Auditing and Access to Electronic Health Records

December 15, 2016 – 12p (Eastern)
## Introductions

<table>
<thead>
<tr>
<th>Name</th>
<th>Title and Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andy Reeder</td>
<td>CISSP, CISA, CISM, HCISPP, CHPC, HIPAA Security Officer; Director, HIPAA Privacy</td>
</tr>
<tr>
<td></td>
<td>Rush University Medical Center, ISSA Healthcare SIG Chair</td>
</tr>
<tr>
<td>Chuck Burbank</td>
<td>CHP, CHSS, Chief Information Security Officer, FairWarning</td>
</tr>
<tr>
<td>Karen McMillen</td>
<td>CISSP, Security Analyst 2, Asante Information, Technology Services</td>
</tr>
<tr>
<td>Roy Wattanasin</td>
<td>Former Healthcare Information Security Officer, MIT Medical</td>
</tr>
<tr>
<td></td>
<td>ISSA Healthcare SIG Member, ISSA CISO Forum Member</td>
</tr>
</tbody>
</table>
Background

Information access is both a privacy and security concern

Increasing use of electronic health records with multi-user access

Concerns over inappropriate access and impermissible disclosures of patient information; impact on trust

Risk issues such as identity misuse or identity theft

Reportable breaches are a focus area for the federal government

Holding workforce accountable for access/actions
<table>
<thead>
<tr>
<th>This is...</th>
<th>This is not...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A discussion about auditing access to electronic patient records</td>
<td>A review of user provisioning, identity management, or access controls strategies</td>
</tr>
<tr>
<td>A review of regulatory requirements for conducting audits</td>
<td>A review of identification or authentication methods, e.g., userid, biometrics, tokens, passwords</td>
</tr>
<tr>
<td>A discussion about technical considerations when implementing solutions</td>
<td></td>
</tr>
</tbody>
</table>
## Why Conduct Access Audits?

- Identify inappropriate access to records
- Establish accountability
- Compliance with internal policies
- Compliance with federal and state regulatory requirements
- Investigate complaints
- Breach incident response
- Enhance trust in privacy and security of records – culture of compliance
- Identify and manage risk
Assets

Patient Records
- Demographics (name, SSN, address, phone)
- Financial (insurance, financial accounts)
- Medical (general and sensitive medical information)

Organizational records
- Employee
- Financial
- Operations
- Marketing
Electronic Records

**HITECH Act of 2009**

- Promoted electronic access
- Electronic Health Records
- Patient Portals
- Health Information Exchanges
- Portable Devices and Apps
- Meaningful Use program
- About 80% of providers now use EHR

http://www.cdc.gov/nchs/products/databriefs/db143.htm
<table>
<thead>
<tr>
<th>Who is accessing the EHR?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Medical Staff</strong></td>
</tr>
<tr>
<td><strong>Nursing Staff</strong></td>
</tr>
<tr>
<td><strong>Advanced Practice Staff</strong></td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
</tr>
<tr>
<td><strong>Medical Records/Health Information Management</strong></td>
</tr>
<tr>
<td><strong>Finance/Billing</strong></td>
</tr>
<tr>
<td><strong>Patient Relations/Complaints</strong></td>
</tr>
<tr>
<td><strong>Support Staff</strong></td>
</tr>
<tr>
<td><strong>Students – Academic Medical Centers</strong></td>
</tr>
<tr>
<td><strong>Other</strong></td>
</tr>
</tbody>
</table>
The risk of inappropriate access has increased for multiple reasons

## Threats

<table>
<thead>
<tr>
<th>External Threats (data exfiltration)</th>
<th>Internal Threats (data snooping)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Advanced Persistent Threats</td>
<td>• Employees/Curiosity</td>
</tr>
<tr>
<td>• Criminal Groups</td>
<td>• Visitors</td>
</tr>
<tr>
<td>• Malware/Phishing</td>
<td>• Other 3rd parties</td>
</tr>
<tr>
<td>• Ransomware</td>
<td>• Malicious intent/data integrity</td>
</tr>
<tr>
<td></td>
<td>• Identity misuse/identify theft</td>
</tr>
</tbody>
</table>

