Audit Log Demands During Litigation: Response Conundrums from a Compliance Perspective

Carey Cothran, MJ, CHC, CHRC
Executive Director, Corporate Compliance & Audit
WellStar Health System

Emily Reilly, JD, CHC, CHPS
Regulatory Corporate Compliance Administrator
WellStar Health System

Prologue

ACME Health System: December 2012

- **Patient:** Sixteen year old boy who suffered hemorrhagic stroke is undergoing repair of the malformed vein mass. During embolization of the malformed vein mass a tragic medical error occurred.
- **Prognosis:** Lifetime paralysis, aphasia, memory loss, impaired cognitive function.
- **Litigation:** Electronic health record (EHR) and accompanying audit logs requested during discovery.
- **The physician:** Found guilty of medical malpractice due to a failure to calibrate equipment.
- **Evidence:** The electronic health record (EHR) audit logs indicate a failure to calibrate equipment before the procedure.

2

Introduction

The increasing use of electronic health records (EHR) means an increased ability to electronically track activities that occur within a specific medical record.

Unintended Consequences of EHRs

- Medical malpractice attorneys are being encouraged to use audit logs to obtain evidence for use in medical malpractice litigation. (1)
- The Office of the Inspector General (OIG) and Centers for Medicare and Medicaid Services (CMS) are encouraging the use of audit logs for identifying fraudulent coding and billing. (2)

3

Audit Logs: Inherent Problems

The use of audit logs to prosecute healthcare organizations or providers for malpractice or fraudulent coding/billing practices is fraught with inherent problems.

Inherent Problems

- Consistency
- Integrity
- Interpretation
- Retention requirements
- Burdensome

4

Definitions

Understanding the audit log conundrum facing healthcare providers begins with understanding the definitions and technical differences between metadata, audit logs or audit trails, and access logs and reports.

- **Metadata:** Metadata is the computer generated and stored "data about other data."
  - Where it was collected, who created it, when it was created, etc.
- **Audit logs/audit trails:** Audit logs/audit trails are a type of metadata that provide documentation of sequential activity within a software application including when the data was created, accessed, revised, etc. (3)
- **Access logs/reports:** An application user access log can be used to create a report of all users who have accessed a specific patient's medical record within an EHR.(4)

5

Potential Uses: Investigations and Litigation

When analyzed properly and within appropriate context, audit logs can provide a useful tool for the investigation and prevention of different types of theft and fraud.(5)

- Theft of patient data
- Inappropriate access (privacy violations)
- Fraudulent billing practices
  - Copy/paste
  - Auto-populate

6

Compliance Conundrums: Integrity

EHRs and Audit Log Integrity Issues

- **Author Identification:** multiple providers can add documentation to the same progress note without allowing or requiring each provider to sign their entry, making it "impossible to verify the actual service provider or the amount of work performed by each provider."(6)
- **Automated Change of Note Author**: automatic author change to the current user of the note, deleting any reference to the original author.
- **Automated Date Assignment:** some systems automatically date an entry while others allow users to change the documentation entry date to the treatment date or the date of service, which may misrepresent the sequence of treatment events.

EHRs and Audit Log Integrity Issues

- **Amendments:** allows providers to amend a record without requiring a date entry or notation that this is a change from the original entry.
- **Disabled Audit Logs:** 2013 OIG survey where nearly half (44 percent) of the hospitals that participated in the survey reported they can disable and/or delete their audit logs.(7)
- **FDA:** "…Health information technology software is a medical device… [but] to date, FDA has largely refrained from enforcing our regulatory requirements." EHRs remain "experimental" according to the FDA.(8)

9

Compliance Conundrums: Disparate Regulations

10

Disparate Regulations for Audit Requirements

- **HIPAA Security Rule:** Requires "audit controls" by implementing "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."
  - Does not specify how this should be accomplished, or who should examine the data. Different employee functions may recognize different problems: IT may recognize hacking, but miss fraudulent billing issues or clinical data integrity issues.

Disparate Regulations for Audit Requirements

- **Meaningful Use:** Audit log content requirement for Meaningful Use certification set by referencing the American Society for Testing and Materials (ASTM)
  - Required: date, time, patient ID, user ID, type of action (addition, deletion, change, queries, print copy)
  - Optional: device used for access, identification of the patient data accessed, source of access, reason for access.
  - Only if you "elect" to participate in Meaningful Use!
- **Federal Rules of Evidence**
  - Standard for validating business records: "evidence describing a process or system and showing that it produces and accurate result."
  - "A record of an act, event, condition, opinion, diagnosis [is admissible] if … (E) neither the source of information nor the method or circumstances of preparation indicate a lack of ***trustworthiness***."

