U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

HIPAA Security Rule and Breach Notification training

HIPAA Security and Breach Notification Rule Training
For the
Indian Health Service

September 13, 2018

Presented By:
KAREL HADACEK, J.D.

Office for Civil Rights (OCR)

Headquarters - Washington, DC

- Policy and regulations
- Guidance materials
- Centralized Case Management Operations and Customer Response Center

Regional Offices – Denver, San Francisco/Seattle/Los Angeles, Dallas, Chicago/Kansas City, Philadelphia, Boston, New York City, Atlanta

- Investigations
- Technical Assistance
- Outreach

Complaint Process

Complaint

Possible Criminal Violation

DOJ

Accepted by DOJ

DOJ declines case & refers back to OCR

Intake & Review

Possible Privacy or Security Rule Violation

Investigation

Resolution

- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

Resolution

- Entity is not covered by HIPAA
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate HIPAA

Numbers at a Glance

- Over 186,453 complaints received to date
- Over 26,152 cases resolved with corrective action and/or technical assistance
- 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 Civil Monetary Penalties
- Expect to receive 24,000 complaints this year

HIPAA Security Rule Overview

Definitions & General Rules

- Definitions
  - Terms defined in 45 CFR § 160.103 cut across all Admin Simp. Rules
  - Terms defined in 45 CFR § 164.304 specific to the Security Rule
- General Rules
  - Establishes the requirements covered entities (and business associates) must meet
  - Includes the consideration for a flexibility of approach
  - Defines the required standards and implementation specifications (both required and addressable)
  - Requires the maintenance of security measures implemented to support the reasonable and appropriate protection of electronic protected health information

HHS Approach to HIPAA Security

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

Scope: What is Covered?

- Electronic Protected Health Information ("ePHI"):
  - Protected health information
  - Transmitted or maintained in electronic media
- Not ePHI:
  - Electronic Transmission Media excludes:
    - Transmissions of paper
    - Transmissions by facsimile
    - Voice by telephone
  - because the information did not exist in electronic form before transmission

Standards and Implementation Specifications

- Standards
  - 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 not implement the specification and its implementation of an equivalent alternative.

Administrative Safeguards

- Administrative Safeguards
  - "…are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." (*Definitions - 45 CFR § 164.304)*

Physical & Technical Safeguards

- Physical Safeguards
  - "…are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." (*Definitions - 45 CFR § 164.304)*
- Technical Safeguards
  - "…means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." (*Definitions - 45 CFR § 164.304)*

Organizational Requirements

- Organizational Requirements
  - standards for business associate contracts and other arrangements
  - 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

45 CFR § 164.314

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 subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider.
- Contracted technical support
- Cloud provider

Administrative Requirements

Security Management

- Risk Analysis
- Risk Management
- Sanctions
- Information System Activity Review

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

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**

Risk Management Plan

- 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 breaching 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.

Risk Management Guidance

- **OCR Guidance:** https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- HIPAA Security Series – Basics of Risk Analysis and Risk Management
- Security Risk Assessment Tool, Videos: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
- Guide for Small Healthcare Practices

Administrative Requirements

"Apply appropriate sanctions for those who fail to comply with the security policies and procedures of the covered entity or business associate." *See 45 CFR § 164.308(a)(1)(ii)(C).*

"Implement procedures to regularly review records of information system activity review, such as audit logs, access reports, and security incident tracking reports." *See 45 CFR § 164.308(a)(1)(ii)(B).*

Administrative Requirements

- Assigned Security Responsibilities

  Identify the security official responsible for implementation. *See 45 CFR § 164.308(a)(2)*

- 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).*

Administrative Requirements

Address 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).*

- Authorization and/or Supervision (addressable)

  "Authorization and/and or supervision of workforce members who work with ePHI or in locations where it might be accessed." *See 45 CFR § 164.308(a)(3)(i)(A).*

Administrative Requirements

Address Insider Threat

- Workforce Clearance procedure (addressable)
  "Determine that the access of a workforce member to ePHI is appropriate."
  See 45 CFR § 164.308(a)(3)(i)(B).

- 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 (addressable)
  Terminate access to ePHI when a workforce member terminates or service ends *See 45 CFR § 164.308(a)(3)(i)(C).*

Administrative Requirements

- Information access management

  Authorizing access to ePHI consistent with the applicable requirements. See 45 CFR § 164.308(a)(4)(i).

