

Peter J. Pizzi (025251978)

Deana I. Davis (406332022)

WALSH PIZZI O'REILLY FALANGA LLP

Three Gateway Center

100 Mulberry Street, 15th Floor

Newark, New Jersey 07102

Tel: (973) 757-1100

ppizzi@walsh.law

ddavis@walsh.law

eDiscovery Counsel for Defendant, HMH Hospitals Corporation

d/b/a Jersey Shore University Medical Center

CANDACE MOSCHELLA, as Administrator
Ad Prosequendum for the Estate of
Alexandrianna Lowe, and CANDACE
MOSCHELLA, individually,

Plaintiffs,

v.

HACKENSACK MERIDIAN HEALTH
HOSPITALS CORPORATION; HMH
HOSPITALS CORPORATION; DR. MICHAEL
P. CARSON; DR. VIKAS SINGH; DR.
SHRINIL PATEL; DR. SHEREEN DAHAB;
DR. HAVILA GANDHI; DR. ERISA ALIA;
ALEXIS CAVEZZA, RN; NANCY MAINA,
RN; MARINA KERBER, RN; WINSTON
BROWN, RN; and JOHN and JANE DOES 1-
98,

Defendants.

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION: MONMOUTH COUNTY

Docket No.: MON-L-2347-20

CIVIL ACTION

ORDER

THIS MATTER, having been brought before the Court on the motion of Walsh Pizzi O'Reilly Falanga, LLP, eDiscovery Counsel for Defendant HMH Hospitals Corporation d/b/a Jersey Shore University Medical Center ("HMH"), in the above captioned matter, seeking the entry of an Order to Enforce the entry of a Discovery Confidentiality Order and the Court, having considered the papers submitted, and for sufficient cause shown:

IT IS, on this 4th day of December 2025, **ORDERED** that Defendants Motion for a Discovery Confidentiality Order is hereby **GRANTED**; and it is further

ORDERED that Defendant HMH shall submit an amended “Exhibit C” indicating that the discovery confidentiality order is not by consent of all parties; and it is further

ORDERED that the filing of this Order onto eCourts shall constitute service upon all counsel of record. Pursuant to Rule 1:5-1(a), a copy of this Order shall be served on all parties not served electronically, nor served personally in Court on this date, by the Movant within seven (7) days of the date of this Order.

The Motion is hereby **GRANTED** for the reasons set forth in the attached Rider.

/s/ Kathleen A. Sheedy
Hon. Kathleen A. Sheedy, J.S.C.

- ☒ Opposed
- ☒ Unopposed

Statement of Reasons Under R. 1:6-2(f)

Re: Moschella v. HMH Hospitals Corporation
Docket No.: MON-L-2347-20
Motion Type: Motion for Protective Order and Cross Motion to Compel
Return Date: October 10, 2025

This matter comes before the Court by way of Defendant HMH Hospitals Corporation, d/b/a Jersey Shore University Medical Center (individually, “HMH”)’s Motion for Protective Order. Plaintiffs Candace Moschella, as Administrator *Ad Prosequendum* for the Estate of Alexandrianna Lowe and individually (“Plaintiffs”) file a Cross-Motion to Compel Discovery. Defendant Dr. Carson and HMH Hospitals Corporation, d/b/a Jersey Shore University Medical Center filed an Opposition to the Cross-Motion and Reply to Plaintiffs’ Opposition. Both Plaintiff and Defendant HMH filed letters providing the Court with a copy of Judge Batista’s decision in *Arroyo v HUMC ESX-L-7679-22* and their request that I follow and ignore that decision.

Facts

This case arises out of an allegation of medical malpractice wherein Plaintiff alleges that Defendants’ negligent care proximately caused the untimely death of decedent Alexandrianna Rowe.

Legal Argument

HMH Defendants’ Argument in Support of the Motion for Protective Order

a. Audit Trails, Which are Not Part of the Medical Record, Contain Complex Healthcare and Proprietary Information That Must be Protected by a DCO

Audit trails of the patient’s medical record are not part of the patient’s medical record itself because they do not drive patient care. Rather, audit trails are a tool created to ensure compliance with HIPAA and its well-known privacy rule, as well as other regulatory regimes in the highly regulated healthcare environment. 45 C.F.R. §164.524(a) provides that “an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set.” The “designated record set” comprises records “[u]sed, in whole or in part, by or for the covered entity to make decisions about individuals.” *Id.* Metadata does not exist when doctors and nurses are making decisions about patient care; it is information, such as the time and amendment to the specific entry of protected health information, not protected health information, which itself is the basis for the decisions about the patient.

While discovery in this State is broad, the Courts of this State are open to the public, and unnecessary exposure of HMH’s employees and internal recordkeeping information would cause undue burden, unpredictable harm, and unnecessary expense for information that is not part of the patient’s medical record. Rule 4:10-3, for example, exists to forestall such exposure.

An audit trail contains confidential and proprietary business information of HMH created by the healthcare operating system that HMH licenses from a third party, which is referred to as its electronic medical or health record system (“EHR”). HMH cannot produce proprietary and sensitive business information, such as EHR audit trails, without the protection of a DCO. The

audit trail file of the electronic medical record, for example, presents tens of thousands of rows of data concerning access to the medical record and annotates those access with the following fields of information:

Time Stamp (EST)	MRN [Medical Record Number]
Access by Name [employee]	Patient ID
Access by ID [employee]	Encounter
Event	Platform
Event Area	Login Department
Type	Workstation
Patient Name	Associated Data

None of this data is part of the patient’s medical record. Whenever a healthcare professional accesses the EHR, a line of data in the patient audit trail is created showing the date and time, information about the area within the EHR accessed, and other metadata. Each distinct item accessed in the EHR creates an audit trail line per access, which means that a single EHR session often creates hundreds of lines of audit trail data.

No sophisticated healthcare provider or other business operating in this State would tolerate production in litigation of the fruits of its information system without appropriate protections against use outside the bounds of the litigation itself. The Health Insurance Portability and Accountability Act (“HIPAA”) requires no less. The stringent HIPAA security rule requires administrative safeguards, physical safeguards, and technical safeguards. Here, the HIPAA administrative safeguard of a business associate agreement (“BAA”) is not in place with Plaintiffs’ counsel so the safeguard of a confidentiality order from the Court must be relied upon.

Without a BAA or a DCO in place, information about HMH’s licensed EHR platform that is disclosed to the public necessarily increases the risk of cyber intrusion by threat actors. In 2023, an HMH-related provider suffered a ransomware attack and was forced to turn away patients. HMH itself also suffered a ransomware attack right before the COVID-19 pandemic. Threats are constant and ever-changing as guidance from the Cybersecurity Infrastructure and Security Agency makes clear. HMH’s deployment of the Epic platform serves as the backbone of its statewide operations and HMH is obligated to protect that existential information system from threat actors if not through a HIPAA-compliant BAA, then through a DCO.

Accordingly, HMH respectfully urges that the Court enter a DCO which would prohibit commercial or other use of any metadata production by HMH except for the purpose of this case. A DCO of this kind is routinely entered into healthcare litigation of this kind, each time HMH is asked to produce an audit trail. A DCO is a standard procedure in any litigation in which the product of sophisticated business information systems is part of the discovery process because such records invariably disclose, reveal, or reflect confidential and proprietary business information. No business organization, whether for profit, or like HMH – not-for-profit, would produce the fruits of the organization’s electronic information and operating system, which here contain employee information and proprietary data points unique to HMH – without an agreement and court order providing that the information will be used only for the prosecution and defense of the case in question with confidentiality maintained.

b. New Jersey Court Decisions on Metadata Provide for Appropriate Protections Concerning Discovery of Metadata

The entry of a DCO has been repeatedly ordered and affirmed by the Courts of this State. Moreover, Plaintiff's counsel entered into a prior DCO with HMH in a separate matter to obtain HMH's proprietary audit trails. HMH merely seeks entry of a DCO so that HMH's proprietary information is not made public.

