United States Department of Health & Human Services

Office for Civil Rights

Updates in Privacy, Security, and Breach Enforcement

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

Danielle Archuleta, Supervisory Equal Opportunity Specialist
Nikki Levy, Equal Opportunity Specialist (Contractor)
June 7, 2019

United States Department of Health & Human Services

Office for Civil Rights

Updates

- Breach Notification
- Enforcement
- Audit

United States Department of Health & Human Services

Office for Civil Rights

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

3

United States Department of Health & Human Services

Office for Civil Rights

Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media
- Business associate must notify covered entity of a 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

4

United States Department of Health & Human Services

Office for Civil Rights

What Happens When HHS/OCR Receives a Breach Report

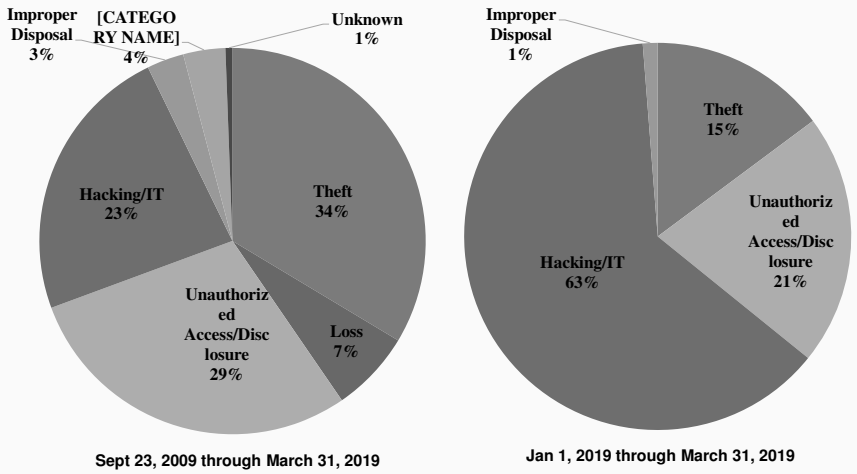
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Receive over 350 breach reports affecting 500 individuals or more per year
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity's compliance prior to breach

5

United States Department of Health & Human Services

Office for Civil Rights

500+ Breaches by Type of Breach



Sept 23, 2009 through March 31, 2019

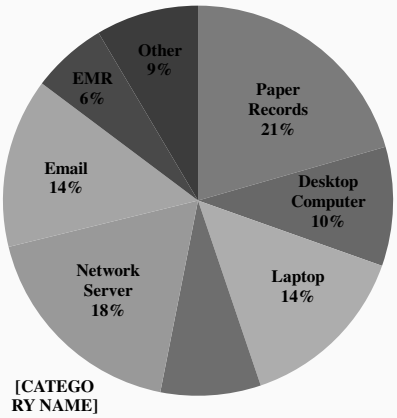
Jan 1, 2019 through March 31, 2019

6

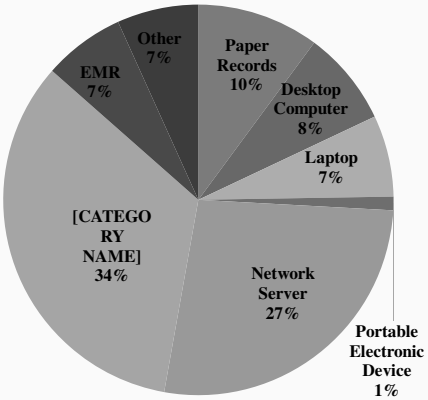
United States Department of Health & Human Services