  - Implement policies and procedures for granting access to ePHI . *See 45 CFR § 164.308(a)(4)(ii)(B).*

  - Implement policies and procedures to establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. *See 45 CFR § 164.308(a)(4)(ii)(C).*

Administrative Requirements

- Security awareness and training. *See 45 CFR § 164.308(a)(5)(i).*
- Protection from malicious software (addressable). *See 45 CFR § 164.308(a)(5)(ii)(B).*
- Log-in monitoring of attempts and reporting discrepancies. *See 45 CFR § 164.308(a)(5)(ii)(C).*
- Password management procedures for creating, changing, and safeguarding passwords. *See 45 CFR § 164.308(a)(5)(ii)(D).*

Administrative Requirements

- "Implement policies and procedures to address security incidents." *See 45 CFR § 164.308(a)(6).*
  - Identify and respond to suspected or known security incidents;
  - Mitigate, to the extent practicable, harmful effects of security incidents; and
  - Document security incidents and their outcomes.

Administrative Requirements

- 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).*

Administrative Requirements

- Evaluation: perform a periodic technical and nontechnical evaluation, in response to environmental or operational changes affecting the security of information, that establishes the extent to which a CE or BA's security policies and procedures meet the requirements. *See 45 CFR § 164.308(a)(8).*

Physical Safeguard Requirements

- Facility access controls. *See 45 CFR § 164.310(a)(1).*
- Contingency operations. *See 45 CFR § 164.310(a)(2)(i).*
- Facility security plan to prevent unauthorized physical access, tampering, and theft. *See 45 CFR § 164.310(a)(2)(ii).*
- Access control and validation of a person's access based on their role or function. *See 45 CFR § 164.310(a)(2)(iii).*
- Maintenance records to the physical components related to security (i.e. hardware, walls, doors, locks, etc.) *See 45 CFR § 164.310(a)(2)(iv).*

Physical Safeguard Requirements

- Workstation use. *See 45 CFR § 164.310(b).*
- Workstation security. *See 45 CFR § 164.310(c).*
- Device and Media controls. *See 45 CFR § 164.310(d)(1).*
- Accountability. *See 45 CFR § 164.310(d)(2)(iii).*

Physical Safeguard Requirements

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.

Technical Safeguard Requirements

- Access Control – allow access to ePHI only by those persons or software programs that have been granted access rights. *See 45 CFR § 164.312(a)(1).*
- Unique user identification. *See 45 CFR § 164.312(a)(2)(i).*
- Encryption and decryption of PHI (addressable) at rest (*See 45 CFR § 164.312(a)(2)(iv))* and in motion (*See 45 CFR § 164.312(d)(2)(ii)).*
- Integrity of ePHI – protected from improper alteration or destruction. *See 45 CFR § 164.312(c).*

Technical Safeguard Requirements

- 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 which 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

Technical Safeguard Requirements

Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed 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)

Technical Safeguard Requirements

Software Patching

- The use of unpatched or unsupported software on systems which 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 which 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.)

Mobile Device Security

OCR Cyber Awareness Newsletter (Oct 2017) – Mobile Devices and PHI

HHS HealthIT.gov Resources

Fact Sheet: Managing Mobile Devices in Your Health Care Organization

Presentation: Mobile Devices and Health Information Privacy and Security

Security Rule Resources

- Summary of the HIPAA Security Rule
- Security Rule Guidance Material
  - Security 101 for Covered Entities
  - Implementation for the Small Provider
  - NIST Special Publications; FTC Guidance
- FAQs for Professionals

http://www.hhs.gov/hipaa/for-professionals/security/index.html

Cloud Guidance

- OCR released guidance clarifying that a cloud service provider (CSP) is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.

- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

Ransomware Guidance

- OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
- Fact Sheet: Ransomware and HIPAA

Cyber Security Guidance Material

- HHS OCR has launched a Cyber Security Guidance Material webpage, including a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.

  - Cyber Security Checklist - PDF
  - Cyber Security Infographic [GIF 802 KB]

Cybersecurity Newsletters

- **OCR Cyber Awareness Newsletters**
- Began in January 2016 – Newsletters Archive (2016-2017)
- Sign up for OCR Security Listserv to receive Newsletters
- 2018 Newsletters
  - January 2018 (Cyber Extortion)
  - February 2018 (Phishing)
  - March 2018 (Contingency Planning)
  - April 2018 (Risk Analyses v. Gap Analyses)
  - May 2018 (Workstation Security)

Breach Notification Rule

Definition of Breach

- The acquisition, access, use, or disclosure of PHI 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

No Harm standard (removed with Omnibus)

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.