In Estate of Lasiw by Lasiw v. Perreira, Judge Messano identified the DCO as a tool which facilitated, not impeded, metadata discovery in that case:

[C]oncerns [about confidential information] could be adequately addressed in a confidentiality agreement entered by the parties; from the appellate records, it appears one already exists. See also N.J.R.E. 530(c)(4) and (5) (regarding non-waiver agreements as to disclosure of discovery covered by the attorney-client and work-product privileges and the enforceability of same by the court); R. 4:10-2(e) (allowing for assertion of privilege for discovery already produced).

457 N.J. Super. 378, 402 (App. Div. 2023).

Other courts have ordered DCOs to be entered, including this Court in the matter of Hammock v. HMH, et al. (MON-L-3760-21). Subsequently, on January 19, 2024, in Estate of Kyle R. Mumford, et al. v. HMH, et al., UNN-L-1114-23, Assignment Judge Lisa M. Walsh granted HMH's motion for a DCO. Then, on June 24, 2024, in Arroyo v. HMH, et al., ESX-L-7679-22, the Court granted HMH's motion for a DCO. In fact, in Arroyo, the plaintiff's counsel filed a motion for leave to appeal the Court's decision regarding the DCO, which the Appellate Division denied, and the Court entered the DCO on the docket on July 26, 2024.

HMH is willing to produce the requested discovery by Plaintiff's counsel, but merely requests that Plaintiffs' counsel not disclose the information conveyed in the audit trails beyond the present case. The undue burden necessitating keeping the audit trail protected from public access includes the insights the metadata may provide into HMH's employee and record-keeping systems and proprietary functionality of the Epic EHR platform. A DCO is a minimal measure aimed at advancing discovery and disclosure to Plaintiffs while mitigating the risks, and therefore, undue burden on the healthcare provider facing unprecedented attacks yet with a mission of providing continuous care and protecting PHI despite threats to continuous service by ransomware exploits and similar electronic intrusions.

For these reasons, the Court should grant HMH's motion for entry of a discovery confidentiality order within this matter to ensure the sensitive information HMH produces remains within the bounds of this litigation.

Plaintiffs' Argument in Opposition and in Support of the Cross-Motion to Compel Discovery

By email dated January 20, 2025, Plaintiffs' counsel served initial discovery demands, which included Form Interrogatories, a Demand for Discovery of Insurance Coverage and a Notice to Produce. To date, counsel for the Carson and HMH Defendants have only provided answers to

Form C and C(3) Interrogatories and Demand for Discovery of Insurance Coverage.

No response to the Notice to Produce served on January 20, 2025 has been provided to date nor has there been any indication as to when Plaintiff can anticipate same despite the Court's previous Case Management Order setting a discovery schedule.

On May 21, 2025, Plaintiffs' counsel spoke with Mr. Liberatore and reminded him that responses to Plaintiffs' discovery requests were outstanding. He asked that Plaintiffs' counsel re-send the requests and Plaintiffs' counsel did so that same day. Plaintiffs' counsel followed up by letter and email with Mr. Liberatore dated July 3, 2025. On July 8, 2025, Mr. Liberatore called Plaintiffs' counsel to discuss the meet-and-confer obligations and advised Plaintiffs' counsel not to file a discovery motion and that he was working on dates for the inspection.

Despite the prior conversation, on July 24, 2025, Mr. Liberatore sent a letter to Plaintiffs' counsel objecting to the production of the audit trail and electronic medical record. During a case management conference, Plaintiffs' counsel raised this issue. The Court indicated that a party could request a meet-and-confer before the Court. Given the about-face from July 8, 2025 to July 24, 2025, Plaintiffs' counsel availed herself of that opportunity and requested the meet and confer before Judge Sheedy by letter dated August 1, 2025.

Mr. Pizzi then submitted a response dated August 4, 2025 to which Plaintiffs' counsel replied that same day. On August 26, 2025, eDiscovery counsel for HMH sent a request to enter into a confidentiality order. Plaintiffs' counsel advised that her client was not authorizing her to enter into a consent order. Thereafter, HMH filed its Motion for Protective Order. This cross-motion now follows in opposition to the confidentiality order and seeking production of documents that are beyond the scope of the request for confidentiality order.

To properly prosecute this matter and obtain meaningful expert reports, Plaintiffs require certified and fully responsive Answers to the Notice to Produce served on January 20, 2025. Plaintiffs respectfully request that their Motion to Compel Discovery be granted.

As HMH and Dr. Carson have provided no basis for failing to provide responses to the Notices to Produce. Pursuant to the Court Rules, Plaintiff is entitled to reasonable costs and fees relating to the cross-motion. Limiting the fee application only to time spent on the cross-motion and not the opposition relating to HMH's confidentiality request, Plaintiff seeks \$500.00, which is one hour of time at counsel's reasonable rate of \$450 per hour for someone with Plaintiffs' counsel's 21 years of experience as a litigator and \$50 for the filing fee.

I. Plaintiff is Entitled to a Response to Her Requests for the Production of Documents

Defendants are obligated to respond to discovery requests. The fundamental theory of New Jersey's judicial system is "that the fullest disclosure of the facts will best lead to the truth and ultimately to the triumph of justice." *In re Selser*, 15 N.J. 393 (1954). Our discovery rules are designed to be "construed liberally in favor of broad pretrial discovery," and are construed liberally to that end. *Estate of Lasiw v. Pereira*, 475 N.J. Super. 378, 392 (App. Div. 2023). Trial courts have broad latitude to manage discovery, and objections must overcome the presumption in favor

of disclosure by showing good cause. R. 4:10-2(a); Lasiw, 475 N.J. Super. at 392.

When a party serves evasive or incomplete responses, the Rules treat those responses as a failure to answer, authorizing orders compelling proper responses and fee-shifting. Keyworth v. CareOne, 258 N.J. 359, 381 (2024); Brugaletta v. Garcia, 234 N.J. 225, 252-53 (2018); R. 4:23-1(b)-(c) and 4:23-5. In New Jersey, Plaintiffs are entitled to seek discovery of any matter which is relevant to the subject matter of the pending action. R. 4:10-2(a). When a responding party declines to turn over requested documents, the requesting party may file a motion to compel discovery. R. 4:23-5(c).

Here, HMH and Dr. Carson have failed to serve any response to Plaintiff's requests for production of documents. The time has run for answers. Plaintiff diligently followed up on numerous occasions. Accordingly, the Court should compel a response to the requests pursuant to R. 4:23-5(c).

Under R. 4:23-1(c), the Court "shall" require the offending party to pay the movant's reasonable expenses, including attorney's fees, unless the opposition was substantially justified. Here, there is no justification for not providing any response to Plaintiff's requests for the production of documents. The EMR is a completely separate issue and no justification was offered for completely failing to provide any response to requests for production of documents. Accordingly, fees and costs should be awarded for Plaintiff having to file this cross-motion.

II. Audit Trails are Part of the Medical Record and Do Not Contain Proprietary Information Such That There is No Basis for Protective Order

HMH provides no basis for the assertion that the audit trail is not part of the patient's medical record. Under HIPAA, if a patient requests the audit log, then the medical provider is required to produce it. See 45 C.F.R. §170.210(h) (requiring ASTM E-2147-18 standards to be incorporated).