Office for Civil Rights

500+ Breaches by Location of Breach



Sept 23, 2009 through March 31, 2019

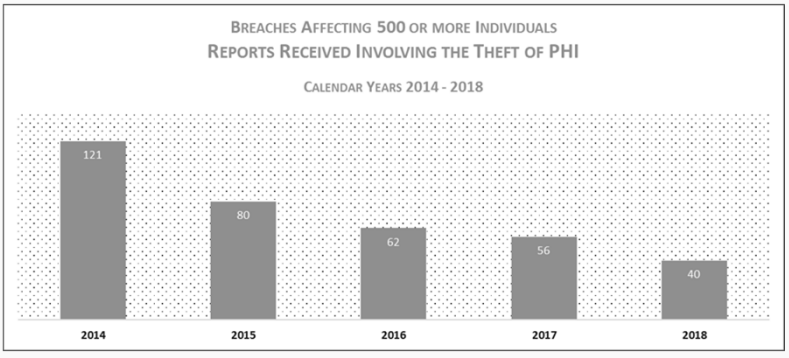


Jan 1, 2019 through March 31, 2019

7

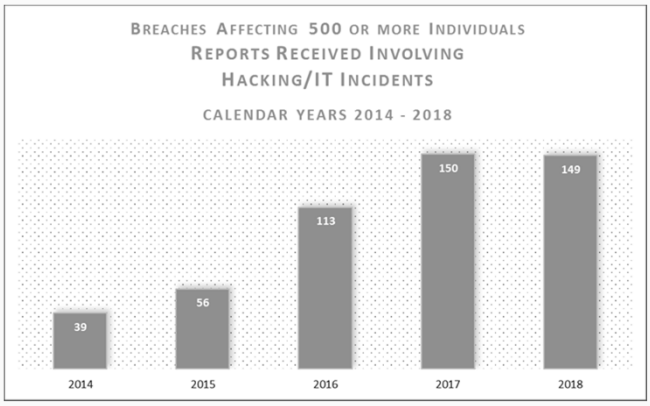
United States Department of Health & Human Services

Office for Civil Rights



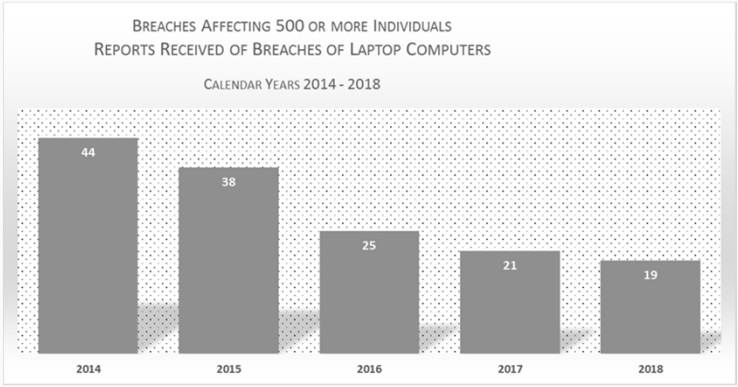
United States Department of
Health & Human Services

Office for Civil Rights



United States Department of
Health & Human Services

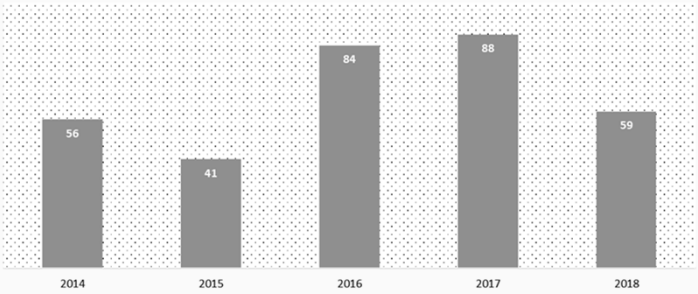
Office for Civil Rights



United States Department of
Health & Human Services

Office for Civil Rights

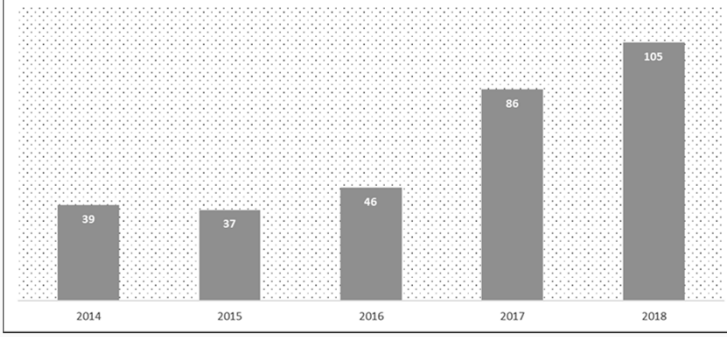
BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES OF NETWORK SERVERS
CALENDARS YEARS 2014 - 2018



United States Department of
Health & Human Services

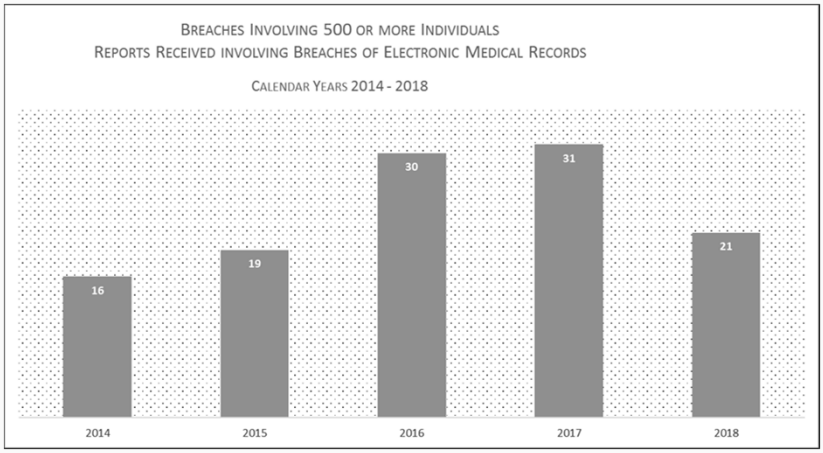
Office for Civil Rights

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES INVOLVING EMAIL ACCOUNTS
CALENDAR YEARS 2014 - 2018



United States Department of Health & Human Services

Office for Civil Rights



United States Department of Health & Human Services

Office for Civil Rights

General HIPAA Enforcement Highlights

- Expect to receive over 26,000 complaints this year
- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 60 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

As of March 31, 2019

United States Department of Health & Human Services

Office for Civil Rights

2018 Enforcement Actions

2/2018	Fresenius Medical Care North America	$3,500,000
2/2018	Filefax	$100,000
6/2018	University of Texas MD Anderson Cancer Center (CMP)	$4,348,000
9/2018	Boston Medical Center	$100,000
9/2018	Brigham and Women's Hospital	$384,000
9/2018	Massachusetts General Hospital	$515,000
10/2018	Anthem	$16,000,000
11/2018	Allergy Associates of Hartford	$125,000
12/2018	Advanced Care Hospitalists	$500,000
12/2018	Pagosa Springs Medical Center	$111,400
12/2018	Cottage Health	$3,000,000

Total $28,683,400

United States Department of Health & Human Services

Office for Civil Rights

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
- Individual Right to Access

Issue: 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 held by the [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

Case Example: Anthem, Inc.

- Largest U.S. PHI breach in history.
  - 78.8 million individuals affected
- Failure to conduct an enterprise-wide risk analysis
- Inadequate safeguards to prevent and address spear phishing attacks
- Settlement with RA/CAP, $16,000,000

Issue: Lack of Business Associate Agreements

- HIPAA generally requires that covered entities and business associates enter into agreements with their business associates (BAAs) to ensure that the business associates will appropriately safeguard protected health information.
- See 45 CFR §§ 164.502(e), 164.504(e), and 164.308(b).

Case Example: Advanced Care Hospitalists

- Filed a breach report confirming that patient information was viewable on a medical billing services' website
- Never had a BAA with the individual providing medical billing services
- No policy requiring business associate agreements until April 2014; in operation since 2005
- Settlement with RA/CAP, $500,000

Issue: Impermissible Disclosures

- A covered entity, including a health care provider, may not use or disclose protected health information (PHI), except either:

  (1) as the HIPAA Privacy Rule permits or requires; or

  (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

Case Example: Allergy Associates of Hartford, P.C.

- A patient contacted a local television station to speak about a dispute that had occurred between the patient and a doctor at Allergy Associates. The reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's protected health information to the reporter.
- OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights.
  - The disclosure occurred after the doctor was instructed by Allergy Associates' Privacy Officer to either not respond to the media or respond with "no comment."
- Settlement with RA/CAP, $125,000

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- CAPs may include third party or outside 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

Some Best Practices:

- 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

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; and
  - 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

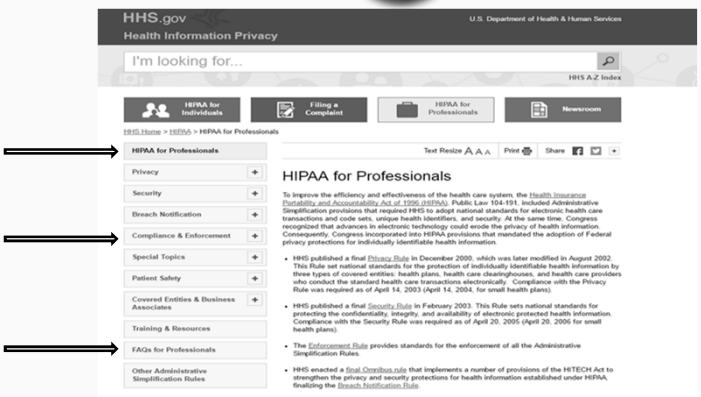
Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- Website updates with summary findings will be published in 2019

United States Department of Health & Human Services

Office for Civil Rights

More Information



http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr

31