Update on Administration and Enforcement of the HIPAA Privacy, Security, and Breach Notification Rules

Erin Walker, JD
Anne-Sophie Whitaker, JD

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

OCR Overview & Updates

- Overview of the Privacy Rule, Security Rule and Breach Notification
- Policy Development & Guidance Materials
- Enforcement Highlights

What is the Office for Civil Rights (OCR)?

- Part of the U.S. Department of Health and Human Services
- Enforces a number of civil rights laws as they relate to recipients of Federal financial assistance (FFA) from HHS, public entities, and programs & activities conducted by HHS
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules
- Headquartered in D.C. with 8 regional offices (in 11 locations) across the U.S.

Enforcement and Compliance Activities

- Complaint Investigations
- Compliance Reviews
- Voluntary Resolution Agreements ($)
- Formal Enforcement
- Audits
- Outreach and Public Education
- Policy Development

Complaint Process

- Any person or organization may file a complaint with OCR by mail or electronically
  - Complaints should be filed within 180 days of when the complainant knew or should have known that the act or omission occurred
- Informal review may resolve issue fully without formal investigation
- If not, begin investigation
  - Voluntary resolution may be possible through:
    - Education
    - Training
- Technical Assistance
- Some cases may require formal enforcement

Major Laws Enforced by OCR

- Title VI of the Civil Rights Act of 1964
- Section 504 of the Rehabilitation Act of 1973
- Title II of the Americans with Disabilities Act of 1990
- The Age Discrimination Act of 1975
- Section 1557 of the Affordable Care Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA Privacy, Security, and Breach Notification Rules)

OVERVIEW OF THE HIPAA RULES

Scope: Who is Covered?

- Limited by HIPAA to:
  - "Covered Entities" (CEs):
    - 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

Business Associates (BA)

- Agents, contractors, and others hired to do the work of, or to work for, the CE, and such work requires the use or disclosure of protected health information (PHI).
  - A BA expressly includes Health Information Organizations and E-prescribing Gateways.
  - Subcontractors of a BA are also defined as a BA.
  - BAs are directly liable for certain violations of the Privacy, Security, and Breach Notification Rules.
- The Privacy Rule requires "satisfactory assurance," in the form of a contract (or Business Associate Agreement), that a BA will safeguard the PHI, and limit its use and disclosure.

§160.103

Business Associate Liability

- Direct liability
  - Impermissible uses and disclosures (including more than minimum necessary)
  - Failure to comply with Security Rule
  - Failure to provide breach notification
  - Failure to provide e-access as provided in BA contract
  - Failure to disclose PHI to HHS for compliance and enforcement
- Contractual liability for requirements of the BA contract

PRIVACY RULE

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 (per Safe Harbor or expert method)
  - Employment records
  - FERPA records

Permissive Uses and Disclosures

- For treatment, payment, and health care operations (TPO)
- With the individual's opportunity to agree or object
- For specific public priorities (e.g., public health or where required by law)
- "Incident to" a permitted use or disclosure
- Limited data sets
- As authorized by the individual

§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

- If a disclosure is not otherwise permitted or required by the Privacy Rule, an individual's written authorization is required
- Authorizations must include certain elements to be valid:
  - Description of PHI to be released
  - Who will disclose the PHI
  - Who will receive the PHI
  - Purpose of the disclosure
  - Expiration date or expiration event
  - Required statements (revocation, no conditioning, potential for re-disclosure)

§164.508

Administrative Requirements

- Covered Entities must:
  - Designate a Privacy/Security Officer;
  - Provide an internal complaint process for individuals;
  - Provide privacy training to all workforce members;
  - Develop and apply sanctions policy;
  - Implement policies and procedures designed to comply with standards;
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable;
  - Refrain from intimidating and retaliatory acts;
  - Not require individuals to waive their rights.

Disclosures to the Media

- Disclosures to media allowed:
  - As permitted or required by the Privacy Rule
  - With prior written authorization
- Limited circumstances are disclosures permissible without authorization:
  - Help identify or locate family of an unidentified and incapacitated patient
  - Facility directory
- Safeguards

Access Provision

- Guidance issued in 2016
    - Form and Format and Manner of Access; Timeliness; Fees; Directing Copy to a Third Party, and Certain Other Topics
- Individual or Personal Rep has the right to access designated record set directed to another designated person or entity
- Designated record set:
  - Medical information
  - Billing records
- CE to respond within 30/60 days
- In form or manner requested
- Reasonable cost-based fee

OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions:
  - New tab for mental health in “FAQs for Professionals”
  - 9 new FAQs added (as PDF and in database)
- New Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

SECURITY RULE

Security Rule Standards

- 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?