HIPAA and its implementing regulations guarantee individuals have a "right of access to inspect and obtain a copy of protected health information ["PHI"] about the individual . . ." 45 C.F.R. §164.524(a). This right extends to electronically stored information ("ESI") maintained by covered entities such as HMH. HIPAA's Privacy Rule establishes that individuals must be granted access to inspect their PHI, including electronic medical records ("EMR"). 45 C.F.R. §164.524. An audit trail is part of a patient's EMR because it is:

. . . a document that shows the sequence of events related to the use of and access to an individual patient's [EMR]. For instance, the audit trail will reveal who accessed a particular patient's records, when, and where the health care provider accessed the record . . . Each time a patient's [EMR] is opened, regardless of the reason, the audit trail documents this detail. The audit trail cannot be erased and all events related to the access of a patient's EMR are permanently documented in the audit trail. Providers cannot hide anything they do with the medical record. No one can escape the audit trail.

Lasiw, 475 N.J. Super. at 385 n.3 (alterations in original) (quoting Gilbert v. Highland Hosp., 31 N.Y.S.3d 397, 399 (Sup. Ct. 2016)).

Here, HMH provides no support for the statement that “Audit trails of the patient’s medical record are not part of the patient’s medical record itself because they do not drive patient care.” In fact, the citation to the regulation confirms that a patient has a right to the audit log. 45 C.F.R. §164.524(a). HIPAA further mandates that covered entities must act on requests to access PHI within 30 days and must provide the records in the format requested, provided the records are readily producible in that format. 45 C.F.R. §164.524(b)(2)(i) and (c)(2)(ii). In its guidance, the U.S. Department of Health & Human Services (“HHS”) has reinforced that individuals have a right to access their health information in the form and format requested. As HHS emphasizes:

[C]overed entities should have in place reasonable procedures to enable individuals to inspect their PHI, and requests for inspection should trigger minimal additional effort by the entity, particularly where the PHI requested is of the type easily accessed onsite by the entity itself in the ordinary course of business. . . . Further, a covered entity may not charge an individual who, while inspecting her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information.

[Individuals’ Rights Under HIPAA to Access Their Health Info., 45 C.F.R. §164.524, U.S. Dept. of Human Servs. (May 30, 2025), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>]

Federal standards explicitly state that “Audit logs and healthcare information shall be provided when specifically requested by . . . the patient, his personal representative, advocate, and/or designee.” The Center for Medicare & Medicaid Services has reinforced this, affirming that patients should be entitled to audit log information because, “at the end of the day, it’s all of the patient’s data. If it affects and touches their medical record, then that belongs to them.” EPIC has certified to the federal government that it complies with 45 C.F.R. §170.210, and thus, tracks all additions, deletions, and changes to the electronic medical record.

Here, Plaintiff has a right under HIPAA to inspect the audit log of the Decedent’s EMR because it is part of the Decedent’s medical record. See 45 C.F.R. §164.524; N.J.S.A. 26:2H-12.8. The audit trail reveals who accessed the Decedent’s medical records and where they accessed them from, which helps reveal what is at the heart of the issue in this case – who was responsible for the negligent care of the Decedent. Defendant’s refusal to permit an inspection of the audit trails of the medical record violates federal standards. This refusal constitutes an unreasonable barrier to access and directly contradicts HIPAA’s purpose of ensuring patients have complete access to their medical information. Further, contrary to Defendant’s assertion, the audit trails do not contain proprietary information but rather information on “who accessed a particular patient’s records, when, and where the health care provider accessed the record.” Lasiw, 475 N.J. Super. at 385 n.3. Such an inspection would not cause “unnecessary exposure of HMH’s employees and internal recordkeeping information.” For these reasons, the Court should deny Defendant’s motion for a protective order and compel the inspection of the audit trails.

Our courts have long recognized the importance of liberal discovery policies to facilitate the search for truth. Rule 4:10-2(a) broadly permits discovery of any matter that is relevant to the subject matter of the action, including ESI such as audit trails. The Rule emphasizes that discovery is permitted so long as the information is not privileged, and the scope of discovery is not limited to hardcopy documents but includes all ESI, which encompasses EMRs, audit trails, metadata, and

other electronic health information. See id.; see also R. 4:10-2(f). The courts have stressed the State's strong policy in favor of broad discovery, noting that restrictions on discovery should be an exception rather than the rule. Payton v. New Jersey Turnpike Authority, 148 N.J. 524, 535 (1997); see also Lipsky v. N.J. Assoc. of Health Plans, Inc., 474 N.J. Super. 447, 463 (App. Div. 2023).

In line with the State's policy favoring broad discovery, New Jersey courts have compelled defendants to produce audit trails of the Decedent's EMR. Lasiw, 475 N.J. Super. at 405. With electronic medical records, New Jersey courts may order an inspection of the EMR to capture on-screen views and metadata/audit trail content. Lasiw, 475 N.J. Super. at 390, 404.

In Lasiw, the Appellate Division endorsed a supervised, on-site EMR inspection. This is precisely the minimal-risk, high-benefit protocol Plaintiffs propose here. Moreover, Lasiw recognizes that certain metadata and audit information integral to the truth often only exist in the live system and not in static printouts. 475 N.J. Super. at 399-400. A live review is sometimes the only way to obtain the full picture. Our liberal discovery principles fully accommodate on-site electronic inspections under proper safeguards.

HIPAA independently guarantees an on-site right of inspection and the New Jersey's Patient Bill of Rights aligns. Federal regulations give a patient (or personal representative) the right to inspect and obtain copies of their protected health information maintained electronically. See 45 C.F.R. 164.524. This includes the right to access information in the form and format requested if it is readily producible in that format. See Lasiw, 475 N.J. Super. at 398, n.6 (referencing these authorities; noting that a patient's right to their own records extends to electronic formats). Furthermore, New Jersey's Patient Bill of Rights, N.J.S.A. 26:2H-12.8(g), guarantees patients access to "all records pertaining to [their] treatment." If the hospital's staff can view certain information on-screen as part of "the record," the patient's right of access should be co-extensive. Indeed, HHS guidance confirms that covered entities should allow on-site inspection and may not charge patients who take notes or photos during such inspection. In short, what Plaintiffs seek is not extraordinary; it is aligned with the rights patients already have under law to see their own information.

New Jersey's statutory framework aligns with federal law, including HIPAA, to ensure patients and their representatives have full access to medical records. N.J.S.A. 26:2H-5n(a)(1)(c) explicitly states that requests for access to medical records are governed by the requirements of HIPAA, particularly 45 C.F.R. §164.524, which guarantees individuals the right to access, inspect, and obtain copies of their health information. This statutory provision reflects the State's commitment to ensuring transparency in medical care by obligating healthcare providers to comply with federal law governing access to medical records. By incorporating HIPAA's provisions into state law, New Jersey ensures that patients, or their representatives, can access EMRs in the form and format requested. Defendant HMH's refusal to provide such access to Plaintiff without a confidentiality order is therefore a violation not only of federal law but also of State law, which explicitly mandates compliance with HIPAA's access provisions.

Moreover, under N.J.S.A. 26:8-5, hospitals in New Jersey are required to retain medical records for a period of 10 years following a patient's death. This underscores the state's policy of ensuring that medical records remain available and intact for an extended period, thereby

protecting patients' rights and facilitating legal inquiries or challenges concerning the care provided. The statute's emphasis on retention demonstrates the importance of maintaining accurate and complete medical records, particularly in cases involving potential litigation. Plaintiff's requests for an on-site inspection of the Decedent's EMR aligns with this policy, as Plaintiffs seek to verify the integrity of the records and ensure that no improper modifications were made post-mortem. Additionally, N.J.A.C. 13:35-6.5 requires licensed healthcare providers to maintain complete and contemporaneous records of patient treatment and that the records be created at or near the time of treatment and maintained in a permanent form that accurately reflects the care provided. N.J.A.C. 13:35-6.5(b)(2) further requires medical records must be kept as permanent, unaltered records placing any modifications made after the fact under careful scrutiny to ensure they do not compromise the accuracy of the original record. N.J.A.C. 13:35-6.5(b)(3)(iv) stipulates that healthcare providers must automatically prepare backup copies of the electronic medical records. This ensures that if an EMR is modified, deleted, or lost, the healthcare provider retains an accurate and unaltered backup version of the original records.