“Cybersecurity threat” means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system - *Cybersecurity Information Sharing Act of 2015*
Poll - Threats

• Which do you think is the greatest threat type to healthcare information assets – internal or external?
Insider Threats and the Emerging Cyber Threat Landscape

• User Activity Monitoring
  • Explicit HIPAA Requirement for monitoring PHI access
  • Commonly 'Insider Threat Detection’
  • Detection of identity theft, medical identity theft, 'snooping', fraud
  • Compromised credentials, external attacks

• Escalation of Threats
  • Snooping
  • Identity Theft, Medical Identity Theft
  • Espionage and Politically Motivated Attacks
  • Post-Breached World
In January 2015, a healthcare provider notified 844 patients of inappropriate access to records after discovering a pharmacist employee had been inappropriately snooping on patients' medical data for an entire year. The incident was discovered after the hospital conducted an EHR audit back in October 2014... (Healthcare IT News: http://www.healthcareitnews.com/news/ehr-audit-catches-snooping-employee)

A hospital emergency room (ER) employee and his wife worked for a large not-for profit hospital business with 22 locations...He had access to patient information through the EHR...another employee at the hospital...recruited the hospital employee to participate in an illegal scheme involving EHRs...In July 2011, the hospital terminated the employee for having improperly accessed healthcare records...When the hospital terminated the employee, it did not examine the audit log’s record of his other EHR access events and remained unaware of his other misconduct...Log records later reviewed showed inappropriate access and improper disclosure of information related to thousands of records; the case was referred to the FBI...Detecting and Investigating (Unauthorized Access to Electronic Health Records—A Case Study: https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/ehr-casestudy-booklet.pdf)
Vulnerabilities

Technical

- Passwords
  - shared or compromised
- Logout/Screen Locking
  - patient records left open and accessible

Physical

- Placement of devices
- use of remote, virtual devices
- Shared devices
  - lack of individual accountability
Vulnerabilities

Administrative

- Acceptable Use Policies
  - is appropriate use clearly identified?
- Code of Conduct/Disciplinary actions
  - are consequences made clear?
- Awareness
  - are policy requirements published and trained?
Risk

- Data integrity/Patient safety
- Impermissible Disclosures/Privacy Breach
- Effect on trust/brand/reputation
- Regulatory enforcement/penalties
- State enforcement
- Private cause of action lawsuits
- Risk of inaction if auditing indicates problems
OCR Enforcement Underscores Importance of Managing Security Risk

Trends from this year’s ongoing OCR reviews & investigations
Source: Iliana Peters, Sr. Advisor for HIPAA Compliance & Enforcement at HHS OCR, 2016 NIST/OCR Conference

- Incomplete or Inaccurate Risk Analysis
- Failure to Managed Identified Risk (Risk Management Plan)
  - In September, the ONC released new features to the Security Risk Assessment Tool
- Lack of Transmission Security
  - Use of FTP and other unsecured methods of transmitting data
- Lack of Appropriate Auditing
- Lack of Patching or very delayed patching
- Insider Threat Management
  - Not everyone should have access to everything
  - Access Termination – Access should be terminated same day as employee leaves
§164.308(a)(1)(ii)(D) Security Management Process (Required) - Information System Activity Review

- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

§164.308(a)(3)(ii)(B) Workforce security - Workforce Clearance Procedure (Addressable)

- Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

164.312(1)(b) – Audit controls (Required)

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information
§164.514(d) (1)-§164.514(d) (2) Standard: Minimum Necessary & Minimum Necessary Uses of PHI

- A covered entity must identify:
  - (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and
  - (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

- A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d) (2) (i) (A) of this section to protected health information consistent with paragraph (d) (2) (i) (B) of this section.
Regulatory Background – Meaningful Use/Certified EHR

§170.210(b): 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, deleted, or printed; and an indication of which action(s) occurred must also be recorded.

§170.210(e): Record treatment, payment, and health care operations disclosures

• The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

§170.314(d)(2) - Auditable Events and Tamper-Resistance

• Recording user actions related to electronic health information in an audit log in addition to when the audit log or the encryption status of electronic health information locally stored on end user devices is disabled or enabled.

