HIPAA Compliance and Enforcement Update

Serena Mosley-Day

Senior Advisor
HIPAA Compliance and Enforcement
HHS Office for Civil Rights

March 8, 2019

What is OCR?

- Part of the Office of the Secretary, Department of Health and Human Services.
- Headquartered in D.C. with 8 regional offices (in 11 locations) across the U.S.
- 3 Divisions – Civil Rights, Conscience and Religious Freedom and Health Information Privacy
- The Health Information Privacy Division enforces the HIPAA Privacy, Security, and Breach Notification Rules through the issuance of regulations and technical assistance, as well as outreach to the regulated community and to the public to increase individuals' awareness of their HIPAA rights and protections.

UPDATE ON OCR POLICY ACTIVITIES

Current HIPAA Policy Initiatives

- OCR HIPAA Request for Information (RFI) on Modifying HIPAA Rules To Improve Coordinated Care
  - Care coordination and case management
  - Opioid crisis and parental involvement in care
  - Accounting of Disclosures
  - Notice of Privacy Practices
- Comments closed February 12, 2019
- Public comments are viewable at https://www.regulations.gov/docket?D=HHS-OCR-2018-0028

OCR Responds to the Opioid Crisis

Opioid crisis and national health emergencies have heightened concerns about providers':

- ability to notify patients' family and friends when a patient has overdosed
- reluctance to share health information with patients' families in an emergency or crisis situation, particularly when patients have serious mental illness and/or substance use disorder
- uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self or others

OCR guidance gives providers increased confidence in their ability to share information

Compassionate Communication

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:
  - Tab for mental health in "FAQs for Professionals"
  - 9 FAQs added (as PDF and in database)
- Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

Where to Find OCR's Materials

- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders
- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders
- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for-professionals/faq/mental-health

HIPAA Right of 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

Audit Update

HITECH Audit Program

Purpose:

Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance

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

Audit Program

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

Audit Program

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
- Permanent audit program model

HIPAA Breach Notification Highlights

Breach Notification Requirements

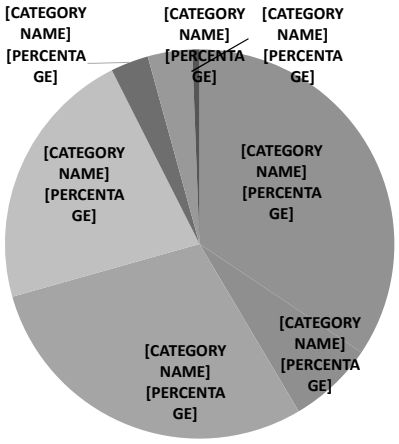
- Covered entity must notify affected individuals, HHS, and in some cases, the media
- Business associate must notify covered entity of a breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller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

Breach Portal:
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

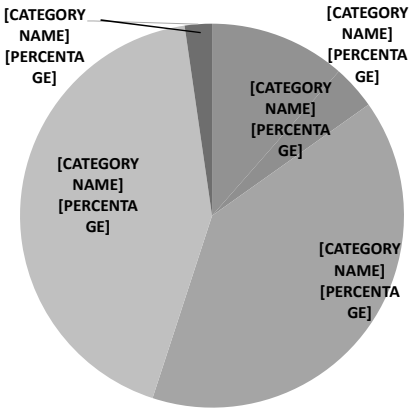
Breach Reporting – What Should be Reported?

- "Acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."
- Presumption of breach unless a covered entity or business associate can demonstrate a low probability that PHI has been compromised based on at least the following factors:
  - Nature and extent of PHI
  - The person who used or received the PHI
  - Whether PHI was actually viewed or acquired
  - Extent risk has been mitigated
- Breach risk assessment
  - Must be documented