Furthermore, HMH misinterprets and misapplies Lasiw in an attempt to justify denying Plaintiff's request for an inspection of the audit trails of Decedent's EMR without a confidentiality order. Although the court in Lasiw did address that the parties had entered into a confidentiality agreement, that was not the basis of the court's decision. The Appellate Division in Lasiw recognized that metadata, including audit trails, is discoverable information and can reveal crucial details about the timing and authenticity of record entries. Specifically, metadata provides insight into when medical records were accessed, modified, or exported – key facts that can help establish whether the records were altered in ways that could affect the plaintiff's claims.

As two different district courts have noted in compelling production of an audit trail, "an audit trail is created in the natural course of business and is not protected by any privilege." Luterek v. Schneider Reg'l Med. Ctr., ST-17-cv-345, 2022 WL 847115 (V.I. Super. Mar. 18, 2022) (quoting Hall v. Flannery, No. 3:13-cv-914-SMY-DGW, 2015 WL 2008345, at *4, 2014 U.S. Dist. LEXIS 57454, at *11 (S.D. Ill. May 1, 2015) ("The audit trail is not created in anticipation of litigation; it is a part of the electronic medical record and is automatically generated as a function of the program. It does not implicate the 'core of attorney work product,' the "'mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.'").

In this case, Plaintiff has similarly requested a "full and complete audit trail for the medical record of Alexandrianna Lowe from July 20, 2018 to present." These audit trails raise serious questions about who was exercising negligent care around the time of Decedent's death. Plaintiff's request for an inspection of such information is fully aligned with the court's analysis in Lasiw and is necessary to ensure full access to all relevant information.

The proponent of a motion for protective order bears the burden to show good cause – specific facts demonstrating a genuine need to protect against a clearly defined harm such as annoyance, embarrassment, oppression, or undue burden R. 4:10-3. DiFiore v. Pezic, 254 N.J. 212, 229 (2023) (quoting R. 4:10-3). Defendants cannot and have not demonstrated any of those defined harms. Defendants cannot and have not demonstrated any of those defined harms. New Jersey recognizes a strong presumption of open access to litigation materials once they are filed with the Court. Overcoming that presumption "requires more than a passing nod; open access is the lens through

which the public views our government institutions.” Lederman v. Prudential Life Ins. Co. of America, 385 N.J. Super. 307, 323 (App. Div. 2006). In other words, a confidentiality order should not be entered or maintained lightly. The Court must balance the parties’ interests with the public interest in transparency. Any order must be narrowly tailored to serve the specific interests at stake.

Good cause must be based on current, specific facts, not speculation or convenient assertions. See Lederman, 385 N.J. Super. at 317-19 (courts must balance interests and require a showing of need for secrecy). Here, it is unclear what “cause” Defendants have to maintain secrecy. The documents at issue pertain to the care of Plaintiffs and the hospital’s own review of what went wrong. Plaintiff, the victim of the incident, has every right to that information. There are no genuine privacy interests (like a third-party’s medical info) or trade secret at stake; and if any tangential privacy issue existed, it could be handled by redaction or a targeted protective clause. The sweeping scope of HMH’s request for confidentiality is unjustified. Indeed, our Supreme Court in Hammock v. Hoffman-LaRoche, Inc. held that even when a protective order is initially entered, the proponent must show a continuing need if it is to remain in place and the Court “must examine each document individually and make factual findings why the presumption of public access has been overcome.” 142 N.J. 356, 382 (1995). The “need for secrecy should extend no further than necessary to protect confidentiality.” Id.

Plaintiff has made clear that she has good cause for the Court to deny a protective order restricting access to decedent’s medical information. First, the records belong to Plaintiff as the Decedent’s representative. Federal law does not require the patient to keep the records confidentially – just the provider, so Plaintiff should be able to use these records as she sees fit and not just related to the litigation. Cf. 45 C.F.R. §164.500 (privacy rule applies to covered entities) with 45 C.F.R. §164.524 (patient has right of access to personal health information). Secondly, the Decedent left behind an heir who has a right to know his mother’s medical history and use that information to help his own medical treatment. There is no reason why Plaintiff should be restricted from sharing the medical records with her grandson.

Additionally, there is no public policy reason that the records should not be maintained confidentially. Alexandrianna was the victim of discrimination and bias because they treaters at HMH did not treat her the same as they would a non-addict. Plaintiff should be entitled to use the records for advocacy so that addicts receive equal and appropriate medical care from the largest healthcare provider in New Jersey, HMH.

Here, Plaintiff is only seeking to inspect Alexandrianna’s medical record for which she has a federal right and which HMH does not have a constitutionally protected right in the Decedent’s audit trail. See Id. at 462. Again, it is Plaintiff – not HMH – that has a federally protected right to inspect the decedent’s own medical record. 45 C.F.R. 164.524(c)(2)(i). HMH has not met its burden under R. 4:10-3. First, there is no burden or expense for HMH to pull the EMR for inspection. The information contained in that document – when the medical record was created, edited, and accessed – is relevant and essential to the medical malpractice claims. Finally, there is no other means to obtain the audit trail, which belongs to the patient. Fred Shulte and Erika Fry, New Rules Will Ease Patients’ Access to Electronic Medical Records, Senate Panel Says, FORTUNE (Mar. 26, 2019), available at <https://khn.org/news/new-rules-will-easepatients-access-to-electronic-medical-records-senate-panel-says/>.

Likewise, HMH's reliance on the fact that there was a voluntary confidentiality agreement in Lasiw does not somehow bind Plaintiff – who was not a party in Lasiw to agree to confidentiality in this matter. In Lasiw, the Court noted that any concerns of “calamities” regarding the inadvertent access to confidential information was addressed through the restrictions that “defendants would control all access to the metadata behind any entry in the EMR that [plaintiff's expert] wished to examine.” 475 N.J. Super. at 402. The court further noted that any inadvertent access was addressed in the Court Rules that permit clawback and provide for ethical limitations for attorneys who inadvertently obtain confidential information. Id. at 402 (citing R. 4:10-2(f)(1); RPC 4.4(b), and Pressler & Verniero, *Current N.J. Court Rules*, cmt. to R. 4:18-1).

Lastly, the Appellate Division agreed with the trial court that “defendants failed to demonstrate [plaintiff's expert]'s inspection would place the EPIC system at risk of a cyber attack.” Id. at 402. While the Appellate Division did note that the concerns, in no way did it require confidentiality agreements for other cases. In fact, the Appellate Division's explanation suggested that such protection was not necessary given the framework of R. 4:10-2(e) and R.P.C. 4.4(b). Importantly, Plaintiff has agreed to the same confidentiality agreement to which the Appellate Division indicated a protective order “could” address – “Maintaining confidentiality of any inadvertently disclosed, unrelated patient information.”

