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

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

Updated through February 28, 2018

Updates

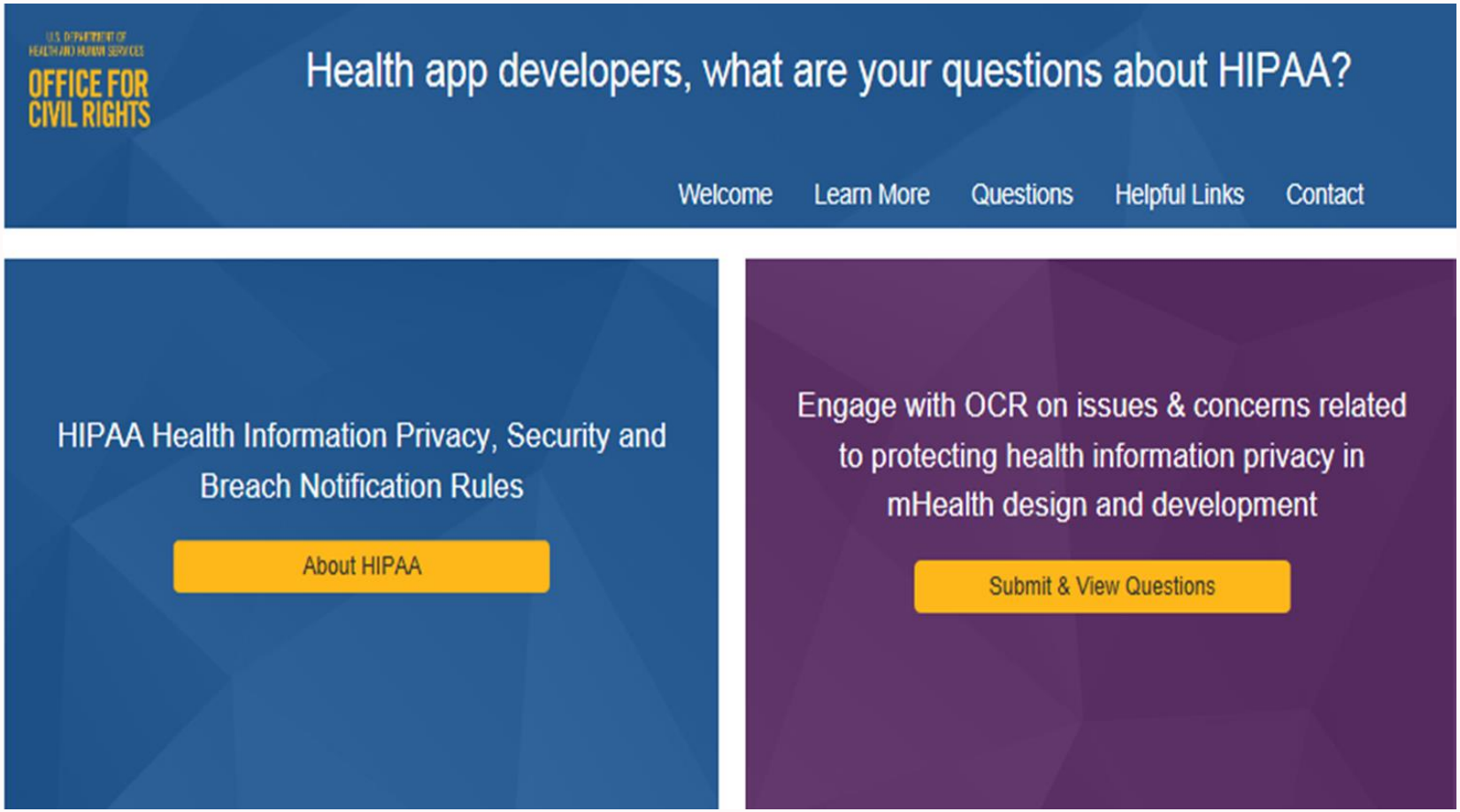
- Policy Development
- Breach Notification
- Enforcement
- Audit

POLICY DEVELOPMENT

HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; purpose is to understand concerns of developers new to health care industry and HIPAA standards
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov/



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 2017-2018 Newsletters
  - October 2017 (Mobile Devices and PHI)
  - November 2017 (Insider Threats and Termination Procedures)
  - December 2017 (Cybersecurity While on Holiday)
  - January 2018 (Cyber Extortion)
  - February 2018 (Phishing)
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/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

