Privacy and Information Security Law

Elizabeth Ortmann-Vincenzo

CLASS 10

October 25, 2016

Health Privacy pt. 2; Consumer Data pt. 3

HIPAA

- What is HIPAA?
  - Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule
    - addresses the use and disclosure of individuals' health information
  - Security Rule
    - Requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address them

2

Security Rule Basics

- "The Security Standards for the Protection of Electronic Protected Health Information (the **Security Rule**) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called 'covered entities' must put in place to secure individuals' 'electronic protected health information."
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

3

Security Rule

- Security rules only applies to e-PHI
- Sets forth administrative, physical, and technical safeguards
  - Safeguards are either required or an alternative may be chosen if justified by explanation

4

Basic Responsibilities under the Security Rule

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- Ensure compliance with this subpart by its workforce.

5

How to carry out responsibilities

- Administrative Safeguards, e.g. policies and procedures
- Technical Safeguards, e.g. system access controls
- Physical Safeguards, e.g., facility access controls
- Required vs Addressable

6

Flexibility

- "[W]hen a covered entity is deciding which security measures to use, the Rule **does not dictate those measures** but requires the covered entity to consider:
  - Its size, complexity, and capabilities,
  - Its technical, hardware, and software infrastructure,
  - The costs of security measures, and
  - The likelihood and possible impact of potential risks to e-PHI

  http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

7

Administrative Safeguards

Required Security Management:
- Risk Analysis
- Risk Management
- Sanctions
- Activity Review

Assigned Security Responsibility
Workforce Security

8

Administrative Safeguards

- **Information Access Management**
- **Security Awareness & Training**
- **Security Incident Procedures**
- **Contingency Planning**
- **Evaluations**
- **Business Associate Agreements**

9

Physical Safeguards

- **Facility Access**
- **Workstation Use**
- **Workstation Security**
- **Device and Media Controls**

10

Technical Safeguards

- Access controls
- Audit Controls
- Integrity
- Authentication
- Transmission Security

11

Breach

- **Breach** means the acquisition, access use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

12

Breach Exclusions

- Any unintentional acquisition, access, or use of protected health information by a person acting under the authority of a CE or BA, if it was made in good faith and within the scope of authority and does not result in further use or disclosure
- Any inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, and the information received as a result of such disclosure is not further used or disclosed
- A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

13

Breach Analysis

Acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

14

Breach Notification Rule

- Individual
- Government
- Media
- Covered Entity (if breach occurs by Business Associate)

15

HIPAA Complaints

Most investigated complaints:

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Uses or disclosures of more than the minimum necessary protected health information; and
5. Lack of administrative safeguards of electronic protected health information.

16

HIPAA Enforcement

17

Genetic Information Nondiscrimination Act

- Prevents insurance companies and employers from using genetic tests to deny individuals health coverage or employment

18

Consumer Data Privacy
Part 3

19

Telephone Consumer Protection Act (TCPA)

- Outgoing calls, texts, faxes
- Auto dialer OR Robo voice
- Not applicable to calling businesses, only consumers
- Different Rules for Residential vs Mobile
- Consent is the key

20

Telephone Consumer Protection Act (TCPA)

- Do not call lists
- Ability to not received further calls after opting out
- Prohibitions on pre-recorded calls and certain auto dialers
- Prohibitions on unsolicited fax advertisements

21

1st Amendment Protection of Commercial Speech

- Commercial speech receives constitutional protection
- However, it is of lower value and receives less protection

22

Program Completed