HMH seeks to rely upon other trial court orders, but such orders are not decisions and serve no precedential value. See R. 1:36-3. The Rule only permits citation to unpublished opinions when counsel provides “all contrary unpublished opinions known to counsel.” Here, HMH failed to do so as there are other Orders that are directly contrary to those upon which HMH relies. See, e.g., Hagan v. JFK Med. Ctr., MID-L-148-22 (Law Div. May 23, 2025) (ordering electronic medical record inspection without confidentiality and subject to parameters to which this Plaintiff has agreed) and (Law Div. Jan. 13, 2024) (ordering production of audit trail without confidentiality)(collecting cases). Additionally, federal and other state courts have permitted the same access to audit trails. See Borum v. Smith, 2017 WL 3014487 (W.D. Ky. 2017) (ordering Defendant to permit Plaintiff the opportunity to perform an on-site inspection of the Plaintiff's EMR and to produce a complete copy of the audit trail); Culpepper v. Wellstar Health System, No. 15A54645E7 (Ga. Dekalb Cty. Ct. Aug. 7, 2017) (permitting Plaintiff's expert to enter the hospital and perform a search for the client's electronic medical records, including archived data and metadata in the presence of a hospital witness); Moan v. Mass. Gen. Hospital, 2016 Mass. Super. LEXIS 28 (Mass. Sup. Ct. Mar. 31, 2016) (ordering hospital to produce full audit trail and requiring the hospital to produce a person capable of accessing the medical record during a deposition) (collecting cases).

These decisions are consistent with Congress's intent to expand right to access personal health information (“PHI”). 42 U.S.C. §400jj-19 (giving Secretary power to establish policies to make a patient's EMR accessible to the patient and the patient's representative); see also 42 U.S.C. §300jj-19 (granting patient access to EMRA). Based upon the interplay of federal and State rights and broad discovery rules combined with HMH's lack of good cause to maintain the confidentiality of Plaintiff's own EMR, HMH's application should be denied.

Finally, Plaintiff has demonstrated reasonable restrictions upon the electronic medical inspection process similar to those accepted by the Appellate Division in Lasiw. See Lasiw, 475 N.J. Super. at 385, 405. As a result, Plaintiff's cross-motion should be granted and HMH's motion

should be denied.

**E-Discovery Counsel for HMH’s Argument in Support of the Motion for Protective Order
and in Opposition to the Motion to Compel Discovery**

**I. The Opposition Relies Upon the Myth That an Audit Trail is Part of the Patient
Medical Record**

The heart of the Opposition and Cross-Motion are the following sentences:

The Health Insurance Portability and Accountability Act (“HIPAA”) and its implementing regulations, specifically 45 C.F.R. §164.524 guarantee patients, or their legal representatives, the right to access, inspect, and obtain copies of their protected health information (“PHI”). This right encompasses inspections of a Decedent’s electronic medical record (“EMR”), including audit trails.

This passage presents the Court with an absolute falsehood.

By virtue of federal law, an audit trail is not part of and is completely different from a patient’s medical record. In quoting 45 C.F.R. 164.524(a), the provision describing what HMH is obligated to produce, Plaintiff conveniently leaves out five words. The passage should read that “an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set . . .” 45 C.F.R. §164.501 clarifies that a “designated record set” contains documents “used, in whole or in part, by or for the covered entity to make decisions about individuals.”

Additionally, the ASTM provision cited by Plaintiffs – ASTM e-2147-18 – is not incorporated wholesale into 45 C.F.R. §170.315. Rather, that CFR provision adopts only limited portions of the ASTM publication which “require certified health IT developer systems to be capable of recording and producing audit information about user actions,” with “user” defined in regulations as members of a healthcare provider’s workforce interacting with the systems, not the patient. Critically, ASTM 32147-18 does not “create new disclosure mandates to patients under HIPAA or the Information Blocking Rule.” Further, the CFR provision referencing ASTM – 45 C.F.R. 170.210 – applies not to hospitals like HMH, but rather to technology vendors and software developers. The applicability provision at the outset of the C.F.R. section cited by counsel makes clear the ASTM provision’s purpose: 45 C.F.R. §170.101 (2024) (“The standards, implementation specifications, and certification criteria adopted in this part apply to health information technology and the testing and certification of Health IT Modules.”).

An audit trail does not exist when doctors and nurses are making decisions about patient care; it is metadata setting forth the time of specific entries of PHI and the identity of the author of such entries. It is not the PHI itself that is the basis for decisions about the patient. To continue to make this representation before multiple judges is a deplorable practice that should not be tolerated.

Further, an audit trail also shows access to the medical record by hospital personnel whose identity is not disclosed in the medical record. Various categories of hospital personnel access

a patient's records for non-treatment purposes, such as to accomplish billing, payment, insurance reimbursement, eligibility review, care authorization, and similar tasks not directly related to patient care.

The identity of, roles assigned to, and processes executed by, employees disclosed in an audit trail comprises proprietary HMH business information which HMH has a right to protect from exploitation outside of the pending litigation, just as any business would protect the identity and roles performed by employees having no connection to the litigation and the underlying dispute. See, e.g., Martin v. Quick Check Corp., No. L-4170-08, 2012 WL 127530, *2 (App. Div. Jan. 18, 2012) (finding that the trial court did not abuse its discretion in denying plaintiff access to the vice president of human resources' notebook which "contained his handwritten notes concerning confidential personnel information relating to other employees not relevant to [the] litigation.").

Beyond disclosing employee personally identifiable information ("PII") routinely protected by courts of this State, a DCO is necessary to prevent commercial as well as threat actor exploitation of HMH's proprietary implementation of the Epic EHR platform as may be revealed by the audit trail. The Epic platform serves as the operating system for HMH's statewide operations. A hospital system would be hard-pressed to respond to regulators (not to mention current and future patients) if, following a cyber intrusion, it was revealed that the provider produced, in routine civil litigation, metadata from its critical information system without limiting use to the litigation in question. HMH has no choice but to insist upon a DCO to protect metadata associated with its mission-critical information platform. A DCO does not impose any additional costs upon the parties, and the eCourts system makes it easy to designate attachments to court filings as private for litigants only.

Plaintiff burdens the Court and HMH with pointless motion practice in response to HMH's reasonable request for protection from any potential dispersal of HMH employee and HMH confidential business information beyond the confines of this case.

II. The Opposition Ignores Federal Law – the HIPAA Security Rule – Compelling Heightened Information Security Measures to Protect Healthcare ePHI and Metadata.

HIPAA Security Rule, 45 C.F.R. 164.302, which requires healthcare providers to protect the personal healthcare information they maintain with administrative safeguards, physical safeguards, and technical safeguards. Plaintiff steers wide of the subject. One HIPAA Security Rule safeguard – the "administrative safeguard" satisfied by a business association agreement ("BAA") – is not in place because adverse counsel will not sign a BAA, yet Plaintiff wants audit trail data to be disclosed with no protection at all, not even a confidentiality order limiting disclosure and use to this litigation. These HIPAA rules, which were designed to protect patient e-PHI and associated system metadata, preempt State discovery rules. "There is an express preemption provision contained in the Privacy Rule, 45 C.F.R. §160.203." In re Diet Drug Litigation, 384 N.J. Super. 546, 557 (Law Div. 2005) (Walsh, J.). That preemption provision states as follows:

§160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of state law.

The HIPAA Security Rule appears at 45 C.F.R. §164.302 and is part of the “subchapter” containing §160.203. That “subchapter” is titled: “Subchapter C – Administrative Data Standards and Related Requirements (§160.101 to §164.535).” The HIPAA Security Rule codified at 164.302 obviously lies within the C.F.R. range which preempts less restrictive State rules.

This means that the Security Rule’s administrative safeguards, physical safeguards, and technical safeguards apply in civil litigation matters and preempt State law decisions that might tend to erode those mandatory protections.

