POST & SCHELL PC
ATTORNEYS AT LAW

PHCA Annual Convention & Trade Show
September 26, 2019

HIPAA And Staff Terminations: Managing Access to Prevent Breaches

Cynthia A. Haines
717-612-6051
CHaines@postschell.com

Kate A. Kleba
215-587-1113
KKleba@postschell.com

1

Overview

- The Health Insurance Portability and Accountability Act (HIPAA)
  - The Legal Framework of HIPAA
  - Training, Managing and Tracking Access to PHI
- Risks of a Data Breach
  - Possible Penalties
  - Reputational Harms
- HIPAA Breach Assessment and Response
  - Types of Breaches
  - Breach Response
- Best Practices When Off-Boarding Employees
  - Off-Boarding Policies and Protocols
  - Enforcement and Logistics

2

The Legal Framework

- The Health Insurance Portability and Accountability Act (HIPAA)
- Public Law 104-191 (1996)
- Overseen by: Department of Health & Human Services ("HHS") and enforced by Office for Civil Rights ("OCR")
- Regulations on:
  - Privacy of health information
  - Security of health information
  - Notification of breaches of confidentiality
  - Penalties for violating HIPAA

3

Summary of the Law

- The basic purpose of the law:
  - To establish basic privacy and security protection of health information
  - To guarantee individuals the right to access their health information and learn how it is used and disclosed
  - To simplify payment for health care

4

What Is Protected By HIPAA?

Protected Health Information (PHI)

- Any Individually Identifiable Health Information
- Created or received by a health care provider, health plan, or health care clearinghouse
- Relating to the past, present or future physical or mental health or condition of an individual (including information related to payment for health care)
- Transmitted in any form or medium - paper, electronic and verbal communications

5

What Is Protected By HIPAA?

Examples of PHI:

- Medical charts
- Problem logs
- Photographs and videotapes
- Communications between health care professionals
- Billing records (including Medicare Claims)
- Health plan claims records
- Health insurance policy number

6

Identifiers

- Name
- Geographic subdivisions smaller than a State
- Street Address
- City
- County
- Precinct
- Zip Code & their equivalent geocodes, except for the initial three digits
- Dates, except year
- Birth date
- Admission date
- Discharge date
- Date of death
- Telephone numbers
- Fax number
- E-Mail Address
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locations (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable data
- Any other unique identifying number, characteristic, or code

7

Training, Managing and Tracking Access to PHI

- The Security Rule specifies safeguards that CEs must implement to protect ePHI confidentiality, integrity and availability. Specifically, CEs must:
  - Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated impermissible uses or disclosures; and
  - Ensure compliance by their workforce

8

Training, Managing and Tracking Access to PHI

- Covered entities (CEs) are required to have policies and procedures in place regarding the handling of PHI
  - These security measures should be designed to reduce risks and vulnerabilities
    - This is not one-size-fits-all
  - CEs must designate a security official who is responsible for developing and implementing its security policies and procedures

9

Policy Content: Key Points

- People consider health information their most confidential information, and as such the we must protect it accordingly:
  - Do not access PHI that you do not need
  - Do not discuss PHI with individuals who do not need to know it
  - Do not provide PHI to anyone not authorized to receive it
  - Misusing PHI can result in discipline, legal penalties and loss of trust

10

Policy Content: Key Points

When using PHI, think about:

- Where you are
- Who might overhear
- Who might see

Avoid:

- Discussing PHI in front of others who do not need to know
- Leaving records accessible to patients or others who do need to see them
- Positioning monitors where others can view them
- Using printers located in public or unsecured areas

11

Policy Content: Key Points

Do not engage in risky practices with computers used to access PHI

- Do not surf the internet
- Do not open attachments to e-mail unless from a trusted source
- Do not install applications unless approved by IT Department

12

Policy Content: Key Points

- Do not unnecessarily print or copy PHI
- When faxing PHI, use a fax cover page
- Do not send PHI in email unless first cleared by your supervisor
- Dispose of PHI when it is no longer needed
- Use shredding bins for paper records
- When retiring electronic media used to store PHI, ensure the media is "cleansed" according to IT Department standards
- Call Help Desk for more details

13

Policy Content: Key Points

- Report unusual activity to your supervisor immediately
- You observe questionable practices
- You find PHI in inappropriate areas
- You suspect unauthorized use of your user ID/password

14

Policy Content: Key Points

- The consequences of failing to adhere to the policy
  - CEs must have and apply appropriate sanctions against those who violate policies and procedures in order to deter noncompliance
  - Should be aimed at reinforcing the substance of the HIPAA access policy

15

Training

- Both the Privacy Rule and the Security Rule impose training requirements
  - In general, anyone who comes into contact with PHI must be trained
- Neither Rule specifies the exact content of the required training
  - In general, training should be keyed to each person's role in the organization

