Establishing an Access Auditing Program

Cindy Matson, CHC, CHPC
Chief Privacy Officer

About Sanford…

- Hospitals: 31
- Clinics: 111
- Long-term care facilities: 31
- Employees: 18,000+
- Physicians: 900+, offering expertise in more than 70 specialties

With headquarters in Fargo, ND and Sioux Falls, SD, we are an integrated healthcare system built from the merger in 2009, of two long-standing organizations. Today, we are the largest, rural, not-for-profit healthcare system in the nation with a presence in 111 communities in eight states. In addition, we are building international clinics (Ghana, Mexico, Ireland ?)

As the largest employer in North and South Dakota, we are seeing dynamic growth and development in conjunction with Denny Sanford's $400 million gift in 2007 – the largest gift ever to a healthcare organization in America. This gift has brought to life the implementation of several initiatives, including global children's clinics, multiple research centers and finding a cure for type 1 diabetes.

About Me…

- Began my career at Sanford in 1987 as an intern (then a 400 bed hospital)
- Worked at staff and supervisory levels in the laboratory for 9 years and as a Regulatory Coordinator for 2 years
- Transferred to Corporate Compliance Office in 1999 and subsequently promoted to Director (2005) and Chief Privacy Officer (2002).
- Transitioned to Chief Privacy Officer for all of Sanford in 2010
- CHC & CHPC

Why Audit?

- Obviously to detect inappropriate access to PHI
- To hold individuals accountable for their activity
- Reduce risk for the organization
- Investigate complaints
- Culture of compliance – it's the right thing to do
- Regulatory and accreditation requirements

HIPAA Security Rule

- §164.308(a)(1)(ii)(c): Information system activity review (required), "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports"
- §164.312(1)(b): Audit controls (required) "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"

HIPAA Privacy Rule

- §164.304: Definitions. "Administrative safeguards are…to manage the conduct of the covered entity's workforce in relation to protection of that information."
- §164.530(i)(1): Administrative Requirements, Policies and Procedures, "The policies and procedures must be reasonably designed, taking into account the size of and the type of activities related to protected health information undertaken by the covered entity, to ensure such compliance."

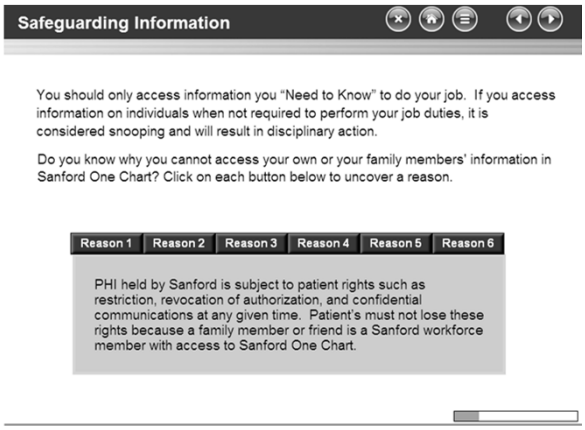
Other Requirements

- HITECH requires monitoring for breaches of PHI
- Meaningful Use requires audit log generation and compliance with HIPAA Security Rule
- Accreditation standards such as Joint Commission
- Payment Card Industry Data Security Standard (PCI) includes audit requirements
- Legal requirements (e-Discovery)

Related Privacy Program Elements

- Education
  - Need to Know
  - Minimum Necessary
  - Protection of Username and Password
  - Consequences of Violations
- Employee Attestation or Understanding
- This is the foundation that will provide for consistent disciplinary action

Education: Need to Know



Employee Acknowledgment Form

Confidentiality, Privacy and Access to Information

I understand that confidential information includes any patient information, personnel information and XYZ competitive and financial information. Under no circumstance will I discuss this information with individuals outside of my job role. I have read and understand XYZ's Confidentiality Policy. Initial here: _____

I understand that my username and password to access electronic information is only for my use and may not be shared with anyone. I agree to only access information necessary to perform my job duties and that I will be held accountable for any inappropriate access. Any access determined to be inappropriate shall result in disciplinary action, up to and including the termination of employment and criminal prosecution. I have read and understand XYS's policy on Sanctions for Privacy and Security Violations.

Initial here: _____

I understand that for access to electronic information, including but not limited to, electronic medical records, I will be assigned a unique identification code. This code, which will consist of an assigned username along with a password of my choosing, will serve as my electronic signature. My electronic signature is legally the same as my written signature and should not be shared with others. I have read and understand XYZ's Electronic Signature policy. Initial here: _____

Corporate Compliance

I agree to follow XYZ's Code of Conduct and all applicable local, state and federal laws, rules and regulations. I also understand that I have the duty to report any suspected violations of law or Compliance policies to my immediate supervisor or the Compliance Hotline at (***)***-****. I have read and understand XYZ's Corporate Compliance Policy, Compliance Human Resources Policy and the Code of Conduct. Initial here: _____

_____ _____

Printed Name Signature Date

Definitions

- Audit log – record of sequential activities maintained by the application or system
  - Note: Be sure you retain logs 6 years
- Audit trail – the log records that identify a particular transaction or event (view/access)
- Audit – review of the records to determine appropriateness of access and a required part of security and risk management process

What to Audit?