One of the HIPAA Security Rule safeguards, a BAA, is lacking yet a release of healthcare patient metadata cannot take place without a protection against misuse. Therefore, a discovery confidentiality order is minimally required to fulfill the HIPAA Security Rule’s administrative safeguard. Plaintiffs cannot invoke cases like Payton to negate the requirement of a DCO protecting the production of healthcare metadata such as the audit trail of accesses to e-PHI because such precedents are expressly preempted by the aforementioned HIPAA provisions. See Smith v. American Home Products Corp. Wyeth-Ayerst Pharmaceutical, 372 N.J. Super. 105, 127 (Law Div. 2003) (“A state law is not preempted unless it is contrary to the federal objectives regarding privacy protections of patient health information. Likewise, a state law deemed “more stringent” or more protective of the use and disclosure of patient health information than afforded under federal law is not preempted.”).

Plaintiff’s reference to the MyChart audit trail produced in the Citta matter is distinguishable because such a report only reflects a patient’s access to his or her own designated record set through a module separate from EPIC, it contains no e-PHI of other patients, and identifies only providers who participated in the treatment of the patient.

Although Plaintiff’s Opposition dismissed concerns about cyber intrusions by threat actors, counsel has no expertise in that area of international and nation-state criminality. No imagine is needed to see that the public disclosure of employee identity, roles, and business processes could facilitate social engineering exploits of the kind rampant throughout healthcare and other industries.

The need to protect ePHI, as mandated by federal law, as well as associated metadata such as audit trail, is not diminishing, either. Threats to healthcare providers are constant and ever-changing as guidance from the Cybersecurity Infrastructure and Security Agency makes clear. Just last December, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) announced changes to the HIPAA Security Rule “to strengthen cybersecurity protections for electronic protected health information (ePHI).”

III. An Inspection Cannot be Held in the Present Case Because Plaintiff’s Records Were Housed in a Legacy EMR System

Addressing Plaintiffs' premature request for a live inspection, Plaintiffs have no grounds for this request because the audit trails have not yet been reviewed. HMH is willing to produce them under cover of a DCO, but they must be received first. Further, the request should also be denied because Soarian Clinical is a legacy EMR system no longer in use and federal regulations preclude such an exercise.

On October 30, 2019, the hospital in question, Jersey Shore University Medical Center ("JSUMC") ceased to utilize EMR application, Soarian Clinical, which had been licensed to HMH by Cerner Corporation and in its place, implemented the Epic EMR system provided by Epic Systems Corporation.

A live inspection would yield no more information than a display of the static record already available to be produced and, therefore, would be unduly burdensome. Given that Plaintiff made the issue of a live inspection of HMH's abandoned EMR system the subject of a cross-motion, HMH lacked adequate time to obtain a client certification providing more detail regarding the futility of a live inspection in the short timeframe allowed, though HMH would have been able to do so had Plaintiff filed a regular motion under the Rules.

In the context of pre-October 2019 patient encounter at JSUMC, other Judges have denied requests for a live inspection given the unavailability of the live Soarian Clinical platform for the patient encounter in question. See the May 16, 2024, Order in Golia v. HMH, et al., ESX-L-7674-18 (denying a live inspection).

Moreover, a live inspection of a hospital's EMR system, the lifeblood of its operations, is not permitted or provided for in any federal or state regulations. In support of this, HMH submits the expert certification of Alicia Farlese, a healthcare regulations expert, which demonstrates that live inspection of hospital EMR system is contrary to both federal or state law and implementing regulations.

Under 45 C.F.R. 164.524, a "covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format . . ." Under this provision, "access" does not equal a live inspection of a hospital's EMR system. Moreover, according to the Office for Civil Rights, Department of Health and Human Services clarified this precise point, "covered entities are not required by this provision to provide individuals with direct access to their systems. They must only provide individuals with an electronic copy of their protected health information."

HMH has already provided all that it is required to under federal and state law: the Plaintiffs' information contained the "designated record set" and more, namely the patient medical record. HMH also seeks to produce audit trails of the medical record but can only do so with a DCO. Plaintiff's request for a live inspection goes above and beyond the "designated records set" and asked for something that HMH is not obligated to provide. Plaintiffs have cited no regulation, HIPAA or otherwise, that would require HMH to permit a live inspection of its EMR system and, in fact, the Office for Civil Rights, Department of Health and Human Services, confirmed that patients or their representatives are not entitled to such risk-laden access.

For all the foregoing reasons, this Court should grant HMH's motion for entry of a discovery

confidentiality order within this matter to ensure the sensitive information HMH produces remains within the bounds of the present litigation and deny Plaintiff's cross motion for a live inspection.

Defendant HMH's Argument in Opposition to the Motion to Compel Discovery

Plaintiffs' Motion to Compel concerns audit logs, EMR inspection, and responses to Plaintiffs' Notice to produce. The issues of audit logs and EMR inspection will be addressed by Mr. Pizzi under separate cover.

With regard to responses to Plaintiffs' Notice to Produce, HMH Defendants' counsel concedes that they are overdue and that this was an oversight on his part. Since the Cross-Motion was filed, Plaintiffs' counsel has served responses to the Notices to Produce on behalf of Dr. Carson. Despite diligent efforts, HMH Defendants' counsel is still in the process of obtaining documents from his client to respond on behalf of HMH Hospitals Corporation d/b/a Jersey Shore University Medical Center. Those responses will be served shortly.

Given the foregoing, counsel for the HMH Defendants understands if the Court must compel responses to the Notice to Produce by HMH Hospitals Corporation d/b/a Jersey Shore University Medical Center within the 14 days requested. HMH Defendants, however, object to Plaintiffs' counsel's request for payment of \$500. Efforts have been made and are continuing to be made to comply with the discovery demands and good cause exists for the Court to deny this request.

Legal Standard Motion for Protective Order

In considering the instant application for a protective order, this Court must begin with the principle that pretrial discovery is afforded the broadest possible latitude and extends not only to relevant information but also to any information that might lead to the discovery of relevant information. See Shanley & Fisher, P.C. v. Sisselman, 215 N.J. Super. 200, 216 (App. Div. 1987). However, the court has discretion to issue Protective Orders if the discovery demand is burdensome. James v. Chevron USA, Inc., 301 N.J. Super. 512, 546 (App. Div. 1997). Further, it should be noted that because R. 4:10-3 follows the text of Fed.R.Civ.P. 26(c), federal case law is instructive on its application as well. Kerr, 295 N.J. Super at 156.

"Implicit in [R. 4:10-3] which allows persons to obtain a protective order against discovery is the notion that movant bears the burden of persuading the Court that good cause exists for issuing such an order." Kerr v. Able Sanitary, 295 N.J. Super 147 (App. Div. 1996). The burden placed on the moving party is heavy, with the moving party having to show "the need for secrecy substantially outweighs the presumption of access." Hammock v. Hoffman-LaRoche, Inc., 142 N.J. 356, 381 (1995). Further, the need for secrecy "must be demonstrated with specificity as to each document. Broad allegations of harm, unsubstantiated by specific examples or articulated reasoning are insufficient." *Id.* at 382. "The burden . . . is upon the movant to show . . . a particular and specific demonstration of fact, as distinguished from

stereotyped and conclusory statements.” General Dynamics v. Selb Mfg. Co., 481 F.2d 1204, 1212 (8th Cir. 1973).