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

Breach Notification Requirements

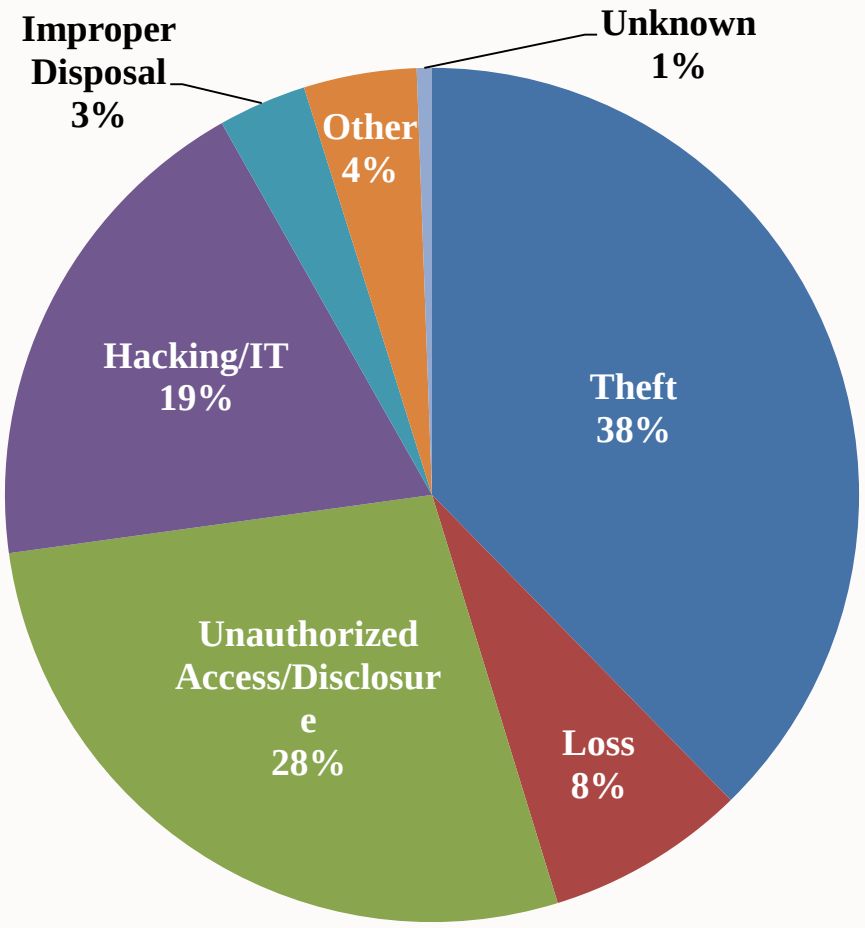
- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS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

September 2009 through February 28, 2018

- Approximately 2,222 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 46% of large breaches
  - Hacking/IT now account for 19% of incidents
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 177,298,024
- Approximately 341,002 reports of breaches of PHI affecting fewer than 500 individuals

