A HIPAA Security Incident and Investigation. It Can Happen to You.

Sandra L. Sessoms, RN, CPHQ, CHC
Director, System Compliance

Robert R. Michalski, CHC
Chief Compliance Officer
Baylor Health Care System

Disclaimer

This presentation and the opinions expressed are not necessarily those of the West Penn Allegheny Health System and it is not intended to provide all the information that is needed to audit or comply with various information privacy or security requirements.
Overview of Presentation

1. The Breach
2. Response to Breach
3. Corrective Actions
4. Notification of Audit
5. Audit Process
6. Response/Corrective Actions
7. Lessons Learned
8. Questions and Discussion

Course Objectives

This presentation will provide the participant with:

- An overview of an actual federal investigation from the viewpoint of a healthcare provider.
- The role of the internal audit and compliance department in auditing to validate allegations.
- The role of the internal audit and compliance department in developing a response to findings and an action plan for correction.
- Strategies to effectively communicate findings and corrective actions to external agents or auditors.
West Penn Allegheny Health System

Key Statistics
- Located in Pittsburgh, Pennsylvania
- Tertiary Hospitals:
  - Allegheny General Hospital
  - The Western Pennsylvania Hospital
- Community Hospital Campuses:
  - AGH -Suburban Campus
  - Alle-Kiski Medical Center
  - Canonsburg General Hospital
  - WPH-Forbes Regional Campus
- Houses nearly 2,000 beds
- Employs over 13,000 people
- Admits nearly 79,000 patients per year
- Logs over 200,000 emergency visits

The Breach: November 2007

- Home Care Employee’s business laptop computer stolen from home during robbery
- Software housed patient demographics, protected health information, Medicare numbers, Social Security numbers
- Computer was left on and database to patient information was left open.
Self-Investigation

- Implemented Security Incident Policy with Identified Team Members
- Tested computer settings to determine if computer auto logged off
- Evaluated database size and elements
- Examined state law for disclosure requirements

Response to Breach

- Interviews with Media
- Establishment of Call Center
- Notification of Patients
- Offering of Credit Monitoring Services
- Daily conference calls to discuss and mitigate issues
- Second Notification of Returned Notification Letters
- Notification of Guarantors
Root Cause Analysis

- Issues identified:
  - Lack of automatic sign-off
  - Lack of modern encryption methodology
  - Lack of limits on the number of patients maintained in database
  - Storing of social security numbers of patients and guarantors

Corrective Actions Implemented

- Auto Log Off mandated and installed
- Medicare and Social Security numbers removed
- Storage of patient data limited to current and recent patients
- Staff re-educated on changes
Fast Forward: April 2008

- Audit Notification: April 30, 2008
  - Letter Sent by PricewaterhouseCoopers on behalf of CMS
- Phone Call Received: May 14, 2008
- Conference Call Held: May 19, 2008
  - Scope of Audit
  - Expectations
  - Initial List of Documents
- Entrance Conference: May 27, 2008
  - Areas of review
  - Primary criteria for evaluation
  - Reporting process
  - Clarification of documents requested

Documents Requested for Review: Administrative Safeguards

- Policies and Procedures on:
  - protection of PHI and EPHI
  - monitoring of access, violations, and follow-up activities
  - granting access, role based profiles and remote access profiles
  - transfer of access
  - recertification of access
  - virus identification software
  - passwords
Documents Requested for Review: Administrative Safeguards

- Risk Assessments
- Job Description for Privacy/HIPAA Official
- Training Materials
- Internal Audit review of HIPAA compliance
- Lists
  - Incident Response Team Members
  - Employees (name, dept/cost center and job title, hire date)
  - IS organization chart, including HIPAA Security Officer

Documents Requested for Review: Physical and Technical Safeguards

- Policies and Procedures (Physical Safeguards)
  - Maintenance of hardware
  - Workstation security
- Policies and Procedures (Technical Safeguards)
  - Use of generic, group or system IDs
  - Disabling vendor supplied defaults
  - Dial-up remote access
  - Encryption/decryption
  - Transmission security
Documents Requested for Review: Physical and Technical Safeguards

- Configuration standards for platforms which store, transmit or process EPHI
- Evidence of implementation of password policies on platforms which store, transmit or process EPHI
- List of all users with dial-up/remote access
- Listing of all user IDs with access to all datasets/files within scope application and General Support Systems

Documents Requested for Review: Remote Access

- Policies and Procedures
  - Back-up of data into remote devices
  - Downloading of EPHI on remote devices
  - Protecting lost or stolen credentials
  - Granting remote access
  - Entity-wide configuration management
  - Entity-wide patch management
- Rules of behavior/personal security for laptop users
- Firewall protection on laptops
- Connection settings for email
- Lists of providers with remote access and laptops
Onsite Audit: May 27- June 9, 2008

- Opening Meeting
- Discussion of Breach and Response
- Interviews
- Formal Updates

Standards Used by Auditors

- HIPAA Security Rules
- National Institute for Standards and Technology (NIST)
- CMS HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information
Testing of Policies

- Granting of Access
- Password Management
- Log On Procedure
- Auto Log-off

Audit Findings

- Corporate-wide policies not updated at specific hospital site
- Not abiding by internal policy for use of locking cables
- Access authorization forms not completed for users who were part of a conversion
- Lack of system-wide patch management policy
Audit Findings

- Password policy did not require complex passwords
- Laptops did not have auto log-off although the software application was updated for this after the incident.
- Lack of detailed guidance on acceptable storage mediums for EPHI

Corrective Action Plan

- Established policy for:
  - Access authorization
  - Patch management
  - Annual user recertification
- Purchased locking cables
- Added formal approval page for risk assessment
- Added review dates to all policies/procedures to track changes; addressed timely updating of policies promulgated by HIPAA Security Officer
- Education and Auditing
Corrective Action Plan

- Hired a full-time dedicated HIPAA Security Officer!

Lessons Learned

- Limit storage of data on mobile devices
- Monitor vendors for maintaining compliance with HIPAA security standards
- Do not permit deviation from policy; require notification of HIPAA Security Officer
- Audit compliance with policies
- Audit corrective action plans
Lessons Learned

- Working with Auditors:
  - Timely response
  - Organization
  - Dialogue
  - Honesty

Audit Tools

- Audit checklist for security of portable devices with or without remote access
- Sample policy on “Locking Cables”
References


Questions, Answers and Open Discussion

Sandra L. Sessoms  Robert R. Michalski  
Director, System Compliance  Vice President, System Compliance
ssessoms@wpahs.org  rmichals@wpahs.org

West Penn Allegheny Health System  
Two Allegheny Center, Suite 100  
Pittsburgh, PA 15212  
412-330-4960

Thanks for joining us today!