The law is clear that unfettered discovery is the rule, with limitation being the exception, placing the burden of demonstrating extraordinary circumstances squarely on the party moving for a protective order. See Hammock, 142 N.J. at 381. R. 4:10-2 provides that “in [g]eneral[,] [p]arties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action.” Moreover, R. 4:10-3 grants the court discretion in determining what matters may warrant a protective order, provided only that “good cause” is shown warranting the limitation imposed on discovery. See, e.g., Alk Associates, Inc. v. Multimodal Applied Systems, Inc., 276 N.J. Super. 310, 316 (App. Div. 1994) (finding trial courts have a high degree of discretion in discovery matters). In Catalpa Inv. Group, Inc. v. Franklin Tp. Zoning Bd. of Adjustment et. al, the New Jersey Supreme Court highlighted nine factors that should be considered when determining whether “good cause” exists:

1. The nature of the lawsuit and the issues raised by the pleadings;
2. The substantive law likely to be applied in the resolution of the issues raised by the pleadings.
3. The kind of evidence which could be introduced at the trial, and the likelihood of it being discovered by the pretrial discovery procedure which is the subject of the application for a protective order.
4. Whether trade secrets, confidential research, or commercial information are sought in the discovery procedure employed, whether they are material and relevant to the lawsuit, and whether a protective order will insure appropriate confidentiality
5. Whether the pretrial discovery seeks confidential information about persons who are not parties to the lawsuit
6. Whether the pretrial discovery sought involves privileged material.
7. Whether the pretrial discovery sought relates to matters which are or are not in dispute.
8. Whether the party seeking discovery already has the materials sought.
9. The burden or expense to the party seeking the protective order.

254 N.J. Super. 270, 273-274 (Law Div. 1991) (citations and footnotes omitted).

“To overcome the presumption in favor of discoverability, a party must show ‘good cause’ for withholding relevant discovery by demonstrating, for example that the information sought is [...] confidential or proprietary.” Capital Health Sys. V. Horizon Healthcare Servs., 230 N.J. 73, 80 (2017). Courts have explained that “broad allegations of harm, unsubstantiated by specific examples or articulated reasoning, are insufficient” to satisfy the “good cause” and “justice” requirements of R. 4:10-3. Id.

Conclusion

This matter comes before the Court by way of Defendant HMH Hospitals Corporation, d/b/a Jersey Shore University Medical Center (individually, “HMH”)’s Motion for Protective Order. Plaintiffs Candace Moschella, as Administrator *Ad Prosequendum* for the Estate of Alexandrianna Lowe and individually (“Plaintiffs”) file a Cross-Motion to Compel Discovery. Defendant Dr. Carson and HMH Hospitals Corporation, d/b/a Jersey Shore University Medical Center filed an Opposition to the Cross-Motion and Reply to Plaintiffs’ Opposition.

According to Rule 4:10-2(a), parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party. R. 4:10-2(a). A party whose discovery request has not been complied with, may move to compel production of documents pursuant to R. 4:23-5(c) rather than immediately move for dismissal of the party’s pleadings under R. 4:23-5(a)(1). The party making such a discovery motion must make a good faith effort to acquire the discovery as required by R. 1:6-2(c).

The law is clear that unfettered discovery is the rule, with limitation being the exception, placing the burden of demonstrating extraordinary circumstances squarely on the party moving for a protective order. See Hammock, 142 N.J. at 381. R. 4:10-2 provides that “in [g]eneral[,] [p]arties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action.” Moreover, R. 4:10-3 grants the court discretion in determining what matters may warrant a protective order, provided only that “good cause” is shown warranting the limitation imposed on discovery. See, e.g., Alk Associates, Inc. v. Multimodal Applied Systems, Inc., 276 N.J. Super. 310, 316 (App. Div. 1994) (finding trial courts have a high degree of discretion in discovery matters). In Catalpa Inv. Group, Inc. v. Franklin Tp. Zoning Bd. of Adjustment et. al, the New Jersey Supreme Court highlighted nine factors that should be considered when determining whether “good cause” exists:

1. The nature of the lawsuit and the issues raised by the pleadings;
2. The substantive law likely to be applied in the resolution of the issues raised by the pleadings.
3. The kind of evidence which could be introduced at the trial, and the likelihood of it being discovered by the pretrial discovery procedure which is the subject of the application for a protective order.
4. Whether trade secrets, confidential research, or commercial information are sought in the discovery procedure employed, whether they are material and relevant to the lawsuit, and whether a protective order will insure appropriate confidentiality

5. Whether the pretrial discovery seeks confidential information about persons who are not parties to the lawsuit
6. Whether the pretrial discovery sought involves privileged material.
7. Whether the pretrial discovery sought relates to matters which are or are not in dispute.
8. Whether the party seeking discovery already has the materials sought.
9. The burden or expense to the party seeking the protective order.

254 N.J. Super. 270, 273-274 (Law Div. 1991) (citations and footnotes omitted).

Rule 4:10-2(g) states, “the frequency or extent of use of the discovery methods otherwise permitted under these rules shall be limited by the court if it determines that: (1) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (2) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (3) the burden or expense of the proposed discovery outweighs its likely benefit ... The court may act pursuant to a motion or on its own initiative after reasonable notice to the parties.” R. 4:10-2(g).

Rule 4:10-3 authorizes trial courts to make “any order that justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.” Ibid.

It is apparent to the Court that the parties have attempted to resolve this issue among themselves prior to the filing of the instant Motion for Protective Order and Cross-Motion to Compel Discovery as to Plaintiff’s request for audit trails from the Defendant, HMH. Plaintiffs’ counsel indicated to HMH Defendants’ counsel that she did not have authority to consent to a Discovery Confidentiality Order (“DCO”). This motion was then filed.

Here, Defendant HMH asserts that Plaintiff should be precluded from accessing audit trails without entry of a Discovery Confidentiality Order (“DCO”) within this matter to ensure the sensitive information HMH produces remains within the bounds of the present litigation.

Specifically, Defendant asserts that an audit trail contains confidential and proprietary business information of HMH created by the healthcare operating system that HMH licenses from a third party, which is referred to as its electronic medical or health record system (“EMR”). HMH cannot produce proprietary and sensitive business information, such as EMR audit trails, without the protection of a DCO. The audit trail file of the electronic medical record, for example, presents tens of thousands of rows of data concerning access to the medical record and annotates those access with the following fields of information:

Time Stamp (EST)	MRN [Medical Record Number]
Access by Name [employee]	Patient ID
Access by ID [employee]	Encounter
Event	Platform
Event Area	Login Department
Type	Workstation
Patient Name	Associated Data

HMH submits that none of this data is part of the patient's medical record. Whenever a healthcare professional accesses the EMR, a line of data in the patient audit trail is created showing the date and time, information about the area within the EMR accessed, and other metadata. Each distinct item accessed in the EMR creates an audit trail line per access, which means that a single EMR session often creates hundreds of lines of audit trail data.

Defendant contends that the audit trails are not part of the medical record as they do not drive patient care, which is required for a document to be in the "designated record set" under the Health Information Portability and Accountability Act ("HIPAA").

Plaintiff contends that Defendant has failed to meet its burden in establishing the need for a protective order under R. 4:10-3 and cross-moves to compel HMH to produce medical record audit trails related to Plaintiff without the need for a confidentiality order. Plaintiffs also seek the ability to conduct a live inspection of the EMR. HMH Defendants contend that such an inspection exceeds HMH's responsibility under the applicable CFR provisions and against public policy.

Plaintiff contends that HMH's refusal to permit inspection of the entire EMR constitutes an unreasonable barrier to critical evidence, contradicting both HIPAA and New Jersey law. Plaintiff further contends that the inspection is needed because the negligent care of Defendant is the heart of the issue in this case. Further, denying Plaintiff access unless a confidentiality order is entered while allowing Defendant's unrestricted use of Plaintiff's records creates an unfair advantage in the litigation. Plaintiff contends that she has a right to access and inspect her own medical records, including electronically stored information, in their native format. See 45 C.F.R. 164.524 (patient has right of access to personal health information). Plaintiff contends that no genuine privacy interest, such as a third-party's medical information, or trade secret is at stake and, if any tangential privacy issue existed, it could be addressed through a redaction or a targeted protective clause. Plaintiff contends that in addition to her need for the information in order to pursue her claims, she is also entitled to the information so that the decedent's son, Plaintiff's grandson, can use his mother's medical history to help his own treatment. Plaintiff contends that only the provider is required to keep the records confidentially, not Plaintiff, citing 45 C.F.R. §164.500.

