[CASE CAPTION]

MOTION TO COMPEL PRODUCTION OF AUDIT TRAIL

Pursuant to Connecticut Practice Book § 13-14, the plaintiffs, [PLAINTIFFS], hereby respectfully move the Court for an order directing the defendant to provide a complete and adequate response to the document requests contained in the Re-Notice of Deposition dated September 5, 2019 (Exhibit A). Briefly summarized, the document requests seek, *inter alia*, the production of the federally mandated audit trail for the October 2, 2014 prenatal ultrasound, in its entirety. In response thereto, the only documents produced by the defendant are two largely undefined and unintelligible documents which appear to be "access logs", and do not in any way meet or satisfy the requirements of federal law, the Connecticut Practice Book, or the document requests made by the plaintiffs in this matter.

The defendant is required by federal law to maintain an audit trail which tracks and records critical information about each entry in a medical record in an electronic hospital chart. The audit trail records*, inter alia*, the identity of any health care provider who accesses, reviews, or edits the document in any way, *and* records the nature of any change made to the document.[1] In this way, entries in an electronic chart may be tracked and accessed, even if the electronic record has been altered at a later date.

[1] Federal regulations governing electronic health information and records require audit trails to be developed and maintained. *See, e.g.*, 21 C.F.R. § 11.10(e) (requiring, in order to ensure the authenticity and integrity of electronic records, the "[u]se of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records."); 45 C.F.R. § 164.312(b) (directing healthcare providers to implement audit controls "that record and examine activity in information systems that contain or use electronic protected health information."); 45 C.F.R. § 170.210(e) (Secretary of U.S. Department of Health and Human Services adopted "standards to protect electronic health information created, maintained, and exchanged," including audit logs to record the date and time of the access event, the patient identification, the user identification, and the type of action).

In the present case, such information is critical to corroborate or disprove the claims of the defendant that are central to its defense. The plaintiffs therefore respectfully urge the Court to order the defendant [DEFENDANT] to produce the audit trail for the October 2, 2014 pre-natal ultrasound.

I. FACTUAL BACKGROUND

In the subject action, the plaintiffs claim, *inter alia*, that the defendant's maternal fetal medicine physician, [DOCTOR], failed to properly interpret and act upon the October 2, 2014 prenatal ultrasound, which revealed diagnostic evidence that the [PLAINTIFFS], were suffering from cytomegalovirus (CMV). Specifically, the ultrasound showed echogenic bowel, which is an indicator of CMV at the 21-week gestation period.[2]

There is no question that the ultrasound report authored by [DOCTOR] clearly documents in capital letters a finding of "HYPERECHOIC SMALL BOWEL" for Fetus A.[3] Notwithstanding the clearly documented finding of "HYPERECHOIC SMALL BOWEL", the defendant failed to perform any of the necessary testing which would have clearly shown that both babies were infected with CMV. At his deposition, [DOCTOR] testified that he had no specific recollection of this case, or reading this ultrasound film or preparing the report.[4]

---

[2] The plaintiffs' experts agree that a finding of echogenic bowel should have triggered further testing that would have revealed the CMV. The defendant's experts do not seriously dispute this [DEFENDANT]ment.

[3] For Fetus B, the report notes: "Prominent bowel – see twin A anatomy comments"; *see* Report, attached hereto as Exhibit B.

[4] *See* excerpt of [DOCTOR] deposition, attached hereto as Exhibit C.

Notwithstanding [DOCTOR] sworn deposition testimony, on July 25, 2019, over a year after his May 21, 2018 deposition, the defendant filed an interrogatory response suggesting that [DOCTOR] was retracting and changing his sworn deposition testimony, as well as contradicting the clear documentation in his report. The interrogatory response reads:

> After review of the entries by the ultrasound technologist (sonographer), [DOCTOR] found no hyperechoic bowel in either twin. [DOCTOR] deleted an informational box captioned “hyperechoic bowel" pulled down into the report by the technologist, but he did not see the second identical informational box in the other fetus’ report findings and, therefore, failed to delete this second informational box."[5]

[DOCTOR] appears to suggest that his non-existent memory was somehow resurrected by a review of the entries of the ultrasound technologist. It is by no means clear as to what entries he is referring, although whatever allegedly jogged his memory was just as available to him before his deposition as after. Needless to say, such a complete reversal of a signed medical report and sworn deposition testimony leads the plaintiff to seriously question [DOCTOR]’s veracity and whether he was forthcoming and honest in *ether* his sworn deposition testimony *or* written discovery. [DOCTOR]’s credibility is very much in issue.

Fortunately, Congress enacted legislation to directly address this type of situation, by tracking the evolution of electronic medical documents. In the present case, the audit trail will show whether the sonographer entered “HYPERECHOIC SMALL BOWEL” for both babies, and it will further show whether [DOCTOR] deleted the entry for one baby, as he now claims, and the source of the referential information in

[5] *See* defendant’s responses dated July 25, 2019 to the Requests for Production dated April 29, 2019, attached hereto in relevant part as Exhibit D.

Baby B's report. In short, the audit trail will either corroborate or disprove the latest rendition of events now being offered by [DOCTOR]. As such, the audit trail is a critically important piece of evidence, which should be produced by the defendant.

Accordingly, the plaintiffs respectfully urge the Court to order that the defendant produce the audit trail for the October 2, 2014 ultrasound.

II. LAW AND ARGUMENT

A. Standard of Review

Practice Book § 13–14(a) provides in pertinent part that a trial court "may on motion [to compel production], make such order as the ends of justice require." "Consequently, the granting or denial of a discovery request rests in the sound discretion of the court ..." (Internal quotation marks omitted.) *Berglass v. Berglass*, 71 Conn.App. 771, 786, 804 A.2d 889 (2002).

B. The Importance of the Metadata in Electronic Medical Records

In response to the plaintiffs' requests, the defendant has provided two documents – attached hereto as Exhibits E and F. Though the defendants offered no clear explanation for either document, both appear to be "access logs" – Exhibit E for the PACS transponder system and Exhibit F for the "Observer" software which runs on a laptop connected to the ultrasound machine and is used to generate the ultrasound report. Neither complies with the Practice Book requirements of fair production; and neither complies with the HIPAA requirements for the preservation of audit trails in electronic medical records.

"Depending on the circumstances and the needs of the case, a particular piece of metadata may be critical . . . ." *The Sedona Principles*, 19 Sedona Conf. J. 1, 170 (2018) (discussing Principle 12, pp. 169–186)(The Sedona Principles have been held to be the leading authority on electronic document retrieval and production.[6]). Further, the principles state that:

> [A]side from potentially bearing upon the merits of the case, metadata also may play a functional role in the usability of [electronically stored information]. For example, system metadata may allow for the quick and efficient sorting of files by virtue of the dates or other information captured in the metadata. Application metadata may be critical to allow the functioning of routines within the file, such as the coding that makes documents display in a certain way to the user. . . . In addition to application and system metadata, some [electronically stored information] in its native format will contain user created data that may not be apparent on the face of the document when printed . . . .
>
> *Id.* at 170–171 (2018).

An electronic medical record (EMR) audit trail is considered system metadata because it contains "a record of every change or addition to an electronic medical record" and "includes the identification of the terminal used to access the record and the date, time, and author of the change or addition to the electronic medical record." Jeffrey L. Masor, "Electronic Medical Records and E-Discovery: With New Technology Come New Challenges," 5:2 Hastings Sci. and Tech. L. J. 245, 254 (2013) (citations omitted). Audit trails can demonstrate whether records have been changed, notes have been added, or items have been deleted from the electronic medical record. However, audit trails provide much more than simply proof of alterations. These audit trails identify

[6] *See generally* John B. v. Goetz, 531 F.3d 448 (6th Cir. 2008); Ford Motor Company v. Edgewood Properties, Inc., 257 F.R.D. 418 (D.N.J. 2009); William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Company, 256 F.R.D. 134 (S.D.N.Y. 2009); Aguilar v. Immigrations and Customs Enforc. Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350 (S.D.N.Y. 2008).

who accessed the patient's records, when they were accessed, who authored each entry, when and from what terminal.

ASTM E2147-01 also lays out a national standard specification for audit trails for use in health information systems.[7] According to the ASTM standard, the audit trail must capture the date and time of the access event and exit event; patient identification information unique to each patient; user identification unique to each health care provider; access device from which the user is accessing the system; type of action completed, including addition, deletion, change, query, print, copy, or other; identification of the patient data that is accessed, such as demographics, pharmacy data, test results, imaging, or transcribed notes; source of access application; and reason for access indicated by the user.

The access logs produced by the defendants provide **none** of this required information. Rather, Exhibit E indicates only a series of "log-ins" between 5:08 and 5:10 p.m. on October 2, 2014, and fails to reflect any access or editing by Ms. Steinhart (the sonographer who conducted the ultrasound). Exhibit F provides a brief and seemingly incomplete "list" of accesses – none of which include access by [DOCTOR], or any other physician. Interestingly, every other date of service referenced on Exhibit F appears to have a physician log-in; and [DOCTOR]'s name appears on the concurrently produced Exhibit E. There is no indication of what, if anything, was completed, edited, changed, accessed or reviewed concomitant with these "log-ins" on either Exhibit, nor – as to Exhibit F – any time code indicating when the software was accessed at all. In short, both exhibits raise many more questions than they provide adequate answers.

[7] ASTM refers to the American Society for Testing and Materials, which is an international standards organization, that develops and publishes consensus technical standards.

And neither appears to indicate *any* of the relevant information HIPAA demands be preserved.

Audit trails show *who* has accessed a computer system, *when* it was accessed, and *what* operations were performed, including input and deletion. Access logs, on the other hand, document and maintain a record of access to confidential health care information, and little else.

The two documents produced by the defendant are crude, unintelligible and inadequate. They do not fulfill the requirements of full and fair discovery, and they do not represent the audit trail the defendant is required to maintain under HIPAA.

C. HIPAA and the HITECH Act Require Preservation of the Audit Trail

The Health Insurance Portability and Accountability Act (HIPAA) gives patients a right of access to their entire medical record. 45 C.F.R. § 164.524(a)(1) states:

> (1) Right of access. Except as otherwise provided… 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, for as long as the protected health information is maintained in the designated record set…

Since 2003, the HIPAA Security Rule has required that hospitals like the defendant undertake regular monitoring of system activity, including audit logs and access reports by IT personnel or compliance officers, on a quarterly basis (if not more frequently) as well as the implementation of software and procedural mechanisms to record and examine system activity. 45 C.F.R. §§160, 162, 164 (2014); 45 C.F.R..§ 164.308(a)(l)(ii)(C); 45 C.F.R. *§* 164.312(b). More specifically, Section 164.132(1)(b) provides that audit controls are required. Under HIPAA, hospitals must " implement hardware, software and procedural mechanisms that record and examine activity and

information systems that contain or use electronic protected health information." 45 C.F.R. § 164.132(1)(b).

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to promote meaningful use of healthcare technology. 42 USC §300jj (2014), §17901(2014). The HITECH Act specifies that EMR Systems must satisfy certain requirements such as recording access to patient records, showing who viewed or changed information, when this was done, and from what location. Specifically, 45 C.F.R. § 170.210 sets forth the standards for health information technology to protect electronic health information created, maintained and exchanged. Subsection (b) provides:

> *Record actions related to electronic health information.* The date, time, patient identification, and user identification ***must be recorded when electronic health information is created, modified, accessed, or deleted;*** and an indication of which action(s) occurred and by whom must also be recorded. (emphasis added).

Together, the HIPAA Security Rule and the HITECH Act provide a legal framework that *requires* organizations using EMRs to track and maintain a log of all access and changes to electronic records. Withholding the data violates a patient' s right of access to her complete medical file. The federal regulations make clear that the standards were established to protect the health information - information regarding the care of the patient for whom the record was created.

HIPAA set the national standard for maintaining patients' medical information, including electronic data. One of its purposes was to ensure that medical records could not be altered without detection, to "protect the security and privacy of individually identifiable health information." 42 U.S.C.A. §1320d-2(d)(2); *See also, R.K v. St. Mary's*

Med Ctr., Inc., 735 S.E.2d 715, 720 (W.Va. 2012), *cert. denied,* 133 S.Ct. 1738 (2013). HIPAA applies to any health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. 45 C.F.R. § 160.102(a)(3).[8]

D. Metadata, Including Audit Trails, Is Fairly Subject to Discovery

1. Connecticut Practice Book § 13-9 Requires EHR Production

The plaintiffs' requests fully comply with the Practice Book requirements. Practice Book § 13-1 specifically allows for the production of electronic health records (EHR) metadata through its definitions, which allow for the production of an electronic writing and/or data and the production of such in its "native form"[9] pursuant to Practice Book § 13-9 (e). Furthermore, metadata is part of the functioning of an EHR during the ordinary course of business and is necessary to ascertain exactly what information was present to the defendants during the care and treatment of the plaintiffs. Practice Book § 13-9 (e) states that when information has been electronically stored the plaintiff is not constrained to delivery of records in non-native format (PDF and print files), but rather may specify the form, including in native format, that is preferred. Conn. Practice Book § 13-9 (e) (discussing that failure of the plaintiff to specify form of production of electronic documents allows production of such in ordinarily maintained form). This section of the Practice Book would be meaningless if the plaintiffs were unable to request alternate forms of the electronically stored information. Furthermore, Practice Book § 13-1 (a) states that electronically stored information "means information that is stored in an

[8] "Health care provider", "health information", "transaction", "protected health information" and "business associate" are all defined terms under 45 C.F.R. § 160.103.
[9] "Native Form" is defined as the original medium in which such data was created and stored/preserved.

electronic medium and is retrievable in perceivable form" and includes "data or data compilations, stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." *See* Practice Book § 13-1(c) (2).

2. Courts Have Repeatedly Held Audit Trails Must Be Produced

Courts nationwide have repeatedly ordered that audit trails must be produced where information contained therein is relevant to the claim or defense of either party. *Gilbert v. Highland Hospital,* 52 Misc. 3d. 555, 558-59 (Sup. Ct., Monroe County, NY 2016) ("while the *Vargas* court concerned itself with the former consideration of relevance, it is the latter consideration, the who, what and when of chart access, which was at issue here."). *See also Moan v. Mass. General Hosp*., No. 15-CV-1122-H, 2016 WL 1294944 (Super. Ct. Mass. Mar. 31, 2016) (defendant hospital was ordered to produce all audit trails or other documents sufficient to identify each person who accessed the patient's EMR; the periods of time they had accessed it; what they had accessed; and, all changes or additions made to the EMR by each person at each time in both paper *and* electronic form).

In *Baker v. Geisinger Community Medical Center,* 2017 WL 1293251 (Pa.Com.Pl., April 7, 2017), the plaintiff produced discovery depositions reflecting disparities between the testimonial recollections of her healthcare providers and the entries contained in her hospital chart. The court granted the plaintiff's motion to compel the audit trail up to the day preceding oral argument on the motion, finding that the "audit trail will reveal which healthcare providers received or reviewed what medical

information, when they possessed that knowledge, where and when they made their respective entries, and whether those entries were ever edited or altered." *Id,* 4-5.

