Addressing Insider Threats

Presented by:
Rob Rhodes
Sr. Director, Patient Privacy Solutions
Iatric Systems, Inc.

Welcome!

Today's Faculty

Welcome

Rob Rhodes
Sr. Director, Patient Privacy Solutions
Iatric Systems, Inc.

History of insider threats and why they are so damaging
Why the new HIPAA regulations make it important to act now
A best practice approach for battling the insider threat

Agenda
"The more things change, the more they stay the same."

Betrayed by an Insider

"Insanity: doing the same thing over and over again and expecting different results."
Insider Threats are on the Rise

2013 Internet Threat Research Center Breach Report:

- Insider Theft soared 80% over 2012, with 72 insider incidents, compared to 40 recorded in 2012.
- Number of breaches attributed to Employee Error/Negligence in 2013 (57), a jump of 72.7% over 2012 figures (33).
- Breaches falling into the category of Subcontractor/Third Party reflected a 67.9% increase over 2012, with 89 and 53 breaches respectively.

Qualitative Risk

Risk = Likelihood X Impact

- Likelihood = Low
- Impact = High
- Risk = Low (maybe not!)

Motivation

Why did Ephialtes betray the Spartans?

**Reward!**

The same reason many insiders today betray their employer’s trust

**Not the only motivation...**

Manning & Snowden were motivated by Activism/Ideology
Most Common Threat Motivators

- Workforce Members Shopping: 80%
- Financial Identity Theft: 57%
- Medical Identity Theft: 51%
- Outsourced Personnel Shopping: 23%
- Cyber-Terrorism: 10%
- Black Market Activities: 11%
- Intellectual Property Theft: 8%
- Business Espionage: 6%
- Other: 2%
- Don't Know: 5%

Source: 2013 HIMSS Privacy and Security Survey

It’s So Easy!

- Insiders have authorized access
- Are supposed to be there
- Many organizations are still auditing manually
- Healthcare Culture
  - Healthcare is behind other industries
  - Culture of sharing/more access vs. less
- Physician Attitudes
  - Executives/Boards not willing to fight battle with docs
  - We like to trust people

Need to Address More than Ever

- Federal Regulation Demands It
- Patients Demand It
- If you choose to ignore, you could be out of business!
More Stringent Regulatory Requirements

Enforcement takes on a more serious tenor with Omnibus Rule changes...

- Business Associates liability
- Harm Threshold removed in favor of “Probability of Compromise”
- Informal resolution no longer required
- Higher penalties

It’s a Matter of Trust

Customers Take Their Business Elsewhere

- Two-thirds of US adults would not return to a business if their personal information were stolen
- 35% would not return to their hospital
- 42% would go to a different drug/pharmacy

Source: Recent Study Conducted by Harris Interactive for Cintas Corporation

The Impact

- Could your organization survive losing 2/3 of the patients?
- Do you think the remaining 1/3 would have the same level of trust?
  - Patients would be less likely to tell their caregiver info they might need to properly care for them
  - Leads to quality issues
    - Higher 30-day readmissions
    - Lower VBP Quality Scores
  - Lower HCAHPS Scores
  - Fewer new patients
  - Lower VBP scores and lower reimbursement
- Serious Financial Impact
How Do We Address This?

**Policies**
Policy is what you stand on

**Procedures**
Procedures and sanctions enforce your policies

**Technology**
Leverage technology to make compliance easier

**Culture**
What your people think is important and how they act

---

**Reduces Impact** | **Reduces Likelihood** | **Reduces Impact and Likelihood**
--- | --- | ---
Least Privilege | Pre-employment Background Checks for all employees | Develop policies that match up with the necessary requirements of HIPAA, HITECH, Omnibus, etc.
Role Based Access Control | Occasional Background Checks for Current Employees | Create policies that help you comply with best practices in Information Security & Patient Privacy
Don’t forget to document your auditing policies | Segregation of duties

---

**Procedures**
- Procedures should be the physical implementation of policy
- Develop auditing procedures based on risk
- Have procedures to document, investigate, and follow-up on incidents
- Improve security by iterative measures focusing on your identified risks
Technology

- Auditing appropriately cannot be done effectively without automating patient privacy monitoring
- We use technology in all other aspects of our business, why not in auditing?
- Aggregate Audit Logs from all systems that contain PHI
- Let the technology identify patterns that may indicate inappropriate use
- Document your audits and any incidents you encounter
- Educate workforce prior to implementing

Security Audit Manager

- Consolidates audit logs from disparate systems
- Proactively monitors and identifies common privacy violations for all patients
- Reduces staffing resources needed for privacy monitoring
- Documents, tracks, and reports on incidents
- Provides executive reporting to show key aspects of your program

Security Audit Manager

- Same Last Name
- Same Household
- Same Street
- Guarantor/Subscriber
- Patients who are Employees
- VIP/Confidential Patients
- Patient/User Location Mismatches
- Discharged or Expired Patients
- Behavioral reporting: Identify users who have been accessing an unusual number of patient accounts
• Report on changes to key indicators that might indicate Medical ID Theft like:
  - Address Changes
  - Date of Birth
  - Race
• Correlate suspected cases with User Activity or Exception Reporting

Security Audit Manager
Medical ID Theft Reporting

- Different algorithms have higher levels of certainty:
  - Same Household Match
  - VIP/Confidential Match
  - Guarantor/Subscriber Match
- Some algorithms have lower levels of certainty
  - Same Street Match
  - Hospital Employee Match
- Use combinations of reports to support your investigation

Security Audit Manager
There's No One Magic Bullet

Culture

- "Culture Eats Strategy for Lunch"
- Develop policies with a multi-disciplinary committee
- Communicate content of policies to your workforce
- Educate workforce on Why!
- Use non-punitive auditing to educate users
Auditing Success

- Most famous insider betrayal in U.S. history
- Commander of West Point
- Disgruntled about being passed over for promotion by Congress – Others took credit for some of his successes
- Offered to surrender West Point to the British
- Papers revealing the plot were intercepted by Militia

Questions & Discussion

Final Thought

“Those who cannot remember the past are condemned to repeat it”

— George Santayana, Spanish philosopher