IT’S 10:00 AT NIGHT: DO YOU KNOW WHERE YOUR CELL PHONE IS?

Mobile Devices and Protected Health Information

October 14, 2014
Presented by: Lawrence J. Tabas, Esq. and Jenna K. Shedd, Esq.

Disclaimer and Copyright Notice

Disclaimer: This presentation is only intended as a high level summary and is not intended to be legal advice. Please consult with an attorney for advice specific to individual circumstances.

Note: Due to time constraints, some slides will not be covered in this presentation and are included as resources only.

All images used in this presentation are for educational and teaching purposes only. All images are either in the public domain and not subject to copyright, or they have been purchased from iStock. Any and all marks used throughout this presentation are trademarks of their respective owners.

Note: URLs were last updated as of September 3, 2014.

MEET THE HEALTH LAW GURUS™

WE’RE NOW LIVING IN A WORLD OF INSTANT AND CONSTANT COMMUNICATION

The First Computer

Print
NEW TECHNOLOGY HAS CREATED NEW RISKS TO PRIVACY AND PROTECTED HEALTH INFORMATION ("PHI")
What is PHI?

- Individually identifiable health information.
- Broadly defined and includes more than just health information. For example:
  - Full name
  - Social security number
  - Date of birth
  - Home address
  - Account number
  - Diagnosis
  - Disability code
- Transmitted by or maintained in electronic media or in any other form or medium.

The Health Insurance Portability and Accountability Act ("HIPAA")

Requires entities that create, receive, maintain or transmit PHI to protect such PHI against unauthorized use or access.

Who Must Comply with HIPAA?

- Covered Entities - Health care providers, health plans, health care clearinghouses.
- Business Associates - Any person or entity that in the course of performing certain functions, services, or activities on behalf of a Covered Entity, has access to, uses, or discloses PHI.
Mobile Devices and PHI

• In this age of modern technology, you must take steps to secure PHI on mobile devices to protect against the risk of a HIPAA breach.

• A PHI breach can trigger a government investigation and enforcement action, which can result in substantial financial penalties and other corrective action.

• Damage to your reputation and your customers'/clients' confidence.

What is a Breach?

• Old Rule: Significant risk of financial, reputational, or other harm to the affected individual.

• New Rule: Presumed to be a breach, unless there is a low probability that the PHI has been compromised.

• Note: Breach exceptions for unintentional access, inadvertent disclosure, and no retention of the PHI.

Risk Assessment Factors

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.
Reporting Requirements for PHI Breach

• When
  – Federal and state guidelines

• How
  – Writing, email, online posting

• Who
  – Patients/Individuals
  – Secretary of the U.S. Department of Health and Human Services
  – State Authorities
  – Media

Enforcement

• There is greater and more intense oversight, and penalties have increased.

• GAO Report - HHS Office for Civil Rights ("OCR") must:
  – Improve guidance and oversight of HIPAA compliance; and
  – Proactively monitor HIPAA compliance.
  – See the report:

You Must Conduct a Risk Analysis

• Covered Entities and Business Associates must comply.

• Required by the HIPAA Security Rule.
  45 C.F.R. § 164.308(a)(1)(i)(A)

• Assess risks and vulnerabilities to PHI (ensure confidentiality, integrity, and availability of PHI).

• Methodologies vary depending on the size, complexities, and capabilities of the organization.

• See HHS guidance regarding elements of a risk analysis:
Elements of a Risk Analysis

1. Scope
2. Data collection
3. Identification and documentation of threats and vulnerabilities
4. Assessment of current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation
9. Periodic review and updates

Develop A Risk Management Plan

- Your management and other key decision makers must be involved.
- Prioritize risks that you identify from the risk analysis.
- Determine options for mitigating the risks (consider required v. addressable risks).
- Develop a plan for implementing security measures.
- Train all staff and retrain regularly.

Implement Policies and Procedures

- Some examples are as follows:
  - Designation of privacy/security officer(s);
  - Breach notification procedures - to include a 24/7 toll-free hotline, answered by a live trained person;
  - Mobile device and BYOD policies;
  - Access to PHI at and away from the workplace;
  - Password protection and remote wiping;
  - Encryption; and
  - Training and personnel accountability.
Monitor Compliance!

• Policies and procedures are pointless if you do not appropriately monitor.

• In all compliance programs, having a plan and not following it is worse than not having a plan at all.

• Enforce your compliance plan and individual accountability.

Business Associate Agreements (BAAs)

• BAAs are required.

• Make sure BAAs are always updated.

• See required and optional provisions here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Business Associate Agreements (BAAs)

• BAAs are necessary to:
  – Set forth the permissible uses and disclosures of PHI
  – Ensure that the Business Associate remains contractually required to perform certain activities for which direct liability does not attach
  – Establish respective responsibilities under HIPAA
  – Notify the Business Associate of its status under HIPAA, so that it is fully aware of its obligations and potential liabilities

Department of Health and Human Services/Office for Civil Rights
HIPAA Enforcement

- Security Risk Areas (identified by OCR)
  - Failure to perform a risk analysis
  - Failure to implement protections for mobile devices that store PHI
  - Failure to properly control and monitor access to PHI

- Privacy Risk Areas (identified by OCR)
  - Individuals’ rights to receive a Notice of Privacy Practices, access their PHI, and authorize disclosures of their PHI


The OCR is Calling: Preparing for OCR Audits and Breach Investigations

- Covered entities and business associates may be audited and/or investigated for a breach of PHI.

- Investigations may be initiated by the report of a breach of PHI or a third party complaint.

- If you are audited or investigated by HHS, expect to produce documents and answer questions relating to all aspects of your HIPAA compliance program.

The OCR is Calling: Preparing for OCR Audits and Breach Investigations

- Have you performed a risk analysis (i.e., a pre-breach review and determination of vulnerabilities and risks to PHI)?

- Can you produce documentation that you conducted a risk analysis?

- Do you have documentation of the specific actions taken in response to the findings of the risk analysis?
The OCR is Calling: Preparing for OCR Audits and Breach Investigations

• Policies and procedures regarding:
  – Access to PHI
  – Access to and removing PHI from the worksite
  – Password protection/remotely wiping devices
  – Encryption

• Do you have a Privacy and Security Officer responsible for your HIPAA compliance?

The OCR is Calling: Preparing for OCR Audits and Breach Investigations

• Do you train and retrain your employees in HIPAA compliance?

• How often do you retrain?

• Do you have documentation (i.e. sign-in sheets, written acknowledgements) to show that employees have attended training and understand their continuing obligations?

• Can you provide HHS with training materials?

CASE STUDIES: RECENT REPORTED PHI BREACH CASES

Source: http://www.hhs.gov/ocr/office/index.html
Community Health Systems, Inc.

- 4.5 million individuals affected by a Chinese cyber-attack.

- Malware and technology used to attack network.

- CHS has completed remediation efforts to protect against future intrusions.

Parkview Health System, Inc.

- Medical records left unattended in physician’s driveway; $800,000 settlement.

- You must safeguard PHI in non-electronic form as well.

- Training is key.

- How do you protect PHI during transfer and disposal?

Affinity Health Plan, Inc.

- Failure to wipe PHI from leased photocopier hard drives; $1,215,780 settlement.

- Copiers are electronic devices!

- Review your contracts with equipment suppliers.

- Make sure PHI stored on copiers is addressed by policies and procedures.
New York and Presbyterian Hospital and Columbia University
- Server breach and PHI became available on public search engines; $4.8 million settlement.
- Breach caused by deactivated server.
- Servers lacked technical safeguards.
- No risk analysis prior to breach.

Concentra Health Services and QCA Health Plan Inc. of Arkansas
- Theft of unencrypted laptops; $1.725 million settlement (Concentra); $250,000 settlement (QCA).
- Theft from physical therapy center and theft from employee’s car.
- Lack of encryption.
- Lack of sufficient policies and procedures.

Adult & Pediatric Dermatology, P.C.
- Stolen thumb drive; $150,000 settlement.
- Encrypt devices.
- Implement breach notification policies and procedures.
- Training.
WellPoint, Inc.

• Failure to implement appropriate safeguards before upgrading information systems; $1.7 million settlement.

• Use extra caution when using web-based applications or portals.

• Analyze risks and implement appropriate safeguards prior to making changes to information systems.

OTHER FACTUAL SCENARIOS THAT COULD RESULT IN A PHI BREACH

Example #1

• One morning you realize that your cell phone is missing. You last saw it the night before. After a diligent search, the phone cannot be located.
  – Not password protected
  – PHI on the phone is not encrypted
  – Work accounts are synced to the phone
  – The PHI contained on the phone through emails or otherwise includes SSNs, test results and images, patients’ names, and patients’ medical history

• Is this a breach?
• Does it matter if the phone was lost or stolen?
Example #2

- A patient emails you seeking medical advice and describes her medical symptoms. She sends the email to your personal email account. You respond from your personal email account.
- Is this a breach?
- Is there a difference if this is done by text?
- If there a difference if you respond from your work account?

PRACTICAL TIPS AND REMINDERS

Lessons Learned

1. CONDUCT A RISK ANALYSIS!
2. Establish security policies and procedures and update regularly (including policies for off-site PHI access).
3. Require strong passwords on all mobile devices and regular changing of passwords.
4. Train employees and retrain regularly.
5. Monitor compliance on an on-going basis.
6. Require and encourage immediate reporting.
7. Establish disciplinary policies for employee non-compliance.
8. Identify and log all mobile devices used by your employees.
9. Encryption
10. Document everything!
Protecting and Securing Information on Mobile Devices (HealthIT.gov)

- Encryption
- Passwords or other user authentication
- Wiping and/or remote disabling
- Do not use file sharing applications
- Firewalls
- Updated security software to protect against malicious applications, viruses, spyware, and malware-based attacks
- Do not download unknown applications
- Maintain physical control of your device
- Beware of public Wi-Fi networks
- Wipe devices before discarding or returning them

Commingling Work And Personal Email Accounts

- WARNING! – DO NOT FORWARD EMAILS FROM YOUR WORK ACCOUNT TO YOUR PERSONAL EMAIL ACCOUNT

- Work Accounts – Encryption and remote wiping capabilities protect the device if it is lost or stolen.

- Personal Accounts – Limited protection from potential HIPAA breach.

Cyber Insurance

- Consider purchasing a cyber insurance policy.

- Purchase a broad policy (covering all types of data).

- Not a complete safeguard, but may have certain benefits (e.g., covers the cost of fines, legal costs, breach notification costs etc.)
Some Risk Analysis Resources


Visit the Health Law Gurus™ at www.healthlawgurus.com