1. Unintentional acquisition, access, or use - examples

- A billing employee receives and opens an email about a patient that was mistakenly sent to her by a nurse at the same facility. The billing employee alerts the nurse and deletes the email. This would not be considered a breach, as the acquisition of the PHI was unintentional, done in good faith and within the employee's scope of authority.
- A nurse for a covered entity who is authorized to view patient records, decides to access the records of her ex-boyfriend, who is not her patient. The nurse was not acting within her scope of authority because her ex-boyfriend was not her patient, the access was intentional and not done in good faith. The exception would not apply.

2. Good faith belief that information was not retained - examples

- A health plan sends EOBs to the wrong individuals, some of the EOBs are returned by the post office as undeliverable and have not been opened. The covered entity can assume that the PHI of the individuals contained in the unopened, returned EOBs was not breached.
- A nurse mistakenly hands the discharge papers of Patient A to Patient B. However, before Patient B has a chance to look at the papers, the nurse realizes her error and immediately retrieves the paperwork from Patient B. Here, if the nurse can conclude Patient B did not look at Patient A's information, this would not constitute a breach.

Breach Checklist for Covered Entities

1. Has there been an impermissible use or disclosure of PHI?

2. Perform 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

3. Determine if the incident falls under any of the exceptions to the definition of breach

Notification obligation only applies to "Unsecured PHI"

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals.
- Acceptable methods of securing PHI are encryption and destruction.
- Loss or compromise of PHI that has been encrypted or properly destroyed does not trigger the duty to notify or report.

Notification to Individuals

- A covered entity must notify each affected individual following the discovery of a breach of unsecured PHI.
- The obligation to notify applies to those breaches that the covered entity knows about or *should have known* about if exercising reasonable diligence.

"Known or should have known" Standard

- Means that covered entities can be liable for failing to provide notice to individuals in situations where they did not know of a breach but would have known if they exercised reasonable diligence.
- Employees of a covered entity are considered agents of the organization and any knowledge an employee has will be attributed to the covered entity (except where the employee is the person committing the breach).
- Because of this standard, covered entities need to have reasonable systems in place to discover breaches including training of staff on prompt reporting of any known breaches.

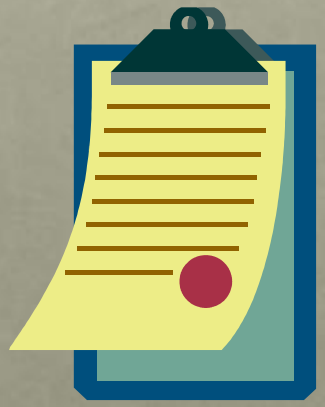
Timeliness of Notification

- Notice must be provided to the individual without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach.
- 60 days is an outer limit, if the covered entity has completed its risk assessment and confirmed the breach within 20 days, it should send the notifications immediately instead of waiting until day 60.

Content of Notification

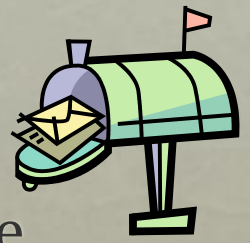
The notification must contain, to the extent possible:

- Description of what happened and dates, if known
- Description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- Description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, email address, website, or postal address



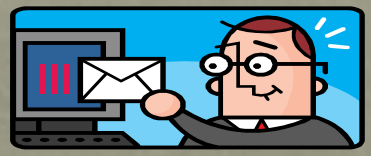
Methods of Notification to Individuals

- Written notice to last known address or by email if agreed to by the individual.



- If the individual is deceased, notification may be sent to the next of kin or personal representative of the individual if the CE knows the individual is deceased and has contact information for the next of kin or personal representative.

- Notification may be provided in one or more mailings as information becomes available.
- In urgent situations, notice may be provided by telephone or other means in addition to written notice.



Substitute Individual Notification

- Where there is insufficient or out of date contact information, a substitute form of individual notice reasonably calculated to reach the individual may be provided such as email or telephone
- If the individual is deceased and there is insufficient contact information, no substitute notification is required

Substitute Individual Notification for 10 or more persons

- If the covered entity does not have sufficient contact information for ten or more affected individuals, the following applies:
  1. Conspicuous posting for 90 days on home page of covered entity's website or posting in print or broadcast media where affected individuals may reside; **and**
  2. Include a toll-free number that remains active for at least 90 days where individuals can learn whether they were affected by the breach.