- Applies to Electronic Protected Health Information (e-PHI) that a Covered Entity or a Business Associate:
    - Creates
    - Receives
    - Maintains
    - Transmits
- Electronic vs. Oral and Paper PHI
    - Privacy Rule applies to all forms of PHI
    - Security Rule applies only to e-PHI

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

Security Rule Standards

- Six Standards:
  - 164.306: Security Standards: General Rules
  - 164.308: Administrative Safeguards
  - 164.310: Physical Safeguards
  - 164.312: Technical Safeguards
  - 164.314: Organizational Requirements
  - 164.316: Policies and Procedures and Documentation Requirements

Cloud Computing 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

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]

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

Cybersecurity Newsletters

- Began in January 2016
- Recent 2018 Newsletters
  - April 2018: Risk Analyses vs. Gap Analyses
  - May 2018: Workstation Security
  - June 2018: Software Vulnerabilities and Patching
  - July 2018: Guidance on Disposing of Electronic Devices and Media
  - August 2018: Considerations for Securing Electronic Media and Devices
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Ransomware Guidance

- OCR 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

BREACH NOTIFICATION RULE

Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted

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 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

Definition of Breach – New Rule

- Harm standard removed
- Now, Impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate a low probability that the PHI has been compromised based on a risk assessment

Breach Risk Assessment

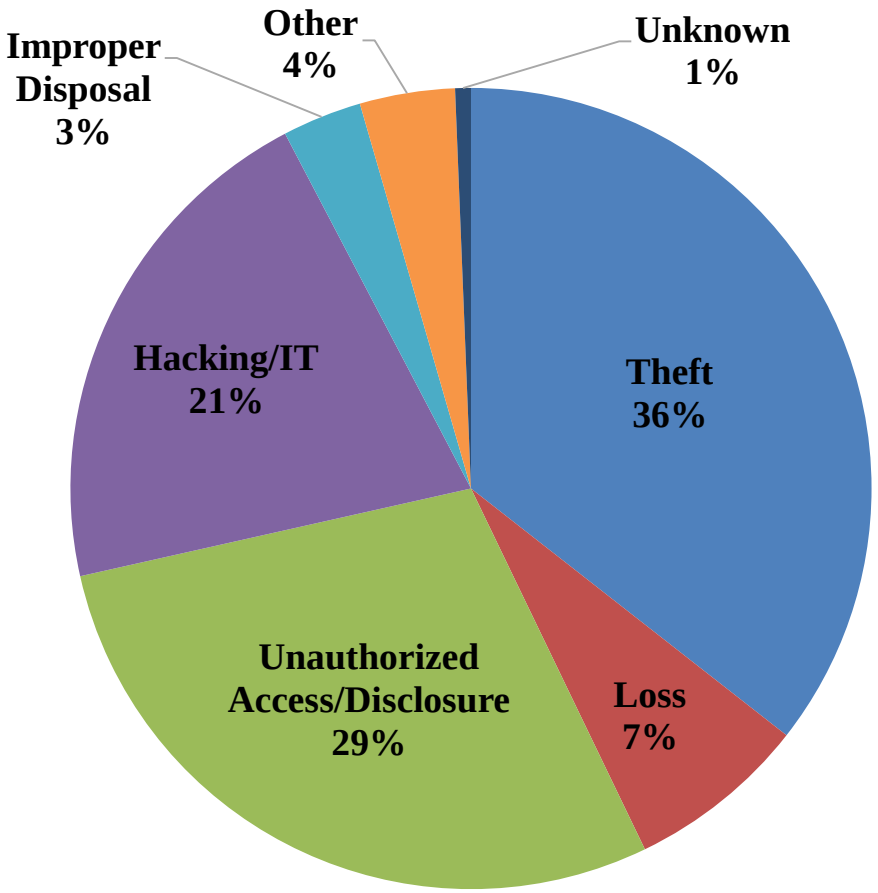
- Risk assessment based on the following:
  - Nature & extent of PHI involved
  - Who received/accessed the information
  - Potential that PHI was actually acquired or viewed
  - Extent to which risk to the data has been mitigated
- Exceptions for inadvertent, harmless mistakes remain

September 23, 2009 through August 31, 2018

- Approximately 2,421 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 43% of large breaches
  - Hacking/IT now account for 21% of incidents
  - Laptops and other portable storage devices account for 24% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 265,911,813
- Approximately 357,320 reports of breaches of PHI affecting fewer than 500 individuals

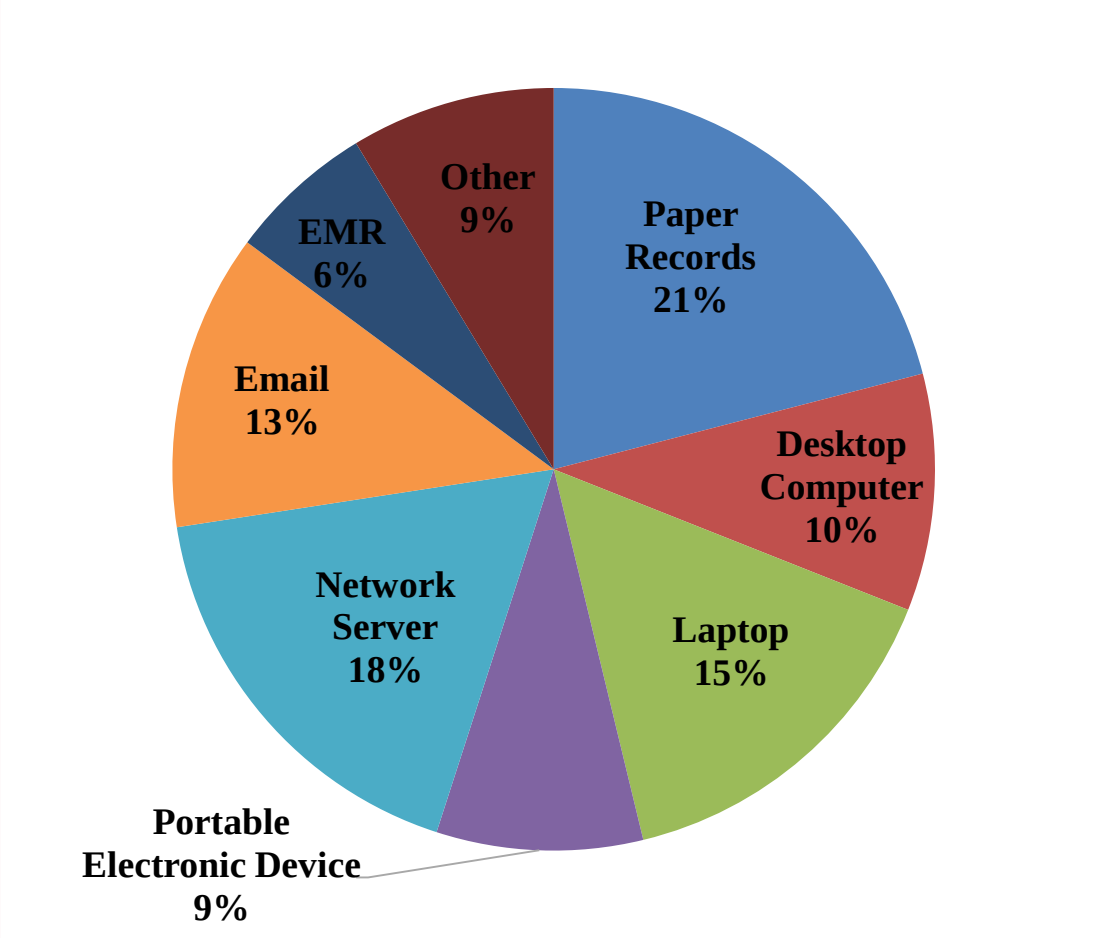
500+ Breaches by Type of Breach

September 23, 2009 – August 31, 2018



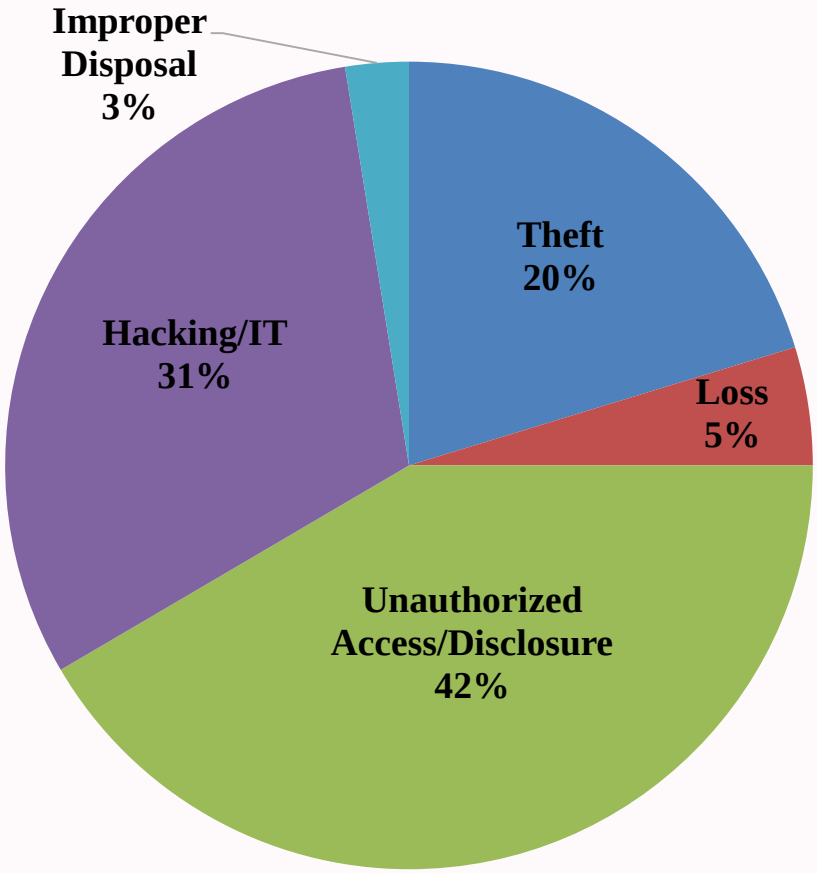
500+ Breaches by Location of Breach

September 23, 2009 – August 31, 2018



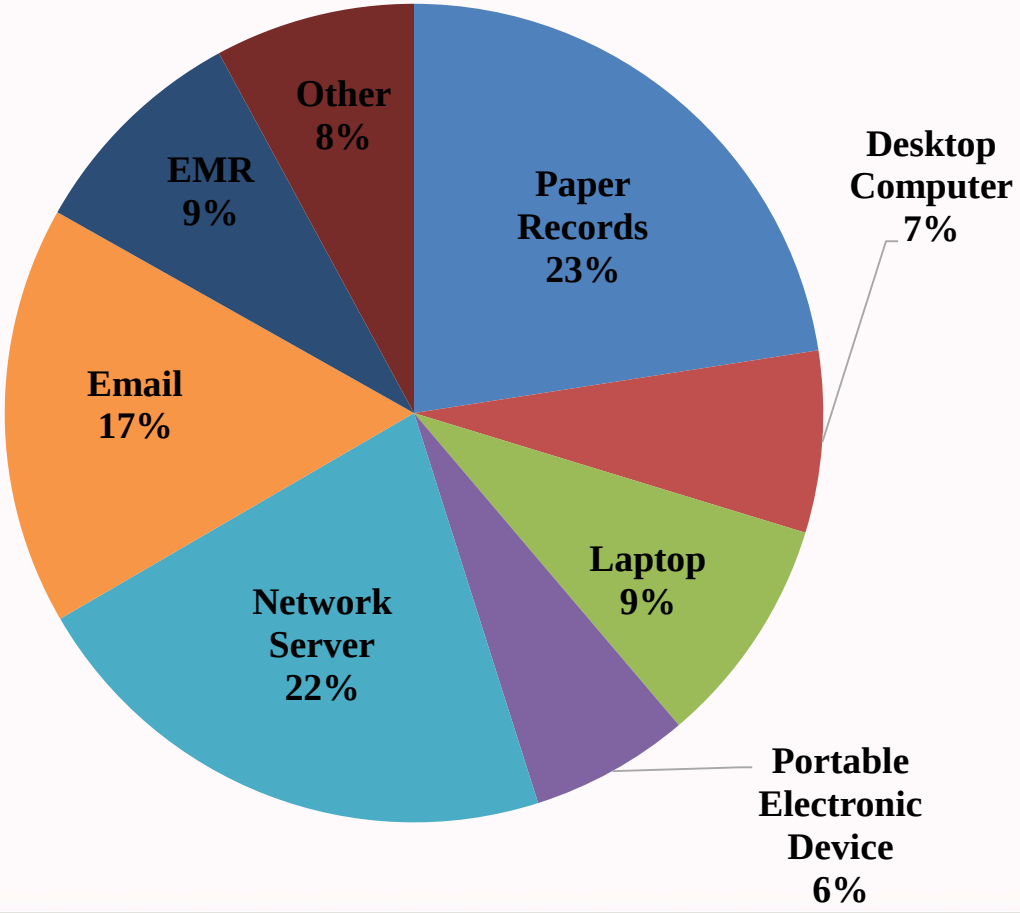
500+ Breaches by Type of Breach

9/1/2015 – 8/31/2018



500+ Breaches by Location of Breach

9/1/2015 – 8/31/2018



RECENT ENFORCEMENT ACTIVITY

General HIPAA Enforcement Highlights as of April 14, 2003 – August 31, 2018

- Over 188,562 complaints received to date
- Over 26,218 cases resolved with corrective action and/or technical assistance
- Expect to receive 24,000 complaints this year

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

As of August 31, 2018

Recent Enforcement Actions

4/12/2017	Metro Community Provider Network	$400,000
4/21/2017	Center for Children's Digestive Health	$31,000
4/21/2017	CardioNet	$2,500,000
5/10/2017	Memorial Hermann Health System	$2,400,000
5/23/2017	St. Luke's-Roosevelt Hospital Center	$387,200
12/28/2017	21st Century Oncology	$2,300,000
2/1/2018	Fresenius Medical Care North America	$3,500,000
2/13/2018	Filefax	$100,000

Total $11,618,200

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

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

Some 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

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr