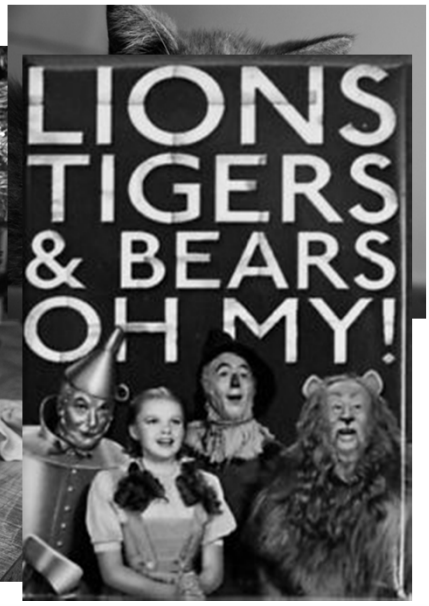
You Know What They Say.. Curiosity Killed the Cat!

Best Practices and Tips on How to Implement a Pro-Active Breach Monitoring Plan

Shallie J. Bryant

Disclaimer: I love ALL Animals!

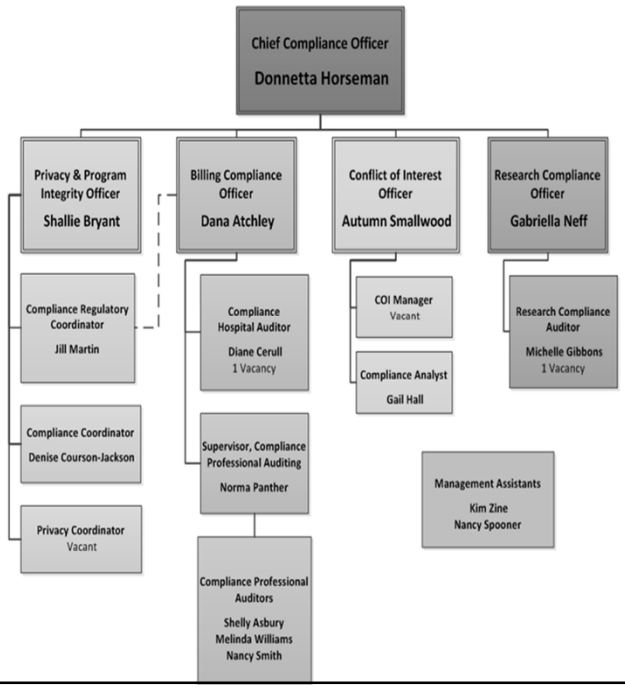


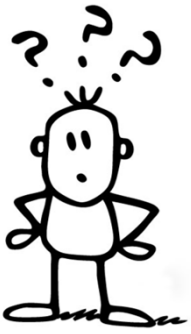
Background

H. Lee Moffitt Cancer Center & Research Institute

Established by the Florida Legislature in 1981 to address the burden of cancer in Florida.

- Hospital – 206 Licensed Bed, 32-Bed BMT Unit, CRU
- Moffitt at International Plaza – Outpatient Center
- McKinley Campus – Outpatient Surgery Center
- 5400 employees





Defining Our WHY?

What's Required?

Section 164.308(a)(1)(ii)(c) – states covered entities must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Audit Procedures

Inquire of management as to whether formal or informal policy and procedures exist to review information system activities; such as audit logs, access reports, and security incident tracking reports. Obtain and review formal or informal policy and procedures and evaluate the content in relation to specified performance criteria to determine if an appropriate review process is in place of information system activities. Obtain evidence for a sample of instances showing implementation of covered entity review practices Determine if the covered entity policy and procedures have been approved and updated on a periodic basis.