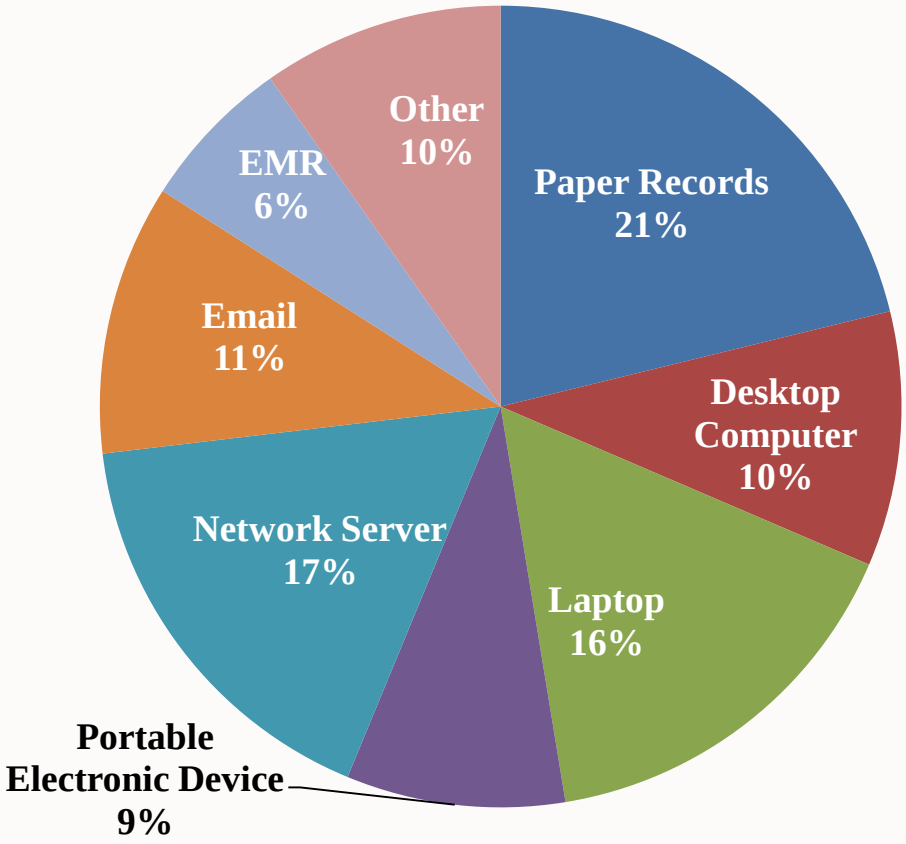
500+ Breaches by Type of Breach

April 14, 2003 – February 28, 2018



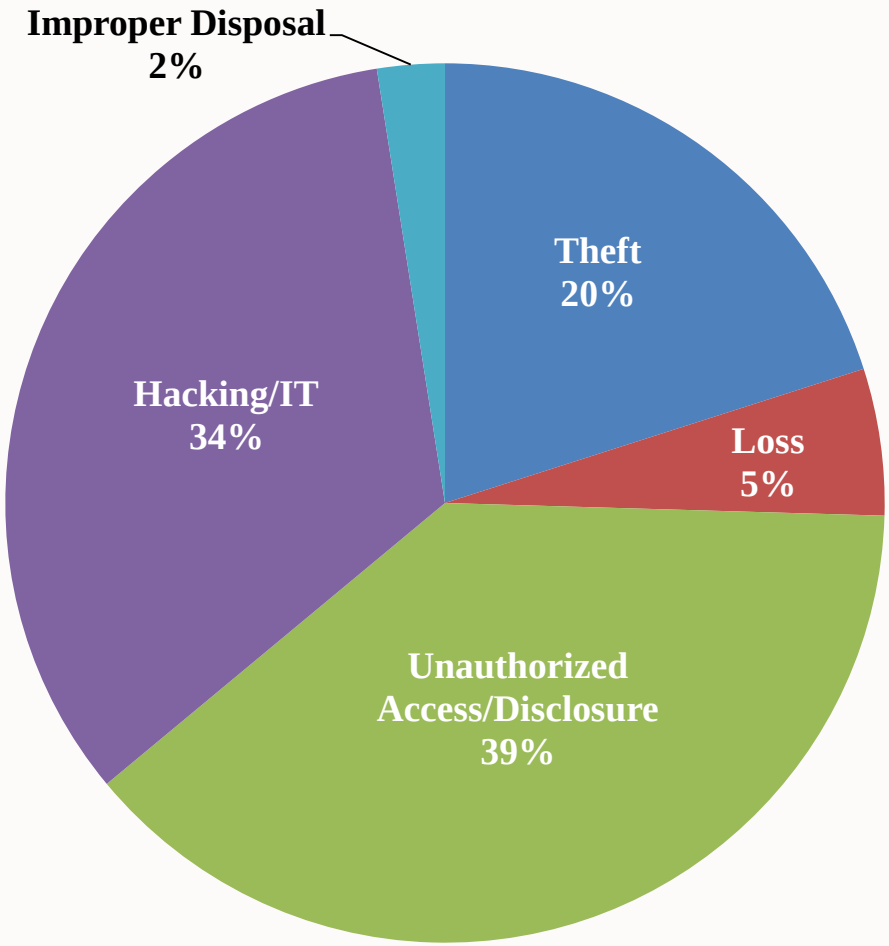
500+ Breaches by Location of Breach

April 14, 2003 – February 28, 2018



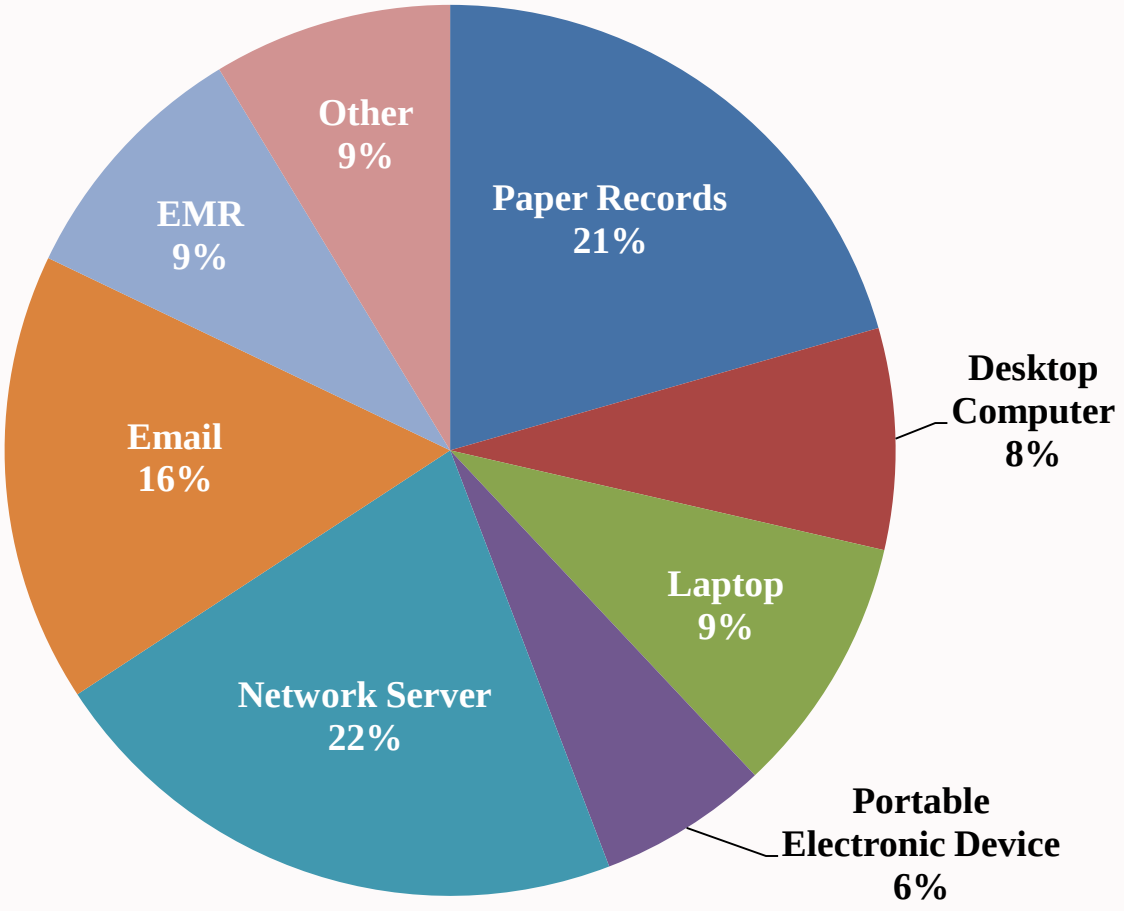
500+ Breaches by Type of Breach

3/1/2015 – 2/28/2018



500+ Breaches by Location of Breach

3/1/2015 – 2/28/2018



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

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

- Over 175,534 complaints received to date
- Over 25,742 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
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

As of February 28, 2018

Recent Enforcement Actions

2017 - 2018

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

AUDIT

HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open a compliance review (for example, if significant concerns are raised during an audit)
  - Learn from Phase 2 in structuring permanent audit program

History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)
- Pilot phase (2011-2012) – comprehensive, on-site audits of 115 covered entities
- Evaluation of Pilot (2013) – issuance of formal evaluation report of pilot audit program
- Phase 2 (2016-2017) - desk audits of 207 covered entities and business associates

Phase 2 - Selected Desk Audit Provisions

- For Covered Entities:
  - Security Rule: risk analysis and risk management;
  - Breach Notification Rule: content and timeliness of notifications; **or**
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management **and**
  - Breach Notification Rule: reporting to covered entity
- See auditee protocol guidance for more details: http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- After Phase 2, more comprehensive on-site audits will be conducted as a part of the permanent audit program
  - On-site audits will evaluate auditees against a comprehensive selection of controls in the audit protocol: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/
- Website updates with summary findings will be published summer 2018

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr