To Heal. To Teach. To Discover.

Houston, We've Had a Problem: Addressing Data Breaches with an Incident Response Team

HCCA 16th Annual Compliance Institute
Las Vegas, NV
April 30, 2012

Jennifer Edlind, JD, CHC
Paula Moran, M.Ed., PMP

Introduction

• Jennifer Edlind
  – Director of Privacy and Compliance Operations
  – University Hospitals Health System (UH), Cleveland, OH

• Paula Moran
  – Privacy and Security Manager
  – Massachusetts General Hospital (MGH), Boston, MA

• Our experience with incident response teams
Agenda

- Current state
- Incident Response Team (IRT) Model
- Case Study
- Scenario(s)
- Lessons Learned
- Questions

Houston, We’ve Had a Problem

“[T]he great test lies not in the crisis itself but in the ways we respond.”

Steve Forbes, The Communicators: Leadership in the Age of Crisis
Current State: The Age of the Data Breach

- Number of privacy violations increasing
- KPMG conducting up to 150 audits for OCR by December 2012
- Consumer awareness and concern
- Increased visibility and importance of the Privacy Office

The Incident Response Team Model

- Internal review & remediation
- Incident reported or detected
- Risk assessment & notification
- Involve external experts?
- Internal investigation
- Incident response team
- Privacy & Information Security programs
The Incident Response Team Model: Privacy/Information Security Program

- Getting beyond the Privacy and Security Officer titles
- Cross-department collaboration and integration
- Training
- Policies
- Education
- Process Documentation

Who reports? Where? When?

Assembling the team
- Legal and Risk Management
- Public Relations
- Human Resources
- Information Security
- Compliance/Privacy Officers
- Police and Security
- Physicians and/or Chiefs
- Research and the IRB

Timeframe
The Incident Response Team Model: Internal Investigation, Part 1

- Compiling the team: roles and responsibilities
- Status reports
- Documentation
- Legal issues
  - Role of counsel
  - Deciding whether investigation will be privileged
  - Navigating federal and state law
  - Multi-state breaches require expertise and possible outside counsel
  - May be faced with unique or conflicting requirements

The Incident Response Team Model: Specially Protected & Privileged Information

Please answer YES or NO to each of the following questions, to indicate if we may release the information below (if it is in your medical record):

- Yes [ ] No [ ] HIV test results (PATIENT AUTHORIZATION REQUIRED FOR EACH RELEASE REQUEST.)
- Yes [ ] No [ ] Genetic Screening test results (SPECIFY TYPE OF TEST)
- Yes [ ] No [ ] Alcohol and Drug Abuse Records Protected by Federal Confidentiality Rules 42 CFR Part 2 (FEDERAL RULES PROHIBIT ANY FURTHER DISCLOSURE OF THIS INFORMATION UNLESS FURTHER DISCLOSURE IS EXPRESSLY PERMITTED OR WRITTEN CONSENT OF THE PERSON TO WHOM IT PERTAINS OR AS OTHERWISE PERMITTED BY 42 CFR PART 2.) This consent may be revoked upon oral or written request.
- Yes [ ] No [ ] Others: Please List
- Yes [ ] No [ ] Details of Mental Health Diagnosis and/or Treatment provided by a Psychiatrist, Psychologist, Mental Health Clinical Nurse Specialist, or Licensed Mental Health Clinician (LMHC) (I understand that my permission may not be required to release my mental health records for payment purposes)
- Yes [ ] No [ ] Confidential Communications with a Licensed Social Worker
- Yes [ ] No [ ] Details of Domestic Violence Victims’ Counseling
- Yes [ ] No [ ] Details of Sexual Assault Counseling
The Incident Response Team Model: Internal Investigation, Part 2

- Internal Communications Issues
  - Issue regular communications to appropriate leadership (identified in advance)
  - Communicate to leaders in affected departments/entities
  - Limit the number of content editors
  - Protect privacy of employees involved

The Incident Response Team Model: Involving External Experts?

- Computer forensics
- Legal counsel
- Insurance carrier
- Notification vendors
- Call center vendors
- Law enforcement
The Incident Response Team Model: Risk Assessment and Notification

- Risk assessment: required by HITECH
- Notification issues
  - Make personal contact with patients (in addition to letters) whenever possible
  - Establish central call center
    - Provide staff with key talking points
    - Define customer service expectations
  - Have Public Relations manage and review all external messaging
  - Engage national/community organizations

The Incident Response Team Model: Internal Review and Remediation

- Returning to the “new” normal
- Conducting a root cause analysis
- Tracking data to present at IRT meetings
  - Recommend regular meetings when not in “crisis” mode
  - Use data to spot trends for areas where further controls or training would be helpful
- Ensuring mitigation steps are followed through to completion
Case Study: MGH Corrective Action Plan

- Incident response to patient information left on public transportation
- PHI included clinical information: some HIV/AIDS
- Timeline of case investigation
- Involved local community groups
- Letters to patients sent according to HITECH

Case Study: CAP Requirements

- Attest that all workforce received policies
- Require workforce not to remove PHI until trained
- Train all workforce on three policies
- Meet monitor requirements
- Audit workforce compliance
- Report policy violations
Case Study: Challenges and Opportunities

- National story
- Resolution agreement for $1 million
- Large, complex, decentralized workforce
- Interdepartmental workgroups; silos broken
- Not a privacy issue but an MGH issue
- Online education platform
- Heightened awareness and support

Scenario #1

Physician is traveling between offices and brings home the 15 face sheets for the patients she will see the next day. She also carries her laptop, on which she has saved all of her human subject research files. That evening, a thief smashes her car window, stealing both the laptop and the briefcase containing the patient face sheets.
Scenario #1: Discussion Questions

- Where is this issue likely to be reported in your organization?
- What do your policies require for paper PHI to leave your organization?
- Who is going to manage the team?
- What are the key facts for the team to uncover?
- What external parties may become involved?

Scenario #2

A clinician is asked by a relative to look at a patient’s medical record. The clinician agrees to the request and provides details from the records. The records include detailed social work notes. The social worker contacts the privacy office to see who has been in the record because the patient confronted her about items from those notes.
Scenario #2: Discussion Questions

- What good decisions were made here?
- Do your policies permit or prohibit employee access?
- What other information do you need to address this situation?
- What issues might there be with the social worker notes?
- Who else would you involve in this case?
- Should sanctions be imposed?

Lessons Learned, Part 1:

- Data breaches are not a matter of if, they are a matter of when
- Most people do not act with malicious intent
- Human error is a common and preventable cause of many breach events
- Training needs to be regularly reviewed and refreshed with current material (internal and external)
Lessons Learned, Part 2:

- Supplementing training with other methods
- Breaking down silos and implementing multi-disciplinary IRT is a significant cultural change
- Cultivating stakeholders and champions
- Communicating key messages and simple action steps to employees

“Our mission was a failure, but I like to think it was a successful failure.”

James A. Lovell, *Apollo Expeditions to the Moon*
Questions?