U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

HIPAA Training for Small Providers

Hyla Schreurs, J.D., Supervisory Equal Opportunity Specialist

Emily Prehm, J.D., Equal Opportunity Specialist

August 31, 2017

Overview

Office for Civil Rights (OCR)

Headquarters - Washington, DC

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

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

- Investigations
- Technical Assistance
- Outreach

Who We Are

As the Department's civil rights, conscience and religious freedom, and health 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.

Numbers at a Glance

- Over 158,293 complaints received to date
- Over 25,312 cases resolved with corrective action and/or technical assistance
- 49 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties
- Expect to receive 17,000 complaints this year

Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Health care clearinghouses
- Business Associates

§ 160.301

Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the covered entity, and such work requires the use or disclosure of protected health information ("PHI," see next slide).
- The Privacy Rule requires "satisfactory assurance," which usually takes the form of a contract, that a BA will safeguard the PHI, and limit its use and disclosure.

§ 160.301

Requirements for Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule; criminal and civil liabilities attach for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of a BA are now defined as a BA; clarifying that BA liability flows to all subcontractors

Scope: What is Covered?

- Protected Health Information ("PHI"):
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by Covered Entities or their Business Associates
- Not PHI:
  - De-identified information
  - Employment records
  - FERPA records

§ 160.301

Uses and Disclosures: Key Points

- No use or disclosure of PHI unless permitted or required by the Privacy Rule.
- *Required* Disclosures:
  - To the individual who is the subject of the PHI.
  - To the Secretary of HHS in order to determine compliance.
- All other uses and disclosures in the Privacy Rule are *permissive.*
- Covered Entities may provide greater protections.

§ 164.502

Permissive Uses and Disclosures

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- "Incident to"
- Limited data sets
- As authorized by the individual

§ 164.502

To Individuals

- Besides making required disclosures, Covered Entities may also disclose PHI to their patients or enrollees. For example:
  - Health plans may contact their enrollees.
  - Providers may contact or speak with their patients.
- Covered Entities must treat a personal representative -- person who has authority to make decisions related to health care -- as an individual

Treatment, Payment, Health Care Operations (TPO)

- What is “treatment?”
- What is “payment?”
- What are “health care operations?”
- Using and disclosing for TPO
- Using and disclosing for TPO of another Covered Entity

§ 164.502

Opportunity to Agree or Object

- To use PHI in facility directories (name, location, general condition, religious affiliation to clergy)
- To disclose PHI to persons involved in care or payment for care and for notification purposes. For example:
  - Friends may pick up prescriptions.
  - Hospitals may notify family members of a patient's condition.
  - Covered entities may notify disaster relief agencies.

§ 164.510

Public Priorities

- Covered Entities may use or disclose PHI without authorization only if the use or disclosure comes within one of the listed exceptions and follows its conditions. Some examples:
  - As required by law
  - For public health activities
  - For judicial and administrative proceedings
  - For specialized government functions

§ 164.512

Incidental Uses and Disclosures

- The Privacy Rule permits uses and disclosures incidental to an otherwise permitted use or disclosure, provided minimum necessary and safeguard standards (discussed following) are met.
  - Examples: talking to a patient in a semi-private room; talking to other providers if passers-by are present; waiting-room sign-in sheets; patient charts at bedside.
- Allows for common practices if reasonably performed

§ 164.502

Minimum Necessary Standard

- Covered entities must make reasonable efforts to use, disclose, or request the minimum necessary ("MN") PHI based on purpose.
- Exceptions to the MN standard: e.g., disclosure of PHI for the purpose of treatment
- Covered entities must identify classes of workforce members who need access to PHI to do their jobs.
- Covered entities must develop criteria to limit disclosures of and requests for PHI to the MN.

§ 164.502

Authorizations

- Covered Entities *must* obtain an individual's authorization before using or disclosing PHI for purposes other than:
  - TPO;
  - Where the opportunity to agree or object is required;
  - Specified public priorities.
- Authorizations *must* be obtained for marketing (with limited exceptions).

§ 164.508

Marketing

- Communications about health-related products and services by covered entity (or business associate) to individuals now marketing and require authorization if paid for by third party
- Applies to receipt of financial remuneration only; does not include receipt of non-financial benefits
- Authorization must state that communication is paid for
- Authorization can be obtained to make subsidized communications generally
  - Scope of authorization need not be limited to single product/service or products/services of one third party

Marketing

- Limited exception for refill reminders (and similar communications)
  - Includes generic equivalents, adherence communications, drug delivery systems
  - Payment must be reasonably related to cost of communication
- Face to face marketing communications and promotional gifts of nominal value still permitted without authorization

Sale of PHI

- Even where disclosure is permitted, covered entity is prohibited from disclosing PHI (without individual authorization) in exchange for remuneration
  - Includes remuneration received directly or indirectly from recipient
  - Not limited to financial remuneration
- If authorization obtained, authorization must state that disclosure will result in remuneration

Sale of PHI

- Exceptions:
  - Treatment & payment
  - Sale of business
  - Remuneration to BA for services rendered
  - Disclosure required by law
  - Providing access or accounting to individual
  - Public health
  - Research, if remuneration limited to cost to prepare and transmit PHI
  - Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI

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

Individual Rights

Individual Rights

- Notice of Privacy Practices
- Access: inspect and copy
- Amendment
- Accounting
- Alternative communications
- Request restriction
- Complaints to Covered Entity and Secretary

Amendment

- Amendment:

  An individual has the right to request that a CE amend PHI about the individual in a DRS as long as the DRS is maintained.

§ 164.526

Accounting

- Accounting:

  An individual has the right to receive an accounting of disclosures of PHI made by a CE in the six years or less prior to the request.

§ 164.528

Alternative Communication

- Alternative Communication

  A covered health care provider must permit the individual to request and must accommodate reasonable requests to receive communications of PHI by alternative means and at alternative locations. The requirement applies to health plans if the individual clearly states that the disclosure could endanger the individual.

§ 164.522(b)

Right to Request Restrictions

- A covered entity must permit an individual to request that the covered entity restrict uses and disclosures of PHI for treatment, payment, or health care operations purposes, and for disclosures to family and friends (opportunity to agree or object disclosures).

- Covered entities are not required to agree to the request (unless to a health plan under certain circumstances).

§ 164.522(a)

Right to Request Restrictions

- Covered entity must agree to individual's request to restrict disclosure of PHI to health plan if:
  - PHI pertains solely to health care for which individual (or person on behalf of individual other than health plan) has paid the covered entity in full out of pocket
  - Disclosure is not required by other law

§ 164.522(a)

Right to Request Restrictions

- Preamble provides guidance on scope of restriction & other issues
  - Scope of restriction to health plan extends to health care item or service paid for out of pocket
    - Restriction on follow-up care – individual must pay out of pocket and request restriction for follow-up care
    - Restriction on downstream providers – individual has obligation to request restriction from downstream providers but providers encouraged to assist individual in notifying downstream providers of individual's desire to restrict

Right to Request Restrictions

- Preamble provides guidance on scope of restriction & other issues
  - Can't require individual to restrict all or none of a provider's health care items or services; however, recognize issues with bundled items or services
  - If original form of payment dishonored, must make reasonable efforts to obtain payment prior to billing health plan
  - How to address other legal requirements

Notice of Privacy Practices

An individual has a right to adequate written notice of:

- uses and disclosures of PHI that may be made by the Covered Entity, and
- Individual's rights and Covered Entity's legal duties with respect to PHI

Notice Elements

- Header – specific language in Rule
- Description of uses and disclosures
- Individual rights and how to exercise those rights
- Covered Entity duties and contact name or title & telephone number to receive complaints
- Effective Date

Notice of Privacy Practices

- Content must include:
  - Statements regarding sale of PHI, marketing, and other purposes that require authorization
  - For covered entities engaging in fundraising, statement that individual can opt out of fundraising communications
  - For providers, statement that covered entity must agree to restrict disclosure to health plan if individual pays out of pocket in full for health care service
  - Statement about individual's right to receive breach notifications
  - For plans that underwrite, statement that genetic information may not be used for such purposes

Provision of Notice

- **By Direct Treatment Providers**
  - First service delivery after compliance date
  - Good faith effort to obtain a written acknowledgment of receipt
- **By Health Plans**
  - At compliance date and thereafter at enrollment to new enrollees
  - Every 3 years, must tell enrollees of availability of Notice and how to obtain
  - *Health plans may distribute materially revised NPPs*:
    - By posting on web site by effective date of change and including in next annual mailing to individuals; or
    - Mailing to individuals within 60 days of material revision
- **By All Covered Entities**
  - On request to **any person**

Complaints

- Covered Entity process for individuals to complain concerning Covered Entity's privacy policies or procedures
- No provisions on how Covered Entity's complaint process must operate other than to document complaints and their disposition
- Individuals may also complain to OCR

Access Guidance

- Issued in two phases in early 2016
  - Comprehensive Fact Sheet
  - Series of FAQs
    - Scope
    - Form and Format and Manner of Access
    - Timeliness
    - Fees
    - Directing Copy to a Third Party, and Certain Other Topics

Access Guidance

- Access – **Scope**
- Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  - Doesn't matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports and underlying information (including genomic information)

Access Guidance

- Access – **Scope** (cont.)
- Very limited exclusions and grounds for denial
  - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
  - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
  - No denial for failure to pay for health care services
  - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access

Access Guidance

- Access – **Requests for Access**
  - Covered entity may require written request
  - Can be electronic
  - Reasonable steps to verify identity
  - BUT cannot create barrier to or unreasonably delay access
    - E.g., cannot require individual to make separate trip to office to request access

Access Guidance

- Access – **Form and Format and Manner of Access**
- Individual has right to copy in form and format requested if "readily producible"
  - If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  - Depends on capabilities, not willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by e-mail (or mail), including unsecure e-mail if requested by individual (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity's systems

Access Guidance

- Access – **Timeliness and Fees**
  - Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner
  - Limited fees may be charged for copy
    - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
    - No search and retrieval or other costs, even if authorized by State law
    - Entities strongly encouraged to provide free copies
    - Must inform individual in advance of approximate fee

Access Guidance

Calculating Costs for Access Fees: 3 Acceptable Methods

1. **Actual costs**
   - Actual labor for copying (at reasonable rates, including only the time to create and send a copy in the form, format, and manner requested)
   - Actual postage
   - Supplies (paper, toner, CD, USB drive)
2. **Average costs**
   - Cost schedule based on average labor costs for standard requests is okay
   - Per page fee acceptable only for paper records (copied or scanned)
   - Applicable supply and postage costs may be added to average labor costs
3. **Flat fee for electronic copies of electronic PHI only ($6.50 cap).**
   - An alternative to calculating actual or average costs for certain requests
   - Not a cap on all permissible fees

Access Guidance

No Fees Permitted For:

- Providing access through certified EHR technology (*i.e.*, View, Download, Transmit)
- Administrative overhead costs for outsourcing access requests to a business associate
- Viewing and inspecting PHI only

Access: Designated 3rd Party

- **Third Party Access to an Individual's PHI**
  - Individual's right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR 164.524)
  - Individual may also authorize disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR 164.508)

Access Guidance

New video training module; once completed, you will receive CME or CE credit:

https://www.hhs.gov/hipaa/for-professionals/training/index.html

Access Guidance available on OCR's website at:

http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

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 E-PHI
- 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 ("E-PHI"):
  - Protected health information
  - Transmitted or maintained in electronic media
- Not E-PHI:
  - 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 either implement the specification, implement an equivalent alternative, or not implement the specification

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
  - 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

Compliance Challenges

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 C.F.R. § 164.308(b).* Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involves 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.

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 C.F.R. § 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**

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 C.F.R. § 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 Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- http://scap.nist.gov/hipaa/
- http://www.healthit.gov/providers-professionals/security-risk-assessment

Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. *See 45 C.F.R. § 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 C.F.R. § 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 C.F.R. § 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

No Patching of Software

- 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.)

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 C.F.R. § 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 C.F.R. § 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 C.F.R. § 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 C.F.R. § 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 C.F.R. § 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 C.F.R. § 164.308(a)(7)(ii)(D).*

Mobile Device Security

http://www.healthit.gov/mobiledevices

Security Rule Resources

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

- The Security Rule
- Security Rule History
- Security Rule Guidance and Notices
- NIST Toolkit
- FAQs

Cloud Guidance

- OCR released guidance clarifying that a 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.
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Cybersecurity Newsletters

February 2016	Ransomware, "Tech Support" Scam, New BBB Scam Tracker
March 2016	Keeping PHI safe, Malware and Medical Devices
April 2016	New Cyber Threats and Attacks on the Healthcare Sector
May 2016	Is Your Business Associate Prepared for a Security Incident
June 2016	What's in Your Third-Party Application Software
September 2016	Cyber Threat Information Sharing
October 2016	Mining More than Gold (FTP)
November 2016	What Type of Authentication is Right for you?
December 2016	Understanding DoS and DDoS Attacks
January 2017	Audit Controls
February 2017	Reporting and Monitoring Cyber Threats
April 2017	Man-in-the-Middle Attacks and "HTTPS Inspection Products"

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

Breach Notification Rule

Breach Notification Provisions

- 164.400 – applicability
- 164.402 – definitions
- 164.404 – notification to individuals
- 164.406 – notification to media
- 164.408 – notification to Secretary/OCR
- 164.410 – notification by business associates
- 164.412 – law enforcement delay
- 164.414 – administrative requirements and burden of proof

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 e-mail 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 e-mail. 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

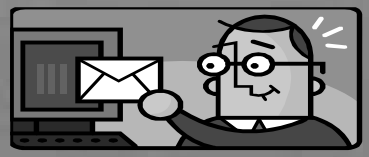
The notification must contain, to the extent possible:

- 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, e-mail address, website, or postal address

Methods of Notification to Individuals

- Written notice to last known address or by e-mail 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 e-mail 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.

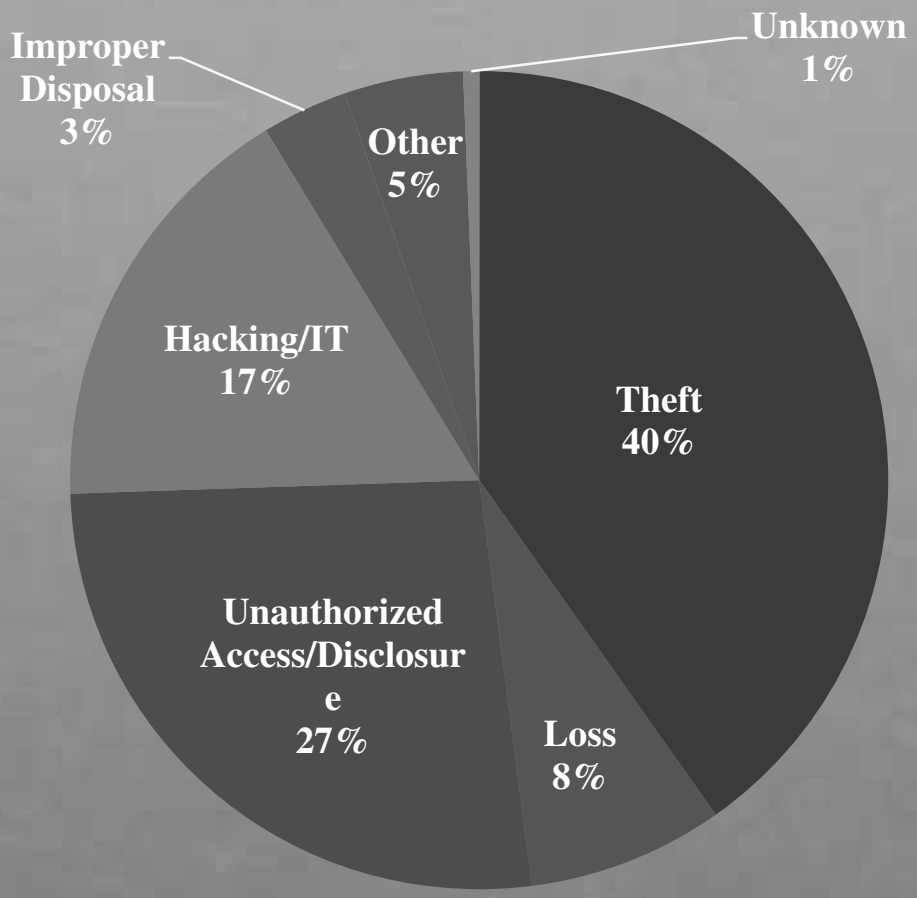
HIPAA Breach Highlights

September 2009 through July 31, 2017

- Approximately 2,017 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 48% of large breaches
  - Hacking/IT now account for 17% of incidents
  - Laptops and other portable storage devices account for 26% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 174,974,489
- Approximately 293,288 reports of breaches of PHI affecting fewer than 500 individuals

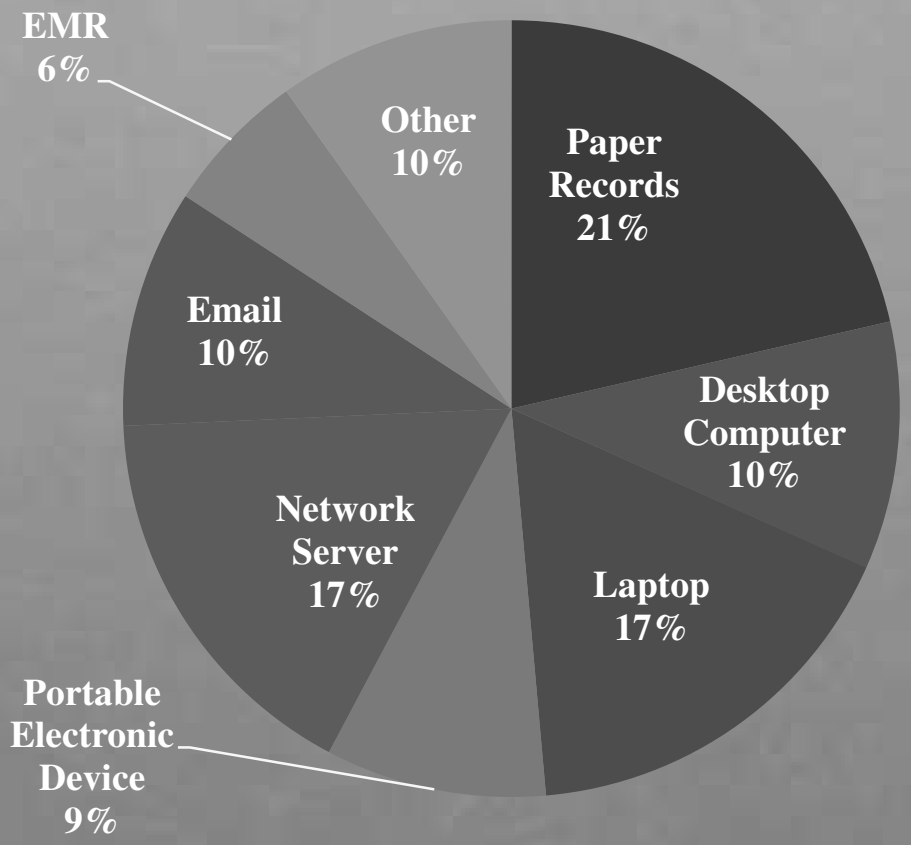
HIPAA Breach Highlights

500+ Breaches by Type of Breach as of July 31, 2017



HIPAA Breach Highlights

500+ Breaches by Location of Breach as of July 31, 2017



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 Notification

- Breach reporting - https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

Enforcement

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

- The violation did not occur after April 14, 2003
- Entity is not covered by the Privacy Rule
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate the Privacy Rule

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

Children's Medical Center of Dallas

- Multiple lost or stolen mobile devices with unsecured ePHI
- Failure to timely implement appropriate risk management
- $3,200,000 Civil Money Penalty

MAPFRE Life Insurance Company of Puerto Rico

- Stolen USB storage device containing the ePHI of 2,209
- Lack of appropriate risk analysis and management, including lack of encryption
- $2,200,000 Settlement with Corrective Action Plan

Recent Enforcement Actions

The New York and Presbyterian Hospital

- Patients complained of impermissible disclosure of PHI to ABC film crew
- Did not obtain patient authorization
- $2,200,000 Resolution Agreement/Corrective Action Plan

University of Missouri Medical Center

- Breach report - stolen laptop with unsecured PHI
- Use of generic username and password on network drive
- Identified risks to PHI as early as 2005 but did not significantly manage
- $2,750,000 Resolution Agreement and Corrective Action Plan
  - Conduct risk analysis and develop risk management plan
  - Implement unique user identification
  - Update policies and procedures

Recent Enforcement Actions

Advocate Health Care

- 3 breach reports
  - Lost/stolen computers with unsecured PHI of approx. 4 million
  - Unauthorized third party access to BA's network
  - $5,550,000 Resolution Agreement with Corrective Action Plan
    - Modify existing risk analysis
    - Develop and implement risk management plan
    - Process for evaluating environmental and operational changes
    - Revise policies and training

Oregon Health & Science Center

- Breach reports – 2 stolen laptops and unencrypted thumb drive
- Storage of ePHI on cloud server without a business associate agreement
- $2,700,000 Resolution Agreement with Corrective Action Plan
  - Conduct risk analysis and risk management
  - Encryption program
  - Revise policies and staff training

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
  - 47 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

As of April 30, 2017

Corrective Action

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

Good Practices

Some Good 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

Questions?

Hyla Schreurs, J.D., Supervisory Equal Opportunity Specialist
hyla.schreurs@hhs.gov
303-844-7508

Emily Prehm, J.D., Equal Opportunity Specialist
emily.prehm@hhs.gov
303-844-7893

U.S. Department of Health and Human Services
Office for Civil Rights
1961 Stout Street, Room 08-148
Denver, CO 80294