HIPAA Compliance

Anne-Sophie Whitaker, Supervisory Equal Opportunity Specialist, OCR
Lakeisha Applegate, Investigator

HCCA Boston Regional Conference
September 10, 2021

1

Who We Are

As the Department's civil rights, conscience and religious freedom, and health information privacy rights law enforcement agency, OCR investigates complaints, enforces rights, and promulgates regulations, develops policy, and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws.

2

Presentation Overview

- Overview of HIPAA Privacy, Security, and Breach Notification Rules
- Compliance Challenges
- OCR Enforcement

3

HIPAA Privacy Rule Overview

4

Scope: Who is Covered?

Limited by HIPAA to:

- Covered entities (CE)
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard (e.g., billing insurance electronically)
  - Health plans
  - Health care clearinghouses
- Business associates (BA)

§ 160.103

Administrative Requirements

- Covered entities must:
  - Designate a Privacy Officer
  - Designate a contact person or office to receive complaints and provide further information
  - Provide privacy training to all workforce members
  - Develop and apply sanction policy for workforce members who fail to comply
  - Implement policies and procedures designed to comply with standards

§ 164.530

Administrative Requirements (cont.)

- Covered entities must:
  - Implement administrative, technical, and physical safeguards to protect privacy of PHI
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable
  - Provide an internal complaint process for individuals
  - Refrain from intimidating and retaliatory acts
  - Not require individuals to waive their rights

§ 164.530

7

HIPAA Security Rule Overview

8

OCR Approach to HIPAA Security

- Standards to ensure the confidentiality, integrity, and availability of ePHI
- Through reasonable and appropriate safeguards
- Addresses risks and vulnerabilities identified through analysis and management of risk
- Appropriate to the size and complexity of the organization and its information systems
- Technology neutral

9

Standards and Implementation Specifications

Standards

- Required - A covered entity (and business associate) must comply with the standards

Implementation Specifications

- Required - a covered entity must implement the specification
- Addressable - a covered entity must assess whether the specification is reasonable and appropriate in its environment and document its decision to either implement the specification or implement an equivalent alternative

10

Organizational Requirements

Organizational Requirements

- Contains the standards for business associate contracts and other arrangements
- Contains the requirements for group health plans

Policies and Procedures and Documentation Requirements

- Requires the implementation of reasonable and appropriate policies and procedures
- Requires the maintenance of documentation (written or electronic)
- Establishes the retention, availability, and update conditions for documentation

11

Breach Notification Rule

12

Definition of Breach

- The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules which compromises the security or privacy of the PHI
- Impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment

Exceptions to the definition of breach

1. Unintentional acquisition, access, or use of PHI by workforce member or person acting under the authority of a CE or BA if done in good faith and in the scope of authority and there is no further impermissible use or disclosure of the PHI.
2. Inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI at the same CE or BA or OHCA and the information received is not further impermissibly used or disclosed by the recipient.
3. CE or BA have a good faith reason to believe the unauthorized recipient could not reasonably have been able to retain the information.

Compliance Challenges

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

15

15

OCR's Right of Access Initiative

Common Compliance issues:

- Untimely Access
- Unreasonable Fees
- Form and Format
- Validation Burdens
- Withholding Access for Non-Payment of Health Care Fees

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

16

16

Lack of Business Associate Agreements

HIPAA generally requires that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. *See 45 CFR § 164.308(b).* Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involve access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider.

17

Incomplete or Inaccurate Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization]. *See 45 CFR § 164.308(a)(1)(ii)(A).*
- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.
- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.); Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

18

The Risk Analysis Process: Key Activities Required by the Security Rule

- **Inventory** to determine where ePHI is stored
- **Evaluate** probability and criticality of potential risks
- **Adopt** reasonable and appropriate security safeguards based on results of risk analysis
- **Implement/Modify** security safeguards to reduce risk to a reasonable and appropriate level
- **Document** safeguards and rationale
- **Evaluate** effectiveness of measures in place
- **Maintain** continuous security protections
- **Repeat**

Failure to Manage Identified Risk

- The Risk Management Standard requires the "[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." *See 45 CFR § 164.308(a)(1)(ii)(B).*
- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the organization failed to act on its risk analysis and implement appropriate security measures.
- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.

Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented unless not reasonable and appropriate. *See 45 CFR § 164.312(e)(2)(ii).*
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

Lack of Appropriate Auditing

- The HIPAA Rules require the "[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *See 45 CFR § 164.312(b).*
- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." *See 45 CFR § 164.308(a)(1)(ii)(D).*
- Activities that could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees
  - Failed log-in attempts

No Patching of Software

- The use of unpatched or unsupported software on systems that access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software that should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. *See 45 CFR § 164.308(a)(3).*
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). *See 45 CFR § 164.308(a)(3)(ii)(B).*
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. *See 45 CFR § 164.308(a)(3)(ii)(C).*

Disposal

- When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. *See 45 CFR § 164.310(d)(2)(i).*
- The implemented disposal procedures must ensure that "[e]lectronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88: Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."
- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

Insufficient Backup and Contingency Planning

- Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. *See 45 CFR § 164.308(a)(7).*
- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. *See 45 CFR § 164.308(a)(7)(ii)(D).*

Breach Checklist for Covered Entities

1. Has there been an impermissible acquisition, access, use, or disclosure of PHI?
2. Determine whether the incident falls under any of the exceptions to the definition of breach. If no exception, breach is presumed.
3. Provide breach notification, or first conduct risk assessment (see below) to determine whether low probability of compromise. If more than a low probability of compromise, provide breach notification.

Breach risk assessment - determine and document at least:

- Nature & extent of PHI involved
- Who received/accessed the information
- Potential that PHI was actually acquired or viewed
- Extent to which risk to the data has been mitigated

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

27

27

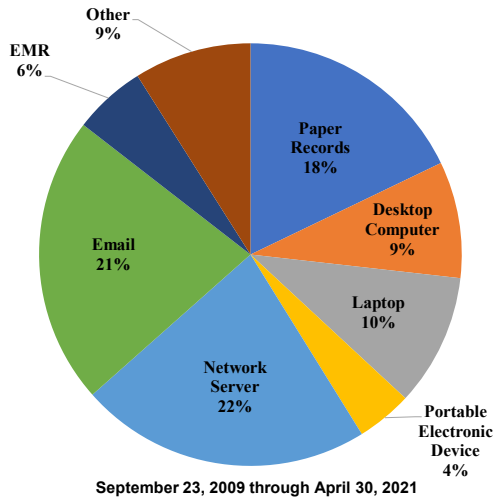
Enforcement

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

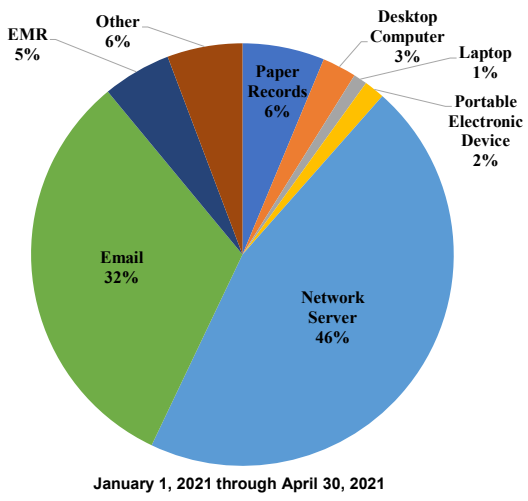
28

28

500+ Breaches by Location of Breach



September 23, 2009 through April 30, 2021



January 1, 2021 through April 30, 2021

29

General HIPAA Enforcement Highlights

- OCR expects to receive over 28,000 complaints this year.
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action.
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action.
- Resolution Agreements/Corrective Action Plans
  - 93 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 6 civil money penalties

As of April 2, 2021

30

Best Practices

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

31

Contact Us

Office for Civil Rights
U.S. Department of Health and Human Services

ocrmail@hhs.gov
www.hhs.gov/ocr

Voice: (800) 368-1019
TDD: (800) 537-7697
Fax: (202) 519-3818

200 Independence Avenue, S.W.
H.H.H Building, Room 509-F
Washington, D.C. 20201

32