16

Risks of a Data Breach

Civil Penalties

17

Risks of a Data Breach

- Civil Monetary Penalties (CMPs) based on tiered civil penalty structure depending on the level of culpability as determined by the Secretary of HHS
  - Unknowing - $100 to $50,000 per violation
  - Reasonable cause - $1,000 to $50,000 per violation
  - Willful neglect corrected within 30 days - $10,000 to $50,000 per violation
  - Willful neglect not corrected within 30 days – no less than $50,000 per violation

18

Risks of a Data Breach

Criminal Penalties

19

Risks of a Data Breach

- OCR can refer HIPAA violations to the Department of Justice (DOJ)
  - Directors, officers or employees could be deemed criminally liable
  - Different levels of severity depending on the level of culpability
    - Penalties range from a fine of $50,000 and imprisonment up to one year to a fine of $250,000 and imprisonment up to 10 years
    - Restitution possible if patients have been defrauded

20

Risks of a Data Breach

- Reputational Harm
  - OCR maintains a *permanent* and *searchable* breach portal (aka the "Wall of Shame") listing breaches of unsecured PHI affecting 500 or more individuals
    - The Wall of Shame includes the details of the breach including the name of the entity breached, the type of breach, the location of the breach and the number of people affected
  - News Coverage

21

Enforcement Results As Of July 31, 2018

- To date: 186,453 HIPAA complaints filed and OCR has initiated over 905 compliance reviews
- OCR investigated and resolved over 26,152 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA CEs and their BAs
- OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the CE or their BA
- OCR has settled or imposed a civil money penalty in 55 cases resulting in a total dollar amount of $78,829,182.00
- In another 11,518 cases, OCR investigations found no violation had occurred

22

HIPAA Breach Assessment and Response

- What is a Breach?
  - A Breach is an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI and poses a significant risk of financial, reputational or other harm to the individual

23

Types of Breaches

- Hacking/IT Incident
- Unauthorized Access/Disclosure
- Theft
- Improper Disposal
- Loss
- Other

24

How Breaches Can Occur: Examples

- Faxing PHI to the wrong fax number
- Theft or misplacement of a laptop, tablet, flash drive, or CD containing PHI
- Clicking on a link in an email or using a computer infected with a virus or malware
- Improperly disposing of electronic equipment containing PHI
- "Snooping" by members of the workforce

25

Wall of Shame and other Examples

- Texas HHS
- Hippler
- Hospice of North Idaho (HONI)
- Pagosa Springs Medical Center
- UCLA School of Medicine

26

Breach Assessment and Response: Questions To Consider

- Was there a breach?
- Do individuals need to be notified?
- Why did this occur?
- How will the breach be mitigated?
- How do we prevent this from happening again?
- Who needs to be involved in risk analysis/ mitigation/future prevention?

27

Breach vs. Incident

- Breach
  - Acquisition, access, use or disclosure of PHI
  - In a manner not permitted under the HIPAA Privacy Rule
  - Which compromises the security and privacy of PHI
- Incident
  - The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system

28

Exceptions To Breach

- *Unintentional* access or use by workforce member if
  - Made in good faith
  - Within scope of authority to access
  - Does not result in further breach
- Inadvertent disclosure from one authorized person to another *authorized* person
- Disclosure where CE has good faith belief that person receiving the information would not reasonably be able to retain such information

29

Presumption of Breach

- Impermissible access, use or disclosure of PHI is ***presumed*** a breach ***unless*** Covered Entity ("CE") or Business Associate ("BA") shows a "low probability" that PHI has been "compromised"
- Determine such probability based on risk assessment

30

Risk Assessment

- Risk assessment requires consideration of at least:
  - Nature and extent of PHI involved
  - Unauthorized user or recipient of PHI
  - Whether PHI *actually* acquired or viewed
  - Extent to which risk to PHI was mitigated
- Assess risk of harm to privacy and security of data, not harm to individual

31

Risk Assessment Factor 1

- Nature/extent of PHI involved, types of identifiers and re-identification risk
  - Whether data is of a sensitive nature
  - Financial, credit card, SSN, DLN
  - Risk of ID theft?
  - Type, amount and effect of clinical data
  - Potential for harm to individual or value to unauthorized person

32

Risk Assessment Factor 2

- Unauthorized user or unauthorized recipient
  - Differences between snoopers, hackers and surfers
  - ID thief versus hardware thief
  - Does recipient have duty to protect?
  - Ability to re-identify

33

Risk Assessment Factor 3

- Was PHI *actually* accessed or used?
  - Must consider actual vs. opportunity
  - Must affirmatively show PHI not accessed
  - Cannot just assume no access
  - System/computer forensics used as example

34

Risk Assessment Factor 4

- Extent risk to PHI has been mitigated
  - Always attempt to mitigate - quickly
  - Consider obtaining assurances
    - Keep PHI confidential
    - Agree to return/destroy
  - Keep in mind HIPAA Security Rule requirements on responding to security incident, reassess risk, manage risks

35

Breach Response: We have a Breach, Now What?