Disparate Regulations for Retention

- **HIPAA Security Rule:** 6 year retention requirement is for documentation created pursuant to the rule (i.e., incident reports, policies, sanctions, etc.)
- **HITECH:** Accounting of Disclosures requirement vs. access report
  - Accounting of Disclosures – 6 years
  - Access Report – disclosures through an EHR – 3 years
- **Meaningful Use:**
  - Audit log retention requirement – 6 years
  - But, participation in Meaningful Use is voluntary

13

Disparate Regulations for Retention

- **False Claims Act:** OIG "noted that auditors use the logs to authenticate medical records supporting claims made to Federal Health Care programs" and indicated "an effective audit of claims based on EHRs requires the use of the audit log."
  - 6-10 years statute of limitations
  - Treat audit logs like part of the medical record?
  - Also consider state law retention requirements
- **OIG and CMS:** recommend retaining audit logs as long as required to retain clinical records to prove medical necessity/accuracy of coding and billing

14

Compliance Conundrum: Case Law

Case Law

Peterson v. Matlock

- Plaintiff sought to compel production of HER records in "native readable format" or by "searchable headings."
- Records were produced in PDF format and organized in chronological order, which were difficult to "navigate and interpret," according to Plaintiff.
- Plaintiff claimed that the records produced were not in the format that the provider views when providing treatment and that the record is missing "the functionality, searchable data points, and metadata which are part of the electronic medical record and are available to a provider."
- Plaintiff had an expectation that the audit logs would be produced as a matter of course based on the request for the EMR alone.
- Defendants explained that their particular HER provides details about what a user did while logged on, but does not have the details indicating which individual user actually was logged on.
- Court ruled that Defendants must produce ERH and audit logs, but not in the format requested by Plaintiff.(9)

Case Law

Hall v. Flannery:

- Plaintiff alleged receiving two "different" medical records related to care, believing that the medical records had been improperly altered by the Defendant.
- Defendant argued that audit logs for access to the medical record after the treatment period had ended were not discoverable and may be protected by peer review or subject to work product privilege.
- Court required that Defendant produce the audit logs.
- Court indicated the audit trail is just one aspect of a patient's medical record "that is generated in the ordinary course of the hospital's business."
- Arguably, this opinion could stand for the proposition that a request for the "entire medical record," now includes audit logs.(10)

17

Case Law

Vargas v. Lee:

- Plaintiff's request for audit logs as part of medical record is denied.
- Court found that Plaintiff had "not distinguished the audit trail's utility from that of its corresponding EMR" and "a party does not have the right to uncontrolled and unfettered disclosure."
- The audit trail may be pertinent if the authenticity of documentation was in question but, details about the patient's treatment were already available in the medical records previously produced.
- That the audit trail may contain information on the "timing and substance of plaintiff's care," is not sufficient to compel production. (11)

18

Case Law

Green v. Penn. Hosp.

- Allegation that certain reports had been altered or deleted from the application used by the hospital.
- An "informatics expert" testified that she "had never before worked with the particular system used by the Hospital as a nurse, had never analyzed or worked with it before in her capacity as an informatics consulting expert, and had never before seen the audit logs generated by [the hospital]."
- The expert stated, "I can't give you specifically what was altered, nor by whom… I can only look at what the audit trail shows as people having documented and then trying to track it back to the medical record and not being able to find entries that support that notation on the audit log."
- The Court recognized that these statements did not fall within the domain of expert testimony, and precluded it from the case. (12)

19

Case Law

United States ex rel. Sheldon v. Kettering Health Network

- Audit logs not requested, but of interest for those familiar with Meaningful Use.
- Qui tam case where relator alleged False Claim Act violation based on a HIPAA Privacy/Security violation.
- Plaintiff alleged that because her PHI was able to be inappropriately accessed and re-disclosed by an employee, the covered entity did not conduct their HIPAA risk assessment in accordance with HITECH standards, but accepted Meaningful Use incentive payments anyway.
- Court dismissed allegations, finding that "attestation of compliance [with the HITECH Act] is not rendered false by virtue of individual breaches." (13)

20

Compliance Conundrum: Burdens to Healthcare Providers

Burden to Healthcare Providers

- **Costly data storage**
  - From EPIC, EHR Vendor to the OCR HIT Policy Committee: access logs are quite large and storing them often "takes up more than 50% of an organization's reporting database capabilities."
- **Expanded definition of medical record**
  - See Hall v. Flannery: In their opinion, the court cited Allen v Crowell-Collier Pub Co. stating that "the words 'material and necessary' are to 'be interpreted liberally to require disclosure, upon request, of any facts bearing on the controversy which will assist in preparation for trial by sharpening the issues and reducing delay and prolixity"; indicating that the "test is one of usefulness and reason."

Burden to Healthcare Providers

- **Rapid technology advancement**
  - To meet OIG and CMS guidelines for storing audit logs, as if they were the clinical record results in "saving large amounts of data that quite likely will be inaccessible and/or unusable in a few years" due to rapid advances in technology.
- **Multiple EHR applications:**
  - Hospitals and health systems often use multiple EHR systems requiring the maintenance and expertise of audit logs for each application.
- **Qualified informatics experts:**
  - Very expensive to hire individuals or entities with the expertise to retrieve and accurately interpret audit log data.

It seems intuitive to think that the ability to store, search and retrieve huge amounts of data would serve as a great resource savings in time, effort, and money, but unfortunately when it comes to the discovery of EHR audit logs, it is exactly opposite.(14)

23

Epilogue

In the Prologue, a physician is found guilty of malpractice based on timestamps from the EHR audit logs…but what if:

- There had been a system patch or a version upgrade?
- The software linking the equipment to the EHR had undergone a recent upgrade which then threw off the synchronization of the audit logs systems to the clinical systems?

It would appear from the audit logs that the physician failed to perform a mandatory system check that resulted in an unfavorable patient outcome.

An excellent physician would have been held accountable and suffered terrible consequences based on data that was neither reliable nor trustworthy.

24

Conclusion

- EHRs were not be designed with discovery and litigation in mind, but were designed for the flow of digital patient data to encourage integrated delivery of treatment to improve the health and reduce costs.
- Audit logs can be misinterpreted when viewed outside of the context of their intended environment.
- Healthcare organizations face increased risks for medical malpractice in addition to "increased scrutiny, investigation, and even prosecution by the very government that promoted the switch to EHRs in the first place."

25

Take-Aways

- Determine the risk to your organization by reviewing relevant retention laws and create policy for retaining audit logs.
- Make a plan for dealing with requests for audit logs pursuant to subpoena.
- Retain and/or train your own experts who can accurately interpret audit logs for your EHRs, and be familiar with exactly what your audit logs can and cannot tell you.

26

References

1. Jennifer Keel, *Follow the Audit Trail*, Trial 29–33 (May 2014); Mark R. Bower, Nursine S. Jackson & Jerry I. Meyers. *Another Trip Down the Audit Trail*, AAJ Prof'l Negligence Newsletter (Fall 2011).
2. Centers for Medicare and Medicaid. Documentation Integrity in Electronic Health Records. June 2016.(2) https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/ehr-docintegrity-factsheet.pdf Ret. Sept. 17, 2016
3. Lee, Patricia A. New Jersey Law Review. Page 2. September 7, 2015. http://www.connellfoley.com/sites/default/files/Lee%20Sept%207%202015%20Handling%20EHR%20System%20Audit%20Trails%20and%20Self-Audits.pdf Retrieved Oct. 1, 2016. Sanford PPT presentation. NIST website. http://csrc.nist.gov/news_events/hiipaa_june2012/day1/day1-3_cmatson_establishing-access-auditing.pdf Ret. Oct. 23, 2014.
4. Epic letter to the OCR. Sept. 2013. https://www.healthit.gov/FACAS/sites/faca/files/0930_EpicHITPCAoDTestimony.pdf Ret. October 23, 2016.
5. Centers for Medicare and Medicaid. Program Integrity Issues in Electronic Health Records: An Overview. Page 6. https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/ehr-provider-booklet-overview.pdf . Ret. Oct. 1, 2016.
6. CMS Detecting and Investigating Unauthorized Access to Electronic Health Records— A Case Study. p.7. https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/ehr-casestudy-booklet.pdf. Ret. Oct. 1, 2016,
7. ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE: ARTICLE: ELECTRONIC HEALTH RECORDS SYSTEMS: TESTING THE LIMITS OF DIGITAL RECORDS' RELIABILITY AND TRUST, 12 Ave Maria L. Rev. 257,pp.261,262. Ret. Oct. 2016
   U.S. Department of Health and Human Services. Office of the Inspector General. (December 2013). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 15–16; Appendix A).
   http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf Ret. Oct. 1, 2016.

27

References

8. Miller, Clay. Weisbrod, Les. ELECTRONIC RECORDS AND AUDIT TRAILS. https://www.millerweisbrod.com/docs/max/Electronic_Records_and_Audit_Trails.pdf Ret. Sept. 25, 2016.
9. Peterson v. Matlock, 2014 U.S. Dist. LEXIS 152994 *, 2014 WL 5475236 (D.N.J. Oct. 29, 2014) p.7.
10. Hall v. Flannery, 2015 U.S. Dist. LEXIS 57454 *, 2015 WL 2008345 (S.D. Ill. May 1, 2015) p.11.
11. Vargas v Lee, 2015 N.Y. Misc. LEXIS 2176, 2015 NY Slip Op 31048(U) (N.Y. Sup. Ct. June 5, 2015) p.1.
12. Green v. Pa. Hosp., 2013 Phila. Ct. Com. Pl. LEXIS 108, 30 Pa. D. & C.5th 245, 2013 WL 8596359 (Pa. C.P. 2013) p.9.
13. Byrne, Terrence K., The Federal Rules Of Civil Procedure, Electronic Health Records, And The Challenge Of Electronic Discovery. Cleveland State University. Journal of Law and Health, p.379. 2015. http://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=1465&context=jlh Ret. Oct. 1, 2016
14. Brouillard, Chad P., Esq., "EHR Audit Trails Might Reveal More Than You Think: Hall v. Flannery, a Sign of the Times". Inside Medical Liability. 2015. http://www.mgma-gkc.com/wp-content/uploads/2015/10/IML-3Q-2015-pp-18-20.pdf Ret. Nov. 26, 2016
15. Szerejko, Joseph D.,NOTE: Reading Between the Lines of Electronic Health Records: The Health Information Technology for Economic and Clinical Health Act and Its Implications for Health Care Fraud and Information Security, 47 Conn. L. Rev. 1103 p.1152

28