis? Have you been deposed or testified in court on these specific topics? That depth of specialized experience is not a luxury. It is the difference between finding the evidence and walking past it.

And the expert must be able to explain it to a jury. Timestamps, VisitIDs, NTP synchronization, workstation identifiers — none of it means anything to the people in the jury box. The expert who can look at the jury and say, simply and clearly: the operative report says the surgery was documented at 12:22, the surgery did not begin until 12:38, and that is not a clerical error — that expert wins the case. The jargon is for the motion. The plain language is for the verdict.

V. The Threat on the Horizon: HTI-5

This Article concludes with a development that should concern any lawyer litigating medical cases. It threatens to place much of what has been described here beyond reach.

The U.S. Department of Health and Human Services has proposed the HTI-5 rule—formally titled *Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity*—which would eliminate a substantial portion of the current certification requirements for electronic health record systems.[46] The proposal removes federal guardrails without first establishing updated standards to replace them. It is deregulation without a successor framework. The practical effect is straightforward: the regulatory floor is being considered for removal before a new one has been built.

Among the criteria at risk is 45 C.F.R. § 170.315(d)(3), which requires certified EHR systems to generate complete, tamper-resistant, machine-readable audit trails. These are not technical formalities. They determine whether the underlying data exists at all. Every case described in this Article turned on data the audit trail either preserved or failed to preserve. Remove the requirement to generate that data, and the consequence is not merely regulatory—it is evidentiary. It changes what can be proved.

If certification requirements are reduced, the standards they enforce must first be modernized. That modernization must address AI-generated content, interoperability across platforms, metadata transparency, retention of ephemeral communications and scribe data, and audit coverage for systems operating outside the certified EHR. Those standards do not yet exist in enforceable form. The IEEE has identified these gaps and called for expanded measures of data completeness, traceability, and auditability.

For more than two decades, the structure of electronic records has placed certain critical information beyond reach. HTI-5 risks transforming that reality from a flaw in the system into its design.

VI. Conclusion

It took years of litigation — multiple court-ordered inspections, three trips to the Eighth District, one to the Supreme Court of Ohio, and a $221,937.98 check — to confirm what my instincts had long told me: the chart you were handed is not the chart that exists.

Every inspection has proved it. The system holds what the paper does not — and someone is counting on no one to look.

Know the system. Know what it holds. And go get it.

*IEEE: A Note on this Standards Authority

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest technical professional organization, with more than 400,000 members in over 160 countries. Its Standards Association develops widely adopted global technical standards, including those governing Wi-Fi (IEEE 802.11), Ethernet (IEEE 802.3), and electromagnetic safety in medical environments (IEEE C95.1).

In 2023, the IEEE Standards Association launched an international Industry Connections workgroup focused on data quality in electronic health records: the ICAID Workgroup on Data Quality Standards of Electronic Health Records. The workgroup includes engineers, informaticists, clinicians, health system architects, and legal practitioners from institutions across the United States and internationally.

Its published outputs are peer-reviewed working documents that provide the definitional and evidentiary foundation for standards currently under development in this area. The materials cited in this Article are publicly available through the IEEE Standards Association.

About the Author

Susan E. Petersen, Esq. is the founding partner of Petersen & Petersen in Chardon, Ohio, where she has represented catastrophically injured individuals and their families for nearly three decades. Her practice focuses on complex medical negligence litigation, with particular emphasis on electronic health record discovery and audit trail analysis. She has served

Susan E. Petersen, doing Zoom inspection.

as lead counsel in cases resulting in significant settlements and verdicts and has obtained court-ordered forensic inspections of live EHR systems across multiple platforms, including EPIC, Soarian, PointClickCare, and Cerner.

Petersen has presented nationally on issues of EHR data integrity and discovery. In 2025, she was invited to join the IEEE Standards Association Industry Connections Activity on Improved Data Quality of Electronic Health Records (ICAID) Workgroup. She is a founding member of the Health Access and Records Protection (HARP) Institute (2026) and argued before the Supreme Court of Ohio in *Paganini v. Cataract Eye Center of Cleveland* (Feb. 10, 2026).

She is the recipient of the 2024 CATA Excellence in Advocacy Award and the 2024 Ohio Association for Justice J. Thomas Henretta Distinguished Advocate Award and was inducted into the Cleveland-Marshall College of Law Hall of Fame in 2023. ■

End Notes

1. Case No. CV-2023-09-3525, Sanctions Order, at *1 (Ohio Ct. Com. Pl., Summit Cnty. Oct. 7, 2025) (finding that defendants failed to comply with the court's Jan. 29, 2025, order and applicable discovery obligations and ordering payment of inspection-related expenses pursuant to Ohio R. Civ. P. 37(B)(3)).
2. Case No. CV-25-113720, Affidavit of Susan E. Petersen, Esq. ¶ 4 (Ohio Ct. Com. Pl., Cuyahoga Cnty. filed Mar. 13, 2026) (attesting that the Summa defendants "paid the full agreed sanctions amount of $221,937.98" in satisfaction of the Summit County sanctions award); see also Case No. CV-2023-09-3525, Journal Entry, at *1 (Ohio Ct. Com. Pl., Summit Cnty. Feb. 27, 2026) (reflecting that the sanctions amount was resolved by agreement and ordering payment by Mar. 6, 2026).
3. Susan E. Petersen, *Overcoming Objections to Production of a Complete and Unredacted Audit Trail*, CATA News, Spring 2023, at 10–11 (describing post-production audit trail disclosures revealing previously concealed record information); https://clevelandtrialattorneys.org/wp-content/uploads/2023/06/CATA-NEWS-26th-Issue-Final-Proof-Spring-2023.pdf.
4. No. 113288, ¶¶ 1–2 (Ohio Ct. App. Dec. 12, 2024) ("We dismiss the appeal for lack of jurisdiction."; dismissing interlocutory challenge to order permitting inspection of electronic medical records); see also *Id.* ¶ 14 ("An order that leaves issues unresolved and contemplates future action is not a final, appealable order."); No. 110373 (Ohio Ct. App. May 5, 2021) (denying reconsideration following dismissal of interlocutory appeal arising from discovery protocol governing electronic medical record inspection).
5. Varadraj Gurupur, *Understanding an Electronic Health Record System and Its Applicable Data Quality Measures*, IEEE SA Industry Connections (Mar. 29, 2024), at 6–7 (explaining that EHR systems vary across healthcare settings and implementations, leading to differences in data structure, format, and interpretation).
6. Varadraj Gurupur, *Understanding an Electronic Health Record System and Its Applicable Data Quality Measures*, IEEE SA Industry Connections (Mar. 29, 2024), at 6–7 (explaining that EHR systems vary across healthcare settings and implementations, leading to differences in data structure, format, and interpretation).
7. Case No. CV-20-934555, Plaintiff's Trial Brief (Ohio Ct. C.P., Cuyahoga Cnty. filed Sept. 21, 2021) (describing post-discharge creation of fall risk care plan and exclusion of "Created On" timestamp from printed records, thereby creating the appearance of contemporaneity); see also Susan E. Petersen, *Overcoming Objections to Production of a Complete and Unredacted Audit Trail*, CATA News, Spring 2023, at 10 (describing production of a fall risk care plan that excluded the "Created On" date, later revealed to have been generated after the patient's discharge and death).
8. Case No. CV-20-934555, Journal Entry (Ohio Ct. C.P., Cuyahoga Cnty. filed June 24, 2021) (finding defendants in contempt for failure to produce audit trail information and imposing sanctions of $1,000 per day, escalating to $5,000 per day; further finding that defendants maintained audit trail information electronically and could produce it "by clicking a few buttons") ; see also *Id.* (ordering production of audit trail information responsive to requests for production).
9. Case No. CV-20-934555, Journal Entry (Ohio Ct. C.P., Cuyahoga Cnty. Mar. 11, 2021) (granting, inter alia, a virtual inspection of the plaintiff's electronic medical chart within the PointClickCare system).
10. No. 110373 (Ohio Ct. App. 2021) (dismissing interlocutory appeal arising from discovery order governing EHR inspection); No. 2021-0780 (Ohio Aug. 17, 2021) (declining jurisdiction) ("the court declines to accept jurisdiction of the appeal").
11. Susan E. Petersen, *Overcoming Objections to Production of a Complete and Unredacted Audit Trail*, CATA News, Spring 2023, at 10–11 (describing post-production audit trail disclosures revealing previously concealed record information); https://clevelandtrialattorneys.org/wp-content/uploads/2023/06/CATA-NEWS-26th-Issue-Final-Proof-Spring-2023.pdf.
12. Case No. CV-23-983480, Plaintiffs' Final Pretrial Statement, (Ohio Ct. C.P., Cuyahoga Cnty., filed Sept. 2, 2025), at 5–6 (describing operative report electronically signed at 12:22 p.m. prior to surgery beginning at 12:38 p.m., and existence of differing operative reports documenting inconsistent surgical findings).
13. 45 C.F.R. § 170.315(g)(7). 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/.
14. Case No. CV-23-983480, Journal Entry (Ohio Ct. C.P., Cuyahoga Cnty., Feb. 6, 2025) (ordering production of additional records and imposing sanctions for noncompliance).
15. Case No. CV-23-983480, Journal Entry (Ohio Ct. C.P., Cuyahoga Cnty. Mar. 13, 2025) (Ordering videotaped inspection conducted pursuant to an agreed protocol).
16. Case No. CV-23-983480, Plaintiffs' Final Pretrial Statement, (Ohio Ct. C.P., Cuyahoga Cnty. Sept. 2, 2025), at 5–6 (describing operative report electronically signed at 12:22 p.m. prior to surgery beginning at 12:38 p.m., and existence of differing operative reports documenting inconsistent surgical findings).

17. Case No. CV-23-983480, Plaintiffs' Final Pretrial Statement, (Ohio Ct. C.P., Cuyahoga Cnty. Sept. 2, 2025), at 6 (quoting Expert Report of Michele Gonsman, RN, BSN, ALNC).

18. Case No. CV-2023-09-3525, Stipulated Order, (Ohio Ct. C.P., Summit Cnty. Jan. 29, 2025) (requiring complete production of EHR records, audit trails, and related discovery materials by agreed deadline);

19. Case No. CV-2023-09-3525, Aug. 21, 2025, Tr. of Proceedings at 3–4 (Ohio Ct. C.P., Summit Cnty. Oct. 9, 2025) (court stating that the issue was not what had been produced but what had not and directing complete compliance with outstanding discovery obligations);

20. Case No. CV-2023-09-3525, Aug. 21, 2025, Tr. of Proceedings at 3–4 (Ohio Ct. C.P., Summit Cnty. Oct. 9, 2025) at 5–6 ("I don't care. If there are another 10,000 pages to produce, then you owe them 6,000 pages.")

21. Case No. CV-2023-09-3525, July16, 2025, Tr. of Proceedings at 7–8 (Ohio Ct. C.P., Summit Cnty. Oct. 30, 2025) (counsel stating expert waiting in the wings to testify who plaintiff was forced to retain because gut told her they did not have everything in terms of the records.).

22. Case No. CV-2023-09-3525, Aug. 21, 2025, Tr. of Proceedings at 9–10 (Ohio Ct. C.P., Summit Cnty. Oct. 9, 2025)(agreement to live EHR inspection)

23. Case No. CV-2023-09-3525, Sanctions Order (Ohio Ct. C.P., Summit Cnty. Oct. 7, 2025) (finding that forensic expert required 19.75 hours to identify and document records that had existed within defendants' EHR systems and had never been produced).

24. Case No. CV-2023-09-3525, Sanctions Order (Ohio Ct. C.P., Summit Cnty. Oct. 7, 2025) (finding that 845 pages of previously unproduced medical records—including revision histories, imaging, and treatment records—were identified during inspection and that locating them required 19.75 hours).

25. Case No. CV-2023-09-3525, Sanctions Order (Ohio Ct. C.P., Summit Cnty. Oct. 7, 2025)(issuing sanctions under Civ. R. 37(B)(3).

26. Case No. CV-2023-09-3525, Journal Entry (Ohio Ct. C.P., Summit Cnty. Feb. 27, 2026), (ordering payment of agreed sanctions amount of $221,937.98); see also Case No. CV-25-113720, Affidavit of Susan E. Petersen, Esq., ¶ 4, Ex. Q, Plaintiff's Reply in Support of Motion to Compel Discovery, (Ohio Ct. Com. Pl., Cuyahoga Cnty, Mar. 18, 2026).

27. No. 113288, ¶ 3 (Ohio Ct. App. Dec. 12, 2024) (noting amended complaint included claim that defendants altered medical records to avoid liability).

28. Case No. CV-22-962194, Plaintiff's Reply in Support of Motion for Leave to File Third Amended Complaint, (Ohio C.P. Cuyahoga Cnty Aug. 28, 2024), at 4–7 (describing post-death record access, undisclosed activity within the EMR, and related factual developments).

29. No. 113288, ¶ 4 (Ohio Ct. App. Dec. 12, 2024) (quoting Civ.R. 30(B)(5) notice and Rule 34 request for virtual inspection of EMR).

30. *Id.* ¶ 5.

31. Case No. CV-22-962194, Journal Entry (Ohio C.P. Cuyahoga County June 5, 2023) (denying motion for protective order and ordering virtual inspection subject to protocol; warning of sanctions for noncompliance); No. 113288, ¶¶ 1–2 (Ohio Ct. App. Dec. 12, 2024) (dismissing interlocutory appeal for lack of jurisdiction).

32. No. 113288, ¶¶ 1–2 (Ohio Ct. App. Dec. 12, 2024) (dismissing interlocutory appeal for lack of jurisdiction).

33. *Id.* ¶¶ 1–2, 5 (holding discovery orders governing inspection and protocol are not final appealable orders and rejecting blanket privilege assertions).

34. Case No. CV-22-962194, Plaintiff's Notice of Compliance with October 8, 2024, Judgment Entry; Supplement to Pending Motion to Show Cause; Emergency Motion for Rule 37 Sanctions, (Ohio C.P. Cuyahoga Cnty. Oct. 28, 2024), at 3, 6.

35. Case No. CV-22-962194, Deposition taken on Oct. 25, 2024, at 76–77, 92, 107, (Ohio Ct. C.P., Cuyahoga Ctny Oct. 29, 2024) (testifying that records produced in August 2024 included materials dating back to 2009–2017, that such records should have been produced in response to earlier requests, and that if records existed in the system in 2024, they would have existed in prior years).

36. Case No. CV-22-962194, Plaintiff's Reply in Support of Motion for Leave to File Third Amended Complaint, (Ohio Ct. C.P. Cuyahoga Cnty. Aug. 28, 2024), at 4–7 (describing post-death record access, undisclosed activity within the EMR, and related factual developments).

37. ASTM International. (2018). ASTM E2147-18, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems §§ 1.1, 4.3 (2018) Retrieved from https://www.astm. org/Standards/E2147.htm.

38. Case No. CV-23-983480, Deposition of ScribeAmerica Representative at 23–24, 35–36, Aug. 28, 2025, (Ohio C.P. Cuyahoga Ctny Sept. 10, 2025) (describing recording and remote scribe process through ScribeAmerica platform).

39. *Id.* at 37–39 (testifying that audio recordings and transcripts are deleted within seventy-two hours after note completion and that audit logs are retained for approximately 400 days before automatic deletion).

40. *Id.* at 42–45 (testifying ScribeAmerica first received notice of litigation in April 2025 and confirming deletion and non-recoverability of data).

41. *Id.*

42. Case No. 50-2025-CA-005912 (Fla. Cir. Ct. Aug. 20, 2025), Order at 1–2, (denying motion to quash and limiting deposition to existence, destruction, and notice of records).

43. Case No. CV-23-983480, Deposition of ScribeAmerica Representative at 37-39, Aug. 28, 2025, (Ohio Ct. C.P., Cuyahoga Ctny Sept. 10, 2025) (testifying that audio recordings and transcripts are deleted within seventy-two hours after note completion and that audit logs are retained for approximately 400 days before automatic deletion).

44. *Id.*

45. Tom Jacob, J.D., *Updating ePHI Definitions: Audit Trail and Audit Data*, IEEE SA Industry Connections, IC23-005 Global Data Quality Standards for Electronic Health Records (Nov. 26, 2025), at 10–11 (explaining need to update audit standards to capture AI system activity, including "AI access, inference, decision outputs, and interactions with clinical workflows," and noting that existing audit trail specifications do not cover "ephemeral messaging platforms in the healthcare context"); *Id.* at 5–6 (describing audit data and audit trails as necessary to ensure trustworthiness, authenticity, and completeness of electronic health records): https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11270031.

46. *Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity*, Docket No. ONC-2025-0001 (proposed Dec. 2025), available at https://www.federalregister.gov (U.S. Dep't of Health & Hum. Servs., Office of the Nat'l Coordinator for Health Info. Tech.). The rule was proposed under the office's then-current designation of "ASTP/ONC," a dual title adopted in July 2024 when ONC was redesignated as the Office of the Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology. That designation was reversed effective Mar. 31, 2026, returning the agency to its original name, ONC. See Office of the Nat'l Coordinator for Health Info. Tech., Reorganization, 91 Fed. Reg. ___ (Mar. 31, 2026). The rule's title reflects the agency's name at the time of proposal; the agency is now again referred to as ONC.