- Notification
  - Upon discovery of a
  - Breach of
  - Unsecured PHI
  - A CE and a BA must notify
  - Individuals, HHS and sometimes media (>500)
  - Subject to certain exceptions

36

Discovery of Breach

- Considered discovered if breach is known, or
- By exercising reasonable diligence, would have been known to a workforce member or agent of CE

37

Notification to Individual

- Must be timely –
  - Without unreasonable delay
  - No later than 60 days
- Must be in writing
- Elements
  - Description of what happened
  - Date of breach
  - Date of discovery
  - Description of PHI involved
  - Steps the person should take to protect self
  - Steps CE is taking to investigate, mitigate and protect from future breaches
  - Contact information to ask follow up questions

38

Notification to Media

- Only if breach involves more than 500 residents of a state or jurisdiction
  - Notify prominent media outlets serving the state or jurisdiction
  - Same elements as notification to individual

39

Notification to Secretary of HHS

- If **more than 500** individuals involved
  - Must notify Secretary at the same time CE notifies individual
  - HHS website describes manner of notification
- If **less than 500** individuals involved
  - Maintain a log
  - Provide log to Secretary within 60 days following end of calendar year
  - HHS website describes manner of notification

40

Protections

- Vigilance
  - Review policies and procedures
  - Document implementation
  - Document training and attendance
  - Encryption
- Risk Analysis
  - Review HHS Risk assessment tool
- Top-down buy in
  - Board must be involved
- Cyber Insurance

41

Best Practices When On- and Off-Boarding Employees

Failing to Plan is Planning to Fail!

- Designate a department or individual to monitor and approve access and use of systems containing PHI/ePHI
- Have a system in place to track which employees have access to which systems and physical locations
- Control access and rights to all devices issues to employees
- Require all new employees to have their own individual logins and passwords
- Don't let employees have administrative rights to computers

42

Off-Boarding Policies and Protocols

- Designate someone to be the point-person who "owns" off-boarding
  - Use a checklist so nothing is forgotten or overlooked
  - Take actions to remove access quickly as possible
  - Notify and coordinate with IT and/or security when employees leave/give notice

43

Key Points for Off-Boarding

- Terminate electronic access to PHI
  - Remove departing employee from authorized user lists, email distribution lists
  - Change passwords for remote computer systems (VPN, remote desktop, and remote web tools)
  - Change passwords and PINs for on-site workstation, voicemail and email
  - Terminate electronic accounts if necessary
  - Collect mobile devices and other company-owned physical assets and files
  - Purge any PHI that may be on departing employee's personal devices and terminate access to PHI from such devices going forward.

44

Key Points for Off-Boarding

- Terminate physical access to PHI
  - Turn off keycard access
  - Collect physical keys, keycards, ID badges, and security tokens
  - Change combination locks, PINS and security codes

45

Enforcement and Logistics

- Timing/Urgency
  - Circumstances matter!
    - Mobile device management solutions
- Distribution list for departures
  - Inform key departments when employees leave
- Discipline task owners who do not follow off-boarding protocols
  - The role of audits

46

Resources

- OCR Breach Notification website: http://ocrnotifications.hhs.gov/
- Medicare Learning Network, "HIPAA Privacy and Security Basics for Providers," *available at* http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf.
- OCR Security Risk Assessment Audit Tool: http://www.healthit.gov/providers-professionals/security-risk-assessment

47

Resources

- Federal Register 45 C.F.R. Part 160 and Subparts A and E of Part 164.
- Office for Civil Rights ("OCR") Website: http://www.hhs.gov/ocr/office/index.html
- OCR FAQ: http://www.hhs.gov/ocr/office/faq/index.html
- HIPAA List Serve: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html
- Audit Program Protocol: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit /protocol.html

48

Resources

- Health Information Privacy Training Resources: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/sec urityruleguidance.html
- Security Rule Guidance Materials: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/sec urityruleguidance.html
- Technical Assistance from OCR Regional Offices: http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html

49

Questions???

Cynthia A. Haines, Principal
Post & Schell, P.C.
17 North Second Street, 12th Floor
Harrisburg, PA 17101
717-612-6051
CHaines@postschell.com

Kate A. Kleba, Principal
Post & Schell, P.C.
Four Penn Center
1600 John F. Kennedy Blvd.
Philadelphia, PA 19103-2808
(215) 587-1113
KKleba@postschell.com

www.postschell.com

50