In *Fernandez-Rajotte v. Dartmouth Hitchcock Medical Center,* 2014 WL 12540494, (N.H. Super. 2014), the plaintiff brought an action for medical malpractice based on complications arising from surgery. The plaintiff requested that the defendant produce an un-redacted copy of the audit trail for the medical records related to her surgery. The court found the medical records pertinent to the surgery were at the heart of the action and the audit trail represented a log of the employees accessing the records, the parts of the records accessed, and the actions taken with the record. The court ordered disclosure of the audit trail since it would "demonstrate whether a [medical center] employee had edited or modified [the plaintiff's] medical records in any way, which would be relevant to the veracity of the information contained in her records." *Id.* at 5. In *Osborne v. Billings Clinic*, 2015 WL 141626 (D.C. Mont. 2015), the hospital argued that audit trails were implemented for quality control purposes and were therefore not “healthcare information” required to be included in a “designated record set” per 45 C.F.R. § 164.524(a)(1). The court rejected this argument, and held that the audit trail “data” related to the patient’s hospital care and treatment was discoverable. In *Hall v. Flannery*, 2015 WL 2008345 (D.C. Ill. 2015), the hospital argued that audit trail logs and metadata associated with the patient’s medical chart were subject to peer review privilege and work product doctrine. The court disagreed, and held that State statutes providing the privilege did not bar access to the audit trail information, nor was such information protected by the work product doctrine.

In *Gilbert v. Highland Hospital,* 52 Misc. 3d. 555, 558-59 (Sup. Ct., Monroe County, NY 2016) the court dismissed the defendant's argument that the plaintiff's request for the audit trail was a "fishing expedition." Instead, the court granted the plaintiffs motion to compel the production of the audit trail to show the sequence of events related to the use of and access to the decedent's medical records. In finding that the request was not a fishing expedition, the court recognized that the plaintiff requested the audit trail to determine the level of involvement of the emergency room doctor with the decedent's care knowing that it existed because it was mandated by federal law. *Id.* In a lengthy opinion, the Court recognized that any medical provider maintaining an electronic records must also maintain an audit trail pursuit to the requirements of 45 C.F.R. § 164.312. The court rejected defense arguments that the audit trail information was not “material and necessary”, that the plaintiff’s request for the documentation constituted a “fishing expedition”, and that plaintiff was required to make a showing that there was an issue about authenticity of the hospital records already produced as a predicate to obtaining the audit trail information. The Court stated that “if the authenticity of a document is questioned, *or if establishing who received what information and when is important to the claims or defenses of a party,*” then the system metadata is inarguably relevant and the defendant was required to produce it. *Id.* at 400; emphasis in original.

In discussing the discoverability of audit trail documentation, the court characterized the information it contains as follows:

> [An] audit trail is a form of metadata created as a function of the medical provider’s computerization of medical records. Metadata is “’secondary information,’ not apparent on the face of the document, ‘that describes an electronic document’s characteristics, origins, and usage’” (*Matter of Irwin v.*

Onondaga County Resource Recovery Agency, 72 AD3d 314, 320, 895 NYS2d 262 [4th Dept 2010]), or, to put it more succinctly, metadata is, "data about data." In discussing the audit trail for computerized medical records, one commentator described it as follows:

> "The audit trail is a document that shows the sequence of events related to the use of and access to an individual patient's EHR [electronic health records]. For instance, the audit trail will reveal who accessed a particular patient's records, when, and where the health care provider accessed the record. It also shows what the provider did with the records – e.g., simply reviewed them, prepared a note, or edited a note. The audit trail may also show how long the records were opened by a particular provider. Each time a patient's EHR 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 EHR are permanently documented in the audit trail. Providers cannot hide anything they do with the medical record. No one can escape the audit trail." (Alice G. Gosfield, Health Law Handbook § 10:9[2011 ed] ["The positive effect of EHRs on reducing health care provider liability – The audit trail"].)
>
> *Id.* at 556-557.

The court granted the plaintiff's Motion to Compel the audit trail documentation over defense objections.

In *Picco v. Glenn*, 2015 U.S. Dist. LEXIS 58703, 2015 WL 2128486 (D.C. Colo. 2015), the Court held that the plaintiff was authorized to have his expert witness conduct a complete forensic examination of his medical records maintained on the hospital's electronic records system, specifically including any audit trail information. In reaching its holding the court cited the following provisions of federal law requiring the maintenance of audit trail records: 45 C.F.R. §§ 164.105, 164.304, 164.306, 164.308, 164.312, and 170.210, setting forth the types of information a hospital is required to record and maintain; 45 C.F.R. § 164.306(a)(1), commanding a hospital to "ensure the confidentiality, integrity, and availability of all electronic protected health information [that it] creates, receives, maintains, or transmits"; 45 C.F.R. § 164.304, providing that

“availability” in this context means “that data or information is accessible and useable upon demand by an authorized person”; 45 C.F.R. § 164.308(a)(7)(ii) provides that a hospital ... must "[e]stablish and implement procedures to create and maintain retrievable exact copies of electronic protected health information”; 45 C.F.R. § 164.312(b) provides that a hospital ... must "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"; 45 C.F.R. § 170.210(b) requires that "[t]he date, time, patient identification, user identification ... must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must be recorded"; 21 C.F.R. § 11.10(e) provides that a hospital shall employ procedures and controls including the "[u]se of secure, computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records" and that "[s]uch audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records ..."; 21 C.F.R. § 11.10(k)(2) states that a hospital shall employ appropriate controls over systems documentation including "[r]evision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation"; 42 U.S.C. §1320d-2(d)(2) provides that a hospital ... "shall maintain reasonable and appropriate administrative, technical, and physical safeguards-(A) to ensure the integrity and confidentiality of the [health] information; (B) to protect against any reasonably anticipated-(i) threats or hazards to the integrity of the information; and (ii) unauthorized uses or disclosures of the information ...”; and 42 U.S.C.§1320d(6)

[provides that] "individually identifiable health information" is defined to include "any information ... created or received by a health care provider ... [that] relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and . . . identifies the individual; or . . . can be used to identify the individual".

Courts around the country, including in Connecticut, have also required production of metadata *in native format,* so that the metadata is reasonably usable.

> Accordingly, the court will grant the plaintiff's request for native format. *See, e.g., In re Porsche Cars North America, Inc. Plastic Coolant Tubes Products Liability Litigation,* 279 F.R.D. 447, 450 (S.D.Ohio 2012) (court granted plaintiffs' request for native format "absent a showing by [defendant] that such a production would be unduly burdensome); *Romero v. Allstate Ins.* Co., 271 F.R.D. 96, 107 (E.D.Pa.2010) ("the Court finds that Plaintiffs are entitled to have documents produced in native format with their associated metadata" where defendants do not allege that they will be financially burdened or prejudicially harmed by the production of metadata); *Camesi v. Univ. of Pittsburgh Med. Ctr.,* No. CIV.A.09–85J, 2010 WL 2104639, at *7 (W.D.Pa. May 24, 2010) (ordering defendants to produce ESI in its native format "absent a clear showing of substantial hardship and/or expense"); *In re Netbank, Inc. Secs. Litig.,* 259 F.R.D. 656, 681–82 (N.D.Ga.2009) ("Although the Defendants have listed a number of hypothetical problems with providing documents in native format, they have not asserted these to be actual problems arising in the present case.... [T]he court is confident that the precision of record citations can be appropriately dealt with should [plaintiff] desire to use any of the documents at issue as exhibits or evidence.... The Defendants having given no good reason why they should not produce [plaintiff's] requested documents in native format, the Motion to Compel production of ESI information in native format is granted.").

Saliga v. Chemtura Corp., No. 3:12CV832 RNC, 2013 WL 6182227, at *2 (D. Conn. Nov. 25, 2013). *See also Innis Arden Golf Club, Inc. v. O'Brien & Gere Engineers, Inc*., No. CV106006581, 2011 WL 6117908, *3 (Conn. Super. Ct. November 18, 2011) (Metadata is an important part of the orderly production of the electronic disclosure).

> Native format production also complies with the Federal Rules of Civil Procedure and this case's ESI order. Moreover, the Court finds that metadata and native format production are relevant and proportional to the needs of discovery. It is untenable to assert in this technology-driven age of litigation that images of electronic documents provided in TIFF and PDF form offer all of the relevant information possible. The metadata that is not visible in TIFF and PDF productions, but is visible in native format production, is relevant information. Therefore, the Court GRANTS Plaintiff's motion on this issue.

Bailey v. Alpha Technologies Inc., 060117 WAWDC, C16-0727-JCC (W.D. Wash June 1, 2017).

E. Full and Fair Discovery Requires the Production of the Audit Trail

In the present case, the relevance of these documents is not reasonably in question. The primary defense by the [DEFENDANT] as now asserted by [DOCTOR] is that he did not intend to document in his report hyperechoic bowel in either fetus. This position is wholly inconsistent with the report produced, which [DOCTOR] himself signed off on, and which clearly indicates in bold letters “HYPERECHOIC BOWEL”. [DOCTOR] *now* apparently claims that he committed a “scrivener’s error”. The defendant asserts that while the ultrasound technician entered “hyperechoic bowel” as a finding for both babies, [DOCTOR], upon review of the ultrasound images, claims he found no evidence of the same. As such, [DOCTOR] claims to have intended to delete the findings from both babies’ charts, but accidentally only deleted it from Baby B. The audit trail will either confirm or deny [DOCTOR]’s story.

In order to reconcile the discrepancies between the disclosed records and [DOCTOR]’s newly developed theory, and to discover fully what occurred during the ultrasound procedure and subsequent care, the plaintiff must be permitted to conduct full and fair discovery – including a review of the electronic medical record and associated audit trail. Moreover, the plaintiff is entitled to such discovery under the

provisions of HIPAA and the Connecticut Practice Book. Audit trails are part of the plaintiff s medical records. Electronic Medical Records replace paper records with computerized record-keeping to document and store a patient' s medical information. The audit trail is the metadata for a patient's electronic chart that documents every time the chart is accessed or altered. "Every time a user views, edits, prints, deletes, downloads, exports, or otherwise manipulates any part of a patient's electronic medical record (EMR), the system makes a contemporaneous record of that activity as it occurs. This audit trail provides direct evidence of exactly what was done - when, where, and by whom - to a patient' s EMR."[10] It is a precise and dynamic system of how patient care information is created. The EMR keeps audit trails of every edit of the record. An audit trail also "includes the identification of the terminal used to access the record and the date, time and author of the change or addition to the electronic medical record."[11] The audit trail is the *only* objective account of when and how a patient's data was viewed, charted and/or altered. The metadata related to the medical record, in short, cannot be separated from the record itself.

Therefore, the audit trail in this case, which details modification, accessions or deletions of the chart, is well within Connecticut's discovery parameters allowing parties to obtain information that is likely to lead to the discovery of admissible evidence. A full and complete EHR audit trail is the only way to authenticate an electronic medical record. Without an audit trail, the record cannot be authenticated as complete and free from alteration. Its production is essential for evidentiary purposes, without exception.

---

[10] Jennifer Keel, " Follow the Audit Trail," The Journal of Legal Nurse Consulting, Vol. 25, No. 2 at p. 26 (May 2014).

[11] Jeffrey L. Masor, " Electronic Medical Records and E-Discovery: With New Technology Comes New Challenges," 5:2 Hastings Sci. & Tech. L.J. 245, 254 (Summer 2013).

Therefore, the plaintiff respectfully requests that the Court issue an order requiring the defendant to produce any and *all* audit trail evidence, in its native format, for full and complete compliance with the plaintiffs' requests for production.