- The posting must include the same information as the written notice to individuals.

Notification to the Media

- For a breach involving more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets serving that state or jurisdiction in addition to written notice to individuals.
- Must be done without unreasonable delay, no later than 60 calendar days after discovery of breach.
- Content of the notification to media is the same as that which was given to individuals.

Examples of Notification to Media

- If a laptop that contains unsecured PHI of more than 500 residents of a particular city is stolen, the covered entity would need to notify a major television station or daily newspaper serving that city or entire state.
- If the stolen laptop contained the unsecured PHI of 200 residents from State A, 200 residents of State B, and 200 residents of State C, no reporting to the media would be required since there were not 500 or more residents affected from any one state. In this case, however, the covered entity would still be required to report the breach to the Secretary.

Notification to the Secretary

- If a breach involves 500 or more individuals, the covered entity must report the breach to the Secretary at the same time it notifies affected individuals.
- If a breach involves less than 500 individuals, the covered entity will make an annual reporting of all such breaches discovered in a calendar year to the Secretary (no later than 60 days after the end of each calendar year, providing notification for breaches discovered during the preceding calendar year).
- Reporting by covered entities will be done via OCR's website.
- This data is collected for reporting to Congress and notification to the Regions.

Business Associates

- Business associates must notify covered entities of breaches without unreasonable delay and in no case later than 60 days.
- Breaches are treated as discovered on the first day that the breach is known or by exercising reasonable diligence would have been known to the BA.
- The content of the notification from the BA to the CE must include, to the extent possible, the identification of the affected individuals and as much information that is known to the BA which the CE would be required to include in its notice to the individual.

Law Enforcement Delay

- If law enforcement makes a written statement to a covered entity or business associate that notification or posting of a breach would impede a criminal investigation, the covered entity must delay notification until the time specified by law enforcement.
- If the requested delay by law enforcement is oral, the covered entity must document the oral request and delay notification for no longer than 30 days from the date of the request.

HIPAA Breach Highlights

September 2009 through July 31, 2018

- Approximately 2,393 reports involving a breach of PHI affecting 500 or more individuals
  - **Theft and Loss** are **43%** of large breaches
  - **Laptops** and other **portable storage devices** account for **24%** of large breaches
  - **Paper** records are **21%** of large breaches
  - **Hacking/IT** account for 20**%** of incidents
  - Individuals affected are approximately 264,728,418
- Approximately 354,334 reports of breaches of PHI affecting fewer than 500 individuals

What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

Breach Resources:

- **Breach Notification Requirements** https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- **Breach Reporting**
- **OCR Breach Portal – Notice to the Secretary of HHS** https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
- Guidance to secure PHI
- OCR List of Breaches Affecting 500 or more

Enforcement

Enforcement Process

- https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html

- OCR reviews the information, or evidence, that it gathers in each case. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement.

Enforcement Process

- Letter of Opportunity with Resolution Agreement and Corrective Action Plan
- Notice of Proposed Determination
  - Entity may request a hearing before Administrative Law Judge
- Notice of Final Determination

Recent Enforcement Actions

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

21st Century Oncology

- PHI of over 2 million people illegally obtained by unauthorized third party
- Failure to conduct accurate and thorough assessment of potential risks and failure to implement risk management plan
- Failure to review records of information system activity
- Disclosures made to vendors without a BAA
- $2,300,000 Settlement with Corrective Action Plan

- **CardioNet**
  - Breach report - stolen laptop with unsecured PHI
  - Insufficient risk analysis and risk management plan in place
  - Failure to implement Security Rule policies and procedures
  - $2,500,000 Resolution Agreement and Corrective Action Plan

Recent Enforcement Actions

Metro Community Provider Network

- Breach report from Federally Qualified Health Center – hacker accessed employees' email accounts and obtained ePHI through phishing incident
- Failure to conduct risk analysis and corresponding risk management plan
- $400,000 Resolution Agreement with Corrective Action Plan

Memorial Health System

- Employees and users at affiliated physician offices impermissibly accessed ePHI
- Failure to implement procedures to review, modify, terminate users' right of access and failure to regularly review records of information system activity despite identifying risks
- $5,500,000 Resolution Agreement with Corrective Action Plan

General Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 Civil Monetary Penalties

Questions?

Karel Hadacek, J.D.
OCR Investigator
Karel.Hadacek@hhs.gov
303-844-7836

Thank You!