More Reasons to Pro-Actively Audit and Monitor

- Beacon Health announced an employee had been discovered to have improperly accessed the medical records of 1,200 patients without any legitimate work reason for doing so. That employee had been snooping on medical records for three years.
- Chadron Community Hospital and Health Services in Nevada discovered an employee had accessed the medical records of 700 patients over a period of five years and St. Charles Health System in central Oregon discovered an employee had accessed medical records without authorization over a 27 month period.
- Trios Health discovered an employee had improperly accessed the medical records of 570 patients. The improper access occurred over a period of 41 months.
- Covenant HealthCare notified 6,197 patients of a privacy breach after an employee was discovered to have improperly accessed medical records over a period of 9 months,

Data says

- IBM's 2016 Cyber Security Intelligence Index found that 60 percent of all breaches are carried out by insiders (Current and former employees)
  - Inadvertent human error
  - Some employees intentionally or unintentionally–take classified or proprietary information with them when they depart.
- More attention has shifted toward Cyber Attacks

Insider Threats

- Emotions
- Employee snooping can go undetected for years
- Difficult to prove guilt
- Hard to distinguish harmful action from regular work
- Staff know you are not watching

Where We Started

- **Past:** Not enough staff to effectively manage a breach detection program. Engaged vendor to conduct audits
  - Pros: We did not have to audit or monitor user activity?? Or did we?
  - Cons: Not apart of the Moffitt's day-to-day culture
    - Thorough analysis
- **Present/Future Goals:** To continue proactively monitoring system activity **with the expectation that all inappropriate usage of our clinical systems will stop.**

More and More Compliance Initiatives??

- Implementing an active breach detection program or process:
  - Helps you to identify users who are engaging in questionable access patterns
  - Allows you to monitor multiple systems in one place

Policies

- Acceptable Use of Information
- Code of Ethics & Professional Conduct
- Breach Notification: Reporting Incidents Involving the Privacy or Security of Protected Health Information
- Confidentiality of Patient Information
- Sanctions for Privacy Violations

Education

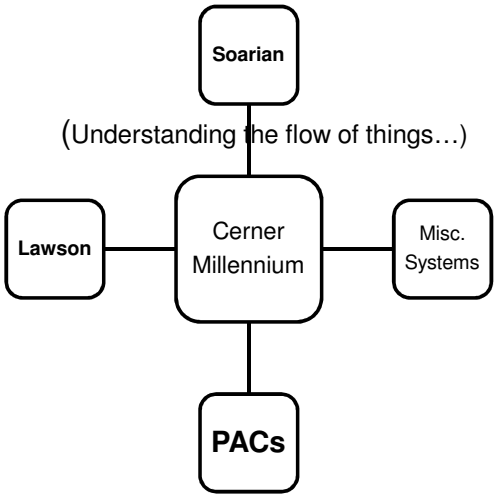
- New Employee Orientation
- In person training
- Web-based training
- Make sure staff know your policy on snooping and looking at their own record

Prevention Through Education

- ONGOING: Education and Awareness
  - New Employee Orientation
  - Monthly Newsletters
  - Compliance Week
  - Annual Mandatories
- Consistent Disciplinary Actions

Before You Flip the Audit Switch

- Identify applications
  - Create a diagram of how PHI flows within the organization
- Define who will manage, conduct audits
- Determine what alerts to activate
- Run tests
- Review alerts and reports



What's the process?

- Understand department workflow
  - **Employee responsibility**
  - Is system access work related
- Understand what types of activity to monitor
  - Self examination
  - Family member or friend snooping
  - High profile patients
  - Employees
  - Audit Alert request

Planning

- Develop a team
  - Privacy/Compliance
  - HIM
  - Human Resources
  - Legal
  - Information Security
  - Information Technology
    - Application and system owners

Planning Example

- **The system generates an alert.**
- **The alert will be reviewed by the Compliance Department.**
- **Additional follow-up may be necessary to determine if access was inappropriate**
- **If access appears to be inappropriate (i.e., no apparent business or clinical reason), then further investigation may include the following:**
  - **Email/memo:** sent to employees manager/ supervisor requesting validation of the purpose of the access to a particular patient account/information
  - **Interview:** The Compliance Department in conjunction with employees manager, may conduct an interview with the employee to obtain additional information
  - **Sanction:** If warranted, disciplinary guidelines will be followed based on the level of violation.

Detection

- Understanding your organizations environment and culture
  - One size doesn't fit all
  - Job description
    - Routine responsibilities
  - Analyze records of human activity to detect suspicious behavior

Incident Investigation

- Incident Investigation and Response Plan
  - Who will do what?
  - Be prepared to investigate alerts
- What kind of information needs to be gathered?
- Was their a breach?
- Does it require notification?

Questionable Findings

1) Carefully review audit report
   - Collaborate with system coordinator/IT/IS
   - Contact department director/manager
     - Employee Role/Responsibility
     - Department/Unit process
2) Involve HR Department
3) HIM Director
4) Interview employee

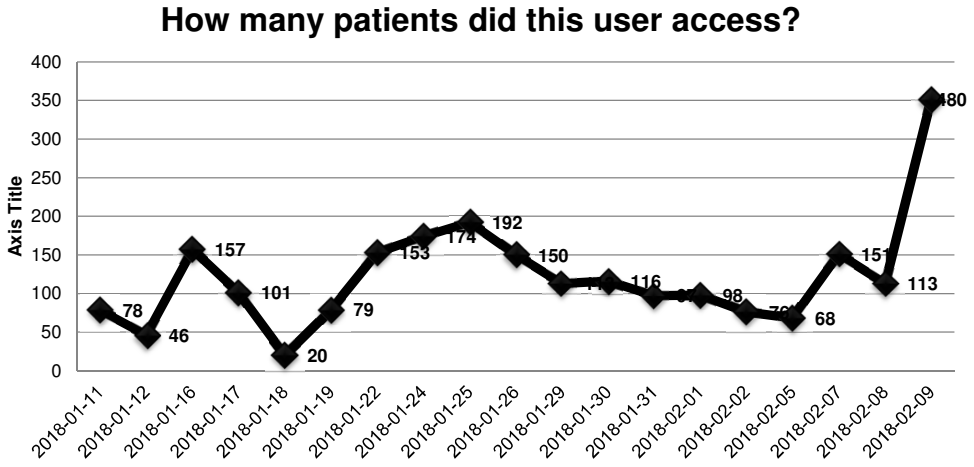
Self Examination

Date	User ID	User Last Name	User First Name	User DOB	Object Type	Patient Last Name	Patient First Name	Patient DOB	User Title	User Description
6/1/2013	sjbryan	Bryant	Shallie	6/27/1973	RD112	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/1/2013	sjbryan	Bryant	Shallie	6/27/1973	Print Doc	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/1/2013	sjbryan	Bryant	Shallie	6/27/1973	RD112	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/5/2013	sjbryan	Bryant	Shallie	6/27/1973	OB117	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/7/2013	sjbryan	Bryant	Shallie	6/27/1973	OB117	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/8/2013	sjbryan	Bryant	Shallie	6/27/1973	LB114	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/8/2013	sjbryan	Bryant	Shallie	6/27/1973	LB114	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/8/2013	sjbryan	Bryant	Shallie	6/27/1973	Print Doc	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds
6/8/2013	sjbryan	Bryant	Shallie	6/27/1973	Print Doc	Bryant	Shallie J.	6/27/1973	RN-Peds	Peds

Challenges

- Ex-wife (employee) snooping into husband medical record
- Unauthorized curiosity access of family medical records
- Employee snooping on behalf of co-worker
- Employee snooping on behalf of family member or friend
- **Boredom**
- Co-worker snooped into brother in-law's medical record and discussed with family members
- Several employees accessed their own medical record to modify appointments
- Employee accessed deceased relative's medical record

Unusually High Access: Patient Population – Age >75



Neighbor Snooping

TimeStamp	Patient First Name	Patient Last Name	Patient DOB	User Address	User City	User State	Event Type	Event Description	Workstation ID	User ID	User First Name	User Last Name	User Address Line 1	User City	User State	User Hire Date	User Title
10/4/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	View Result	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/4/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	View Clinical Note	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/5/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	Radiology - CT Scan	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/5/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	Lab Results	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/5/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	View Result	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/6/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	View Clinical Note	Read	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU
10/6/2012	Denzel	Washington	8/27/1954	125 Snoop Lane	Breach	NC	View Demographics	Print	TQ446	sjbry4	Shallie	Bryant	123 Snoop Lane	Breach	NC	2007-10-01	RN- PICU

Breach Notification

- Develop template notification letters
- Plan in advance
- Credit monitoring
- HHS notification
- Media Notification
- Consider Insurance

TRAIN THE TRAINER GUIDE

rces

General Procedure

1. The NAME OF HOSPITAL/FACILITY will generate a minimum of (6) focused audit reports monthly. An increased audit posture will result in greater protection to the organization and its information, but in no month will less than 6 focused audit reports be reviewed and tracked.
2. At any given time, special audits will be performed on demand to investigate all privacy complaints/concerns.
3. The NAME OF HOSPITAL/FACILITY will run monthly proactive audits in FairWarning. Those monthly audits will include, at a minimum:
   a. Self Exam Activity Report - Finds users that are accessing their own medical records.
   b. Neighbor Snooping Activity Report – Finds users that access medical records of their neighbors.
4. The NAME OF HOSPITAL/FACILITY will conduct ad hoc monitoring at its discretion to attempt to detect inappropriate access. Ad hoc monitoring may be used to meet minimum audit requirements or be conduction in addition.
5. The NAME OF HOSPITAL/FACILITY will investigate suspicious activity.
6. The NAME OF HOSPITAL/FACILITY will initiate scheduled audit alerts at its discretion. These may include:
   Monthly - Executive Team Activity Report – Finds users that access medical records of members of the executive team.
   On Demand - VIP/High Profile Patient – (ex. Employees, patients named in the media, celebrity patients, etc).
   On Demand - VIP /High profile patient – On Demand requests such as employees or patient who request access alerts of their medical record.
7. The NAME OF HOSPITAL/FACILITY will retain documentation that may be used to show this protocol is being followed.
   Currently this information is being tracked in an Excel Spreadsheet on the NAME OF HOSPITAL/FACILITY G: Drive.
8. The NAME OF HOSPITAL/FACILITY will retain audits and other documentation pertaining to suspicious activity or investigations. Currently, these are being tracked in an Excel Spreadsheet on the NAME OF HOSPITAL/FACILITY G: Drive. In the case that an investigation is initiated as a result, documentation is also stored in IntegriLink.
9. NAME OF HOSPITAL/FACILITY will review findings, investigate infractions and/or questionable behaviors. This may include:
   a. Reviewing each entry/access in/to the medical record and determine if the user was involved in the care of the patient. This will usually necessitate forwarding the audit to a knowledgeable member of management to review.
   b. If a discrepancy exists related to inappropriate access to the patient chart NAME OF HOSPITAL/FACILITY will
      - investigate alleged violation
      - notify appropriate manager
      - record and file evidence and action taken
      - execute appropriate disciplinary actions/training

Next Steps

- **Detect inappropriate access quickly**
- **Avoid false positives**
- **Identify relationships between people**
- **Continue to add audit sources**
- **Continue Education**
- **Review and update policies on a regular basis**
- **Track and trend**

References

- Office for Civil Rights (OCR) | HHS.gov *https://www.hhs.gov/ocr/index.html*
- https://www.hipaajournal.com/
- http://privacy.med.miami.edu/
- www.healthit.gov
- https://public.dhe.ibm.com/common/ssi/ecm/77/en/77014377usen/security-ibm-security-solutions-wg-research-report-77014377usen-20180404.pdf

Silly Responses

- I was in the bathroom during that part of the training
- I just wanted to make sure my ex-husband new wife was ok
- I just looked at the schedule I didn't see any PHI
- Your audit it wrong
- Last one…
  - Ativan – Xanax – Margarita?

Thank You!

Shallie J. Bryant
Privacy and Program Integrity Officer
shallie.bryant@moffitt.org
813-745-2265
H. Lee Moffitt Cancer Center &
Research Institute