Role of Audit Trails in Litigation and the Implications of OCR Audit Controls Enforcements

March 9, 2017
FairWarning Executive Series Webinar
Today’s Speakers

Chad P. Brouillard
Attorney at Foster & Eldridge, LLP

Nicholas Heesters, JD, CIPP
Health Information Privacy & Security Specialist
U.S. Department of Health and Human Services, Office for Civil Rights

Kurt J. Long
Founder and CEO
FairWarning
FairWarning Executive Series Webinar Agenda

- Role of Audit Trails in Litigation
- Updates from OCR on Compliance, Enforcement and Cybersecurity
- Implications of OCR Audit Controls Enforcements
- Prevalent Challenges in Audit Controls and Identity Intelligence
Audit Trails in Medical Liability Litigation

Chad P. Brouillard
Attorney at
Foster & Eldridge, LLP

Twitter: @chadbrouillard
LinkedIn: linkedin.com/in/chadbrouillard
What is an Audit Trail?
An **audit trail** (also called **audit log** ) is a security-relevant chronological report(s) that provide documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event.

In the context of an **EHR**: “record that shows who has accessed a computer system, when it was accessed, and what operations were performed.”
Evolution of the Audit Trail

- Data Integrity - Metadata and audit trail used for technical purposes
- HIPAA Privacy & Security - Developed for express statutory purposes
- Depending on design may, or may not, provide information about timing of clinical acts.
Audit Trail Contents

- Type of actions:
  - additions, deletions, view, changes, queries, print, copy,
  - date and time of event,
  - patient identification,
  - user identification, and
  - identification of the patient data that is accessed.

Audit Trail Forms

- Embedded Audit Trail data
- Reports
- System-Level
- User-Level
- Chart-Level
- Filters
- Custom?
## Audit Trail Example

<table>
<thead>
<tr>
<th>Event Timestamp</th>
<th>Audit Source</th>
<th>User First Name</th>
<th>User Last Name</th>
<th>User Title</th>
<th>User Department</th>
<th>Event Name</th>
<th>Event Type</th>
<th>Event Description</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-01-02 14:41:43.0</td>
<td>Meditech</td>
<td></td>
<td></td>
<td>Pediatrics</td>
<td></td>
<td>View</td>
<td>Clinical Diagnosis</td>
<td>The FYI activity was accessed.</td>
<td>The FYI activity was accessed.</td>
</tr>
<tr>
<td>2017-01-02 14:41:43.0</td>
<td>Meditech</td>
<td></td>
<td></td>
<td>Pediatrics</td>
<td></td>
<td>View</td>
<td>Lab Results</td>
<td>The FYI activity was accessed.</td>
<td>The FYI activity was accessed.</td>
</tr>
<tr>
<td>2017-01-02 14:41:43.0</td>
<td>Meditech</td>
<td></td>
<td></td>
<td>Pediatrics</td>
<td></td>
<td>View</td>
<td>REG Account</td>
<td>The FYI activity was accessed.</td>
<td>The FYI activity was accessed.</td>
</tr>
<tr>
<td>2017-01-02 14:41:43.0</td>
<td>Meditech</td>
<td></td>
<td></td>
<td>Pediatrics</td>
<td></td>
<td>View</td>
<td>HIM Record</td>
<td>The FYI activity was accessed.</td>
<td>The FYI activity was accessed.</td>
</tr>
</tbody>
</table>

### Registration Clerk
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited
- Emergency Room: FYI activity accessed
- Emergency Room: FYI activity exited

### Family Medicine
- Chart Review: Encounters tab selected
- Chart Review: Encounters tab selected
- Chart Review: Encounters tab selected
- Chart Review: Encounters tab selected
- Chart Review: Encounters tab selected
Common Audit Trail Triggers

- Same last name as an employee
- VIP patient records
- High profile community events (bombing)
- Isolated activity after no activity for 120 days
- Records with sensitive health information such as psychiatric disorders, drug and alcohol records, domestic abuse reports, and HIV/AIDS diagnoses
- Files of minors who are being treated for pregnancy or sexually transmitted diseases
- Employee had no involvement in treating
- Terminated employees AHIMA.
Litigation Use of Audit Trails

- Discovery
- Evidentiary Concerns
Release of Information
vs.
Discovery
**eDiscovery** refers to the rules governing the disclosure of electronic data, or ESI, contained within any possible electronic medium.

Why do I need to know about eDiscovery?
Federal eDiscovery Rules

- Mandatory conference backed by financial sanctions
- Rules governing disclosure to parties and non-parties
- Consequences for the destruction of data
- Placing de facto requirements on litigants before an eDiscovery suit is filed
- New proportionality standard
Form of Request

1. All electronic records (including but not limited to provider notes, audio, video, images, graphics, recordings, spreadsheets, databases; calendars);

2. All electronic records of laboratory tests for patient

3. All electronic records concerning patient’s condition during surgery including attendance logs, interventions, monitoring, anesthesia, nursing, studies, testing, results, and the timing of each of the previously listed items;

4. All electronic records of medications or blood products ordered and/or dispensed for the patient

5. All electronic "sticky" notes, pop-up notes, and text or memo fields;

6. All electronic communications (including but not limited to electronic mail, text messages, instant messages, voice mail messages, voice recordings, and page records);

7. All system usage logs,

8. All metadata and audit trails relating to any electronically stored information described above.
eDiscovery Preparation Basics

- Data Analysis/Source Mapping
- Document Retention Plan
- Litigation Holds Procedure
- Conversations w/ Vendors & IT
How is the storage of information on an EMR different from a paper chart?
Traditional Spoliation of Evidence
Electronic Spoliation of Evidence
Legal Health Record... Or?

- What is it now in age of electronic stored information?
- Audit Trails
- External Scanned Records
- Emails
- Personal Health Records
- Chat Sessions
- Patient Portals
- Apps, Texts?
The legal definitions of a legal health records have not caught up to the electronic era.

The Legal Health Record will likely give way to the Designated Record Set

Providers can designate records in response to a routine subpoena/ROI

“Complete medical record” does not exist

Designated Record Set does not preclude further discovery
EHRs in Discovery Case Study

- Printout of record
- Audit Trail
- Screen shots
- Depositions of Clinicians, HIM Department, Vendors
- Live Access to EHR
- Custom Read Only Software
EHRs in Discovery Case Study

- Upgraded EMR from time of Care, View Changes
- Impossible to Recreate Exactly What the Clinician Saw
- Different Displays of Data Based on User
- Audit Trail Confusing w/ Baffling Time Stamps, Missing “Pending” Orders in Chart
- Puts Clinicians on Defensive about Record
EHRs as Discovery

- Increased Litigation Costs if forensics involved.
- Audit Trails now as a matter of course.
- Each system is proprietary, so expertise is local.
- A DIY Plaintiff Attorney in a position to generate confusion and costs.
- Without reliable documentation and audit data creates costly production issues.
- Vendor support is a resource.
Audit Trails – Discovery Perspective

- Courts generally view Audit Trails as discoverable.
- Courts inconsistent on application of privilege.
- Courts will tend to force healthcare defendants to create or request standard or custom report if plaintiff can show some need.
- Audit controls underpin a sound document retention and litigation holds strategy.
- Avoiding spoliation may look to reliability of audit capabilities.
- The data owner and custodian are responsible for generating, retaining and producing audit trails. Can be a double edged sword for a clinician defendant.
- Who is auditing the auditors?
Audit Trails Supporting Evidence
Evolution of Evidence

- Hearsay
- Written Documentation – Original Record
- Contemporaneous writing have an indicia of trustworthiness, reliability, business purpose = AUTHENTIC.

EHRs as Evidence

- Is the paper export “the original record”?  
  - Late Notes  
  - Auto-populated Sources  

- Asynchronous Sources  
  - Authorship Issues  
    - No author  
    - Multiple authors  
    - “Make me the author”
Evidentiary Use of the Audit Trail

- Good audit trail functionality provides a defense of the documentation.
- Legal provenance of the record.
- Objective evidence of authenticity.
- Closes the gap.
Audit Trail – Smoking Guns

• The audit trails can include details about:
  • Late entry (contemporaneous or remote)
  • Spoliation (Deleted Entries)
  • Records Tampering (Modified Entries)
  • Rule violation (Privacy & Security)
  • Privileged Review (Peer Review & Attorney Client)
Audit Trail Usability for Litigation

- Built for THAT system as implemented.
- Some Audit Functions are not setup as a default.
- Reporting may vary even within same product.
- Need for expert interpretation in context.
- Example: “null”, “pending orders”, accessing 100 records in one second, etc.
- Without experts in that system, as reliable as reading tea leaves.
Thank You

Chad P. Brouillard
Attorney at
Foster & Eldridge, LLP

Twitter: @chadbrouillard
LinkedIn: linkedin.com/in/chadbrouillard
Nicholas Heesters, JD, CIPP
Health Information Privacy & Security Specialist
U.S. Department of Health and Human Services, Office for Civil Rights

Website: http://www.hhs.gov/hipaa
Twitter: @HHSOCR
Update on Compliance, Enforcement and Cybersecurity

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services
BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY
September 2009 through January 31, 2017

- Approximately 1,825 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss account for 50% of large breaches
  - Hacking/IT account for 15% of large breaches
  - Laptops and other portable storage devices account for 28% of large breaches
  - Paper records are 22% of large breaches
  - Individuals affected are approximately 171,390,576

- Approximately 255,560 reports of breaches of PHI affecting fewer than 500 individuals

- Expect to receive over 17,000 complaints this year
500+ Breaches by Type of Breach as of January 31, 2017

- Theft: 42%
- Unauthorized Access/Disclosure: 26%
- Hacking/IT: 15%
- Loss: 8%
- Improper Disposal: 3%
- Other: 5%
- Unknown: 1%
500+ Breaches by Location of Breach as of January 31, 2017

- Paper Records: 22%
- Laptop: 18%
- Network Server: 16%
- Portable Electronic Device: 10%
- Email: 9%
- Desktop Computer: 11%
- EMR: 6%
- Other: 10%
What Happens When HHS/OCR Receives a Breach Report

• OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  • Public can search and sort posted breaches
• OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
• Investigations involve looking at:
  • The underlying cause of the breach
  • Actions taken to respond to the breach (including compliance with breach notification requirements) and to prevent future security incidents and breaches
  • The entity’s compliance prior to breach
• In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action

• In some cases though, the nature or scope of indicated noncompliance warrants additional enforcement action

• Resolution Agreements/Corrective Action Plans
  • 43 settlement agreements that include detailed corrective action plans and monetary settlement amounts

• 3 civil money penalties
2017 Enforcement Actions

• $5.5 million HIPAA settlement shines light on audit controls – February 18, 2017

• Lack of timely action risks security and costs money ($3.2M) – February 1, 2017

• HIPAA settlement demonstrates importance of implementing safeguards for ePHI ($2.2M) - January 18, 2017

• First HIPAA enforcement action for lack of timely breach notification settles for $475,000 – January 9, 2017
Recurring Compliance Issues

- Risk Analysis
- Failure to Manage Identified Risks
- Lack of Appropriate Auditing
- Insider Threat
- Business Associate Agreements
- Lack of Transmission Security
- No Patching of Software
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
Incomplete or Inaccurate Risk Analysis

• Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

• Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

• Examples: Applications including EHR/PM systems, billing systems, office productivity software; documents and spreadsheets; computer systems including database servers, web servers, fax servers, backup servers; local servers, workstations and laptops as well as cloud based and virtual systems; medical devices; messaging apps including email, texting, and file transfer; removable media such as CD/DVD, flash drives, and tapes
Failure to Manage Identified Risks

- The Risk Management Standard requires the “[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule].” See 45 C.F.R. § 164.308(a)(1)(ii)(B).

- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the breaching organization failed to act on its risk analysis and implement appropriate security measures.

- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.
Lack of Appropriate Auditing

• The HIPAA Rules require the “[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” See 45 C.F.R. § 164.312(b).

• Once audit mechanisms are put into place, procedures must be implemented to “regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.” See 45 C.F.R. § 164.308(a)(1)(ii)(D).

• Regular review of information system activity should promote awareness of any information system activity that could suggest a security incident or breach.
Insider Threat

• Organizations must “[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information ... and to prevent those workforce members who do not have access ... from obtaining access to electronic protected health information,” as part of its Workforce Security plan. See 45 C.F.R. § 164.308(a)(3).

• Appropriate workforce screening procedures could be included as part of an organization’s Workforce Clearance process (e.g., background and OIG LEIE checks). See 45 C.F.R. § 164.308(a)(3)(ii)(B).

• Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization’s workforce exit or separation process. See 45 C.F.R. § 164.308(a)(3)(ii)(C).
Corrective Actions May Include:

• Updating risk analysis and risk management plans
• Updating policies and procedures
• Training of workforce
• Implementing specific technical or other safeguards
• Mitigation
• CAPs may include monitoring
Some Good Practices:

• Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations

• Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned

• Dispose of PHI on media and paper that has been identified for disposal in a timely manner

• Incorporate lessons learned from incidents into the overall security management process

• Provide training specific to organization and job responsibilities and on a regular basis; reinforce workforce members’ critical role in protecting privacy and security
GUIDANCE RESOURCES
• http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

• http://scap.nist.gov/hipaa/

• http://www.healthit.gov/providers-professionals/security-risk-assessment
HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; purpose is to understand concerns of developers new to health care industry and HIPAA standards
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016
Health app developers, what are your questions about HIPAA?

HIPAA Health Information Privacy, Security and Breach Notification Rules

Engage with OCR on issues & concerns related to protecting health information privacy in mHealth design and development

http://hipaaQsportal.hhs.gov/
• June 2016 (What’s in Your Third-Party Application Software)
• September 2016 (Cyber Threat Information Sharing)
• October 2016 (Mining More than Gold (FTP))
• November 2016 (What Type of Authentication is Right for you?)
• December 2016 (Understanding and Preventing DoS/DDoS Attacks)
• January 2017 (Understanding the Importance of Audit Controls)
• February 2017 (Reporting and Monitoring Cyberthreats)

https://www.hhs.gov/hipaa/for-professionals/list-serve/
Thank You

Nicholas Heesters, JD, CIPP
Health Information Privacy & Security Specialist
U.S. Department of Health and Human Services, Office for Civil Rights

Website:
http://www.hhs.gov/hipaa
Twitter: @HHSOCR
Audit Controls – The Basics

• Governance Framework (HIPAA)
• Risk Analysis
• Controls & Monitoring
• Documentation of Investigations
• Risk of Compromise
• Attestation, Evidence & Reporting
• Notification & Disclosure
Prevalent Industry Challenges
Audit Controls and Access Rights Management

FairWarning Dynamic Identity Intelligence

Lawson + AD

Application Access Logs

- Discover
  - Known Users
  - Unmatched Users
  - Dormant Users
- Enables
  - Access after termination
  - Access Control Review
  - Dynamic Identity on Roles, Profiles, History
  - Data Integrity
- Foundational to FairWarning

Healthcare System Network:

- MEDITECH
- Cerner
- McKesson
- Office 365
- Others

Non-Employees w/ Access
- Vendors
- Contractors
- Affiliate Physicians

Employees

3rd Party Physicians and Diagnostics Clinics, etc...

Prevalent Industry Challenges
Audit Controls and Access Rights Management

FairWarning Dynamic Identity Intelligence

Lawson + AD

Application Access Logs

- Discover
  - Known Users
  - Unmatched Users
  - Dormant Users
- Enables
  - Access after termination
  - Access Control Review
  - Dynamic Identity on Roles, Profiles, History
  - Data Integrity
- Foundational to FairWarning

Healthcare System Network:

- MEDITECH
- Cerner
- McKesson
- Office 365
- Others

Non-Employees w/ Access
- Vendors
- Contractors
- Affiliate Physicians

Employees

3rd Party Physicians and Diagnostics Clinics, etc...
Emerging Challenges

- Identity Intelligence
- Cloud
- Big Data
- People Security
Questions?

For more information, please visit: [www.FairWarning.com](http://www.FairWarning.com)
Or email: [Solutions@FairWarning.com](mailto:Solutions@FairWarning.com)

Chad P. Brouillard  
Attorney at Foster & Eldridge, LLP

Nicholas Heesters, JD, CIPP  
Health Information Privacy & Security Specialist  
U.S. Department of Health and Human Services, Office for Civil Rights

Kurt J. Long  
Founder and CEO  
FairWarning

Twitter: [@chadbrouillard](https://twitter.com/chadbrouillard)  
LinkedIn: [linkedin.com/in/chadbrouillard](https://www.linkedin.com/in/chadbrouillard)

Website: [http://www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)  
Twitter: [@HHSOCR](https://twitter.com/HHSOCR)

Twitter: [@KurtJamesLong](https://twitter.com/KurtJamesLong)  
LinkedIn: [https://www.linkedin.com/in/kurt-long](https://www.linkedin.com/in/kurt-long)