Moreover, Plaintiff contends that HMH's reliance on the fact that there was a voluntary agreement in Lasiw does not somehow bind Plaintiff – who was not a party in Lasiw – to agree to confidentiality in this matter. Indeed, the Appellate Division agreed with the trial court that "defendants failed to demonstrate [plaintiff's expert]'s inspection would place the EPIC system at risk of a cyberattack." Id. at 402. While the Appellate Division did note that the voluntary confidentiality agreement was another layer of protection for the concerns, it did not impose a requirement of confidentiality agreements for other cases. Plaintiff contends that there is a federally recognized right to inspect the Decedent's medical record. See 45 C.F.R. 164.524(c)(2)(i).

To reiterate, Plaintiff states that she is only seeking to inspect the decedent's medical record for which she has a federal right and which HMH does not have a constitutionally protected privacy right. Plaintiff further asserts that Defendant has not met its burden under R. 4:10-3 as (1) there is no burden or expense for HMH to produce the EMR for inspection; (2) the information is relevant and essential to Plaintiff's medical malpractice claims; and (3) there are no other means of

obtaining the audit trail, which belongs to the patient.

In response, HMH contends that the provision of the C.F.R. cited by Plaintiff applies to health information systems, not health care facilities like HMH. See 45 C.F.R. 170.101 (“The standards, implementation specifications, and certification criteria adopted in this part apply to health information technology and the testing and certification of Health IT Modules”). Defendant HMH cites the HIPAA Privacy Rule, which does apply to hospitals. It requires a covered entity to provide, upon a patient’s request, an accounting of certain disclosures, including disclosures by any of the entity’s “business associates”, for purposes other than treatment, payment, or healthcare operations. See 45 C.F.R. §164.528.

Moreover, Defendant HMH contends that 45 C.F.R. § 164.524(a) provides that “an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set.” The “designated record set” comprises records “[u]sed, in whole or in part, by or for the covered entity to make decisions about individuals.” Id. The Court agrees that information contained in the designated record set is distinct from the data maintained within an audit trail, which provides information as to when the EMR was accessed, any amendments thereto, and by whom the EMR was accessed or amended by. The data from an audit trail is not used to drive patient care decisions.

While Plaintiff is correct that under 45 C.F.R. 164.524, a “covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format,” access does not necessarily equate to an inspection of HMH’s EMR system. Indeed, under the New Jersey Patient’s Bill of Rights, codified at N.J.S.A. 26:2H-12.8(g), which provides, “[e]very person admitted to a general hospital . . . shall have the right: To privacy and confidentiality of all records pertaining to the patient’s treatment . . . and to access those records, including receipt of a copy thereof at reasonable cost, upon request, unless the patient’s physician states in writing that access by the patient is not medically available.” The Court agrees that receipt of a copy of the medical records is distinct from visiting HMH’s premises to access the EMR system.

Further, as to Plaintiff’s request for a live inspection of the audit trails, Defendant HMH contends that the request must be denied for three reasons. First, it is premature as the audit trails have not yet been received or reviewed and second, Plaintiff’s records were housed in a legacy EMR system, Soarian Clinical, that is no longer in use and federal regulations preclude such an exercise. Third, HMH asserts that a live inspection would yield no more information than a display of the static record already available to be produced and therefore, would be unduly burdensome.

Under the HIPAA Security Rule, HMH bears the responsibility of putting in place administrative, physical, and technical safeguards to protect the personal health information maintained. 45 C.F.R. §160.302. As Plaintiff has not signed a business associate agreement (“BAA”), an approved administrative safeguard, HMH contends that a DCO is warranted to limit disclosure of this information to this litigation. Without entry of a BAA, Defendant contends that a DCO is necessary because an audit trail shows access to the medical record by hospital personnel whose identity is not disclosed in the medical record. Various categories of hospital personnel access a patient’s records for non-treatment purposes, such as to accomplish billing, payment, insurance, eligibility review, care authorization, and similar tasks not directly related to patient

care.

Notably, HMH states it is ready to comply with Plaintiffs' discovery requests and can provide separate audit trails but will only do so with a DCO in place that protects HMH's and third-party's proprietary and business information. The Court notes that Plaintiff does not object to keeping the subject information within this litigation as Plaintiffs merely only seek audit trails in connection with Plaintiff's care only. The Court does find that Defendant has demonstrated that the risk of a ransomware attack may be likely to actualize. The audit trail may contain meta data that users sophisticated in the use of technology may use for purposes outside of this litigation. The Court also acknowledges the public's access to the courts and the interest in ensuring that the audit trails exchanged are accessible only to the parties of this litigation and the Court. HMH bears the responsibility of putting in place administrative, physical, and technical safeguards to protect the personal health information maintained. To require all parties to execute a confidentiality order would ensure that they are complying with that responsibility. While Plaintiff is entitled to the Decedent's medical records, the Court does not consider the information contained within the audit trails to be "medical records" since those records are not used to drive patient care. The information contained in the designated record set is distinct from the data maintained within an audit trail, which provides information as to when the EMR was accessed, any amendments thereto, and by whom the EMR was accessed or amended by. Again, the data from an audit trail, while it contains valuable information is not used to drive patient care decisions. As such, the Court finds it appropriate to issue a protective order and also require the production of the audit trails.

The Court does not find that the measures set forth in the proposed Confidentiality Order (Defendant's Exhibit C) appear to create unreasonable obligations upon Plaintiff but rather imposes an obligation on all parties to ensure that the use of audit trails is limited to the records of the Decedent and this litigation. As this Confidentiality Order is not being entered by consent of the parties, Defendant is to submit an amended Order to reflect that this is a Confidentiality Order entered by Court Order and not by consent of the parties.

Turning next to Plaintiff's Cross-Motion to Compel Discovery, Plaintiff seeks an Order compelling the production of Dr. Carson and HMH Hospitals Corporation d/b/a Jersey Shore University Medical Center's responses to the Notice to Produce in addition to the audit trails and the inspection already addressed herein. This motion is also the result of unsuccessful attempts to meet-and-confer regarding the outstanding discovery.

A party whose discovery request has not been complied with, may move to compel production of documents pursuant to R. 4:23-5(c) rather than immediately move for dismissal of the party's pleadings under R. 4:23-5(a)(1). The party making such a discovery motion must make a good faith effort to acquire the discovery as required by R. 1:6-2(c).

Plaintiffs have made a good faith effort to acquire the requested discovery through multiple attempts to coordinate when Plaintiffs can expect responses from the HMH Defendants, Dr. Carson and HMH, but to no avail.

In their Opposition, the HMH Defendants do not object to producing discovery responses, however, they object to Plaintiffs' counsel's award of attorney's fees. The Court finds that as Dr.

Carson has provided discovery responses; discovery responses need not be compelled from him. Insofar as any discovery demands owed to Plaintiffs are outstanding the HMH Defendants are directed to provide the requested audit trails, documents, and responses. The audit logs shall be produced in accordance with the terms of the Protective Order.

The Court does not find that an award of attorney's fees is appropriate since the parties had a legitimate dispute as to what documents are discoverable.

For these reasons, Defendants' Motion for Protective Order is hereby **GRANTED in part**. For these same reasons, Plaintiffs' Cross-Motion to Compel Discovery is hereby **GRANTED in part**.