- Audit data may include information on:
  - User
  - Patient
  - Time
  - Location (workstation or device)
  - Duration of access
  - Information accessed
  - Location of encounter
  - **Dependent on sophistication of system or application audit logs*

For Cause

- Complaints by patients
- Reports by staff
- Concerns of manager
- Follow-up of previous violation or concern
- Helpful to have detail related to suspected activity or patient/employee connection

Targeted

- Established activity that triggers a review:
  - Same last name/address
  - VIP
  - Media reported events
  - Co-worker/Employee illness or life event
  - Deceased patients after established time frames
  - Patients with no or limited activity after established time frames
  - Sensitive records

Techniques for Targeted

- Privacy breach detection solution
  - Ability to screen all or high number of what might be labeled as high risk access for review
  - Still needs manual review of reports
- Custom reports (matching or time frames)
- Monitoring access daily for VIP or Media reported
  - Manual review of access data
  - Some system tools (if available) may be used to block access or require user to provide rational

Random

- Can be user-centric or patient-centric
- Least productive (IMO)
- Resource intense if you are doing manual review
- Biggest deterrent to staff?
- Will this be the priority to audit or vary in relation to the total number of audits?

Defining a Plan

- What resources do you have? Manual review of audit logs are time consuming.
  - Who will do the review (Privacy, Security, Management or combo?
  - What is a realistic number to review? How often?
- Consider concurrent review of security rights (access to systems or applications)
- Regular review is required but NOT defined in terms of numbers or frequency but “taking into account size and type of activity”

Assess Systems

- Sanford 40+ systems/applications with PHI
- That does not include databases, etc.
- Determine priorities for auditing plan
- Not to be confused with Security Risk Assessment
- Document process behind plan to demonstration that it is reasonable/scalable

Rate Systems According to:

- Amount of PHI
  - 1 – limited
  - 2 – subset
  - 3 – full EMR
- Sensitivity of PHI
  - 1 – subsets of information
  - 2 – no "sensitive" information
  - 3 – sensitive information (SSN, dx)
- Number of users
  - 1 (1 – 100)
  - 2 (101 – 499)
  - 3 (>500)
- Frequency of use
  - 1 – low or infrequent
  - 2 – occasional to moderate
  - 3 – constant

Tale of 3 Systems

System	Amount of PHI	Sensitivity of PHI	# of Users	Frequency of Use	Average Score	Comments
Horizon Decision Support	3	3	1	2	2.25	Business Intelligence/Cost Accounting
Pharmacy Robot	2	2	1	3	2.00	Medication Filling
EPIC	3	3	3	3	3.00	Full EMR

Higher average scores will determine priority to review audit logs.

Connect the Dots

- May be useful to coordinate audit logs from more than one system (if you have an automated detection system this may be easier)
- Review activity during suspect timeframes for “surfing”
- Information from others who know user better can assist in putting together a picture
- Can sometimes tie emails and phone calls to time of inappropriate access

Evaluation of Findings

- Role of the Privacy Officer is to assist in understanding audit data
- Department managers and supervisors must be responsible for final determination
- Use Information Technology resources to further explore concerns – we have been able to “recreate” what access actually looked like by following the same user actions recorded in the audit log.

Proceed with Caution

- Respect your employees and understand there may be other motives for complaints
- Do NOT jump to conclusions
  - Check work schedules
  - Be aware of special projects
  - Compare access or workflow to similar employees
  - Look for searching process and access versus normal workflow

One thing leads to another…

- Evaluate findings for data breach
  - Was the information inappropriately accessed further used or disclosed
  - Was the information "sensitive" in nature?
  - What is the risk of either financial or reputational harm to the patient?
  - Follow you data breach assessment policy
- Consider if pattern of access could indicate any sort of identity theft

Sanctions for Violations

- Have a policy and consistently FOLLOW it
  - Being inconsistent poses a risk to your organization
- Human Resources should ALWAYS be involved
  - Consistent with overall disciplinary policies
  - Assure proper follow through and documentation
  - Consideration for other performance issues

Policy Considerations

- Consider levels of violations so the "punishment fits the crime"
  - Educational issues
  - Barriers to compliance
  - Lack of proper safeguards
- Assign duties so documentation is solid
  - HR documents employee interviews and any disciplinary actions
  - Privacy Officer documents audit findings, conclusion of investigation, corrective action and/or mitigation
  - Proper follow-up with patient if this was complaint based

Goals:

- Compliance!
- Protection of patients
- Protection of your organization