170.314(d)(3) Audit Report(s)

• Requires EHR technology to be capable of enabling a user to generate an audit report for a specific time period, and sort entries in the audit log according to the data elements specified in the audit log content standard.
A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.
OCR Audit Protocol

- Includes a control review: "Does the entity have policies and procedures in place regarding the regular review of information system activity? Does the entity regularly review records of information system activity?"

State Breach Laws

The Joint Commission

PCI

External/Financial Controls Audits
Audit Program Basics

**Policies**
- Establish policies that govern appropriate access (e.g., Code of Conduct)
- Identify what access is permitted by the workforce
- Identify what disciplinary actions exist for inappropriate access

**Inventory**
- Identify systems where PHI is located
- Identify which are most sensitive; business critical

**Coordination**
- Establish a close working relationship with Human Resources, Legal Affairs, Risk Management
- Involvement of managers at all levels in the review of audit data
- Don’t jump to conclusions – investigate fully
- Check for duplicate user names
- Check for job role v. access type
Audit Program Basics

For Cause

- Conducted due to a specific event or reason
- Patient complaints/requests for audit
- Accounting of Disclosures
- Manager concerns
- Staff concerns
- Related to other incident

Not for Cause

- Conducted on a recurring schedule to look for trends
- Establish audit targets
  - Patient
  - User
  - High Profile
  - Same Last Name
  - Other
Audit Program Basics

Investigation/Remediation

- Follow-up on findings of potential inappropriate access
- Employee interviews/checklists
- When to transition from auditing to Breach investigation?
- Disciplinary action/retraining

Establish Indicators

- Parts of record accessed
- Length of activity
- Printing/Disclosure activity
- Location of access
- Reason for access
- Employee assignment to patient
Audit Program Basics

Record Retention

- Where is audit data stored and for how long?
- Where are processed reports kept and for how long?
- eDiscovery considerations

Data Sources

- EHR – differ depending on platform
- Ancillary Systems
- Data flow diagrams
Establish Auditing Program organization placement

- Determine if this is a Privacy, Security, Compliance, or IT function
- Identify processes for collecting audit requests and prioritization
- What types will be conducted and how often?

Determine number of staff needed

- Determined by auditing type (manual, automated, outsourced)
- Competition for resources – automation can help fill the gap

Determine skillsets of audit staff

- Data analysis (Excel, Access)
- Governance/regulatory (HIPAA, State Laws, HR policies)
Solution Types

Data export to manual review (spreadsheets)
- Data is collected in EHR
- Exported for manual review/analysis

Automated auditing
- Data is exported to an application that automates the collection, review, and analysis
- Analysis is accomplished with multiple data sources

Outsourced auditing
- Data is exported to a hosted application and/or site
- Analysis/reporting is managed by a 3rd party vendor
Patient Privacy Intelligence (Automated Auditing)

What you need to get from your automated auditing solution:

- Auto-generated alerting
- Ability to bring in multiple data sources
- Ability to tie authoritative user data together
- Investigation documentation
- Coordination with other layers of your defense framework, i.e. SIEMS
- Seek a solution that maps to the HIPAA audit protocols

View the FairWarning Phase 2 HIPAA Audit Protocol Mapping:
Use Case: High Patient Access Count

• Alert: An access of higher than normal numbers of patient records
  • May indicate snooping
  • May indicate theft of PHI or financial information
  • May indicate compromised user credentials
  • May result in criminal activities, a lawsuit and/or damage to organization’s reputation

• Challenge: Determine whether the unusually high access is for a legitimate business reason or if it indicates a potential threat
Managed Privacy Services
(Outsourced Auditing)

An outsourced auditing solution should provide:

• A massive reduction in your compliance workload
• Function as an extension of your team
• Improvements to your compliance posture
• More time to focus on higher value projects
• Worry-free staffing with certified experts in HIPAA Privacy & Security
Current/Future Challenges

- Health Information Exchanges
- Cloud Services
- Mobile Access
- Remote Access
Discussion/Contact Information

- Andy Reeder – andrew_reeder@rush.edu

- Chuck Burbank -
  www.FairWarning.com;
  Solutions@FairWarning.com
Auditing and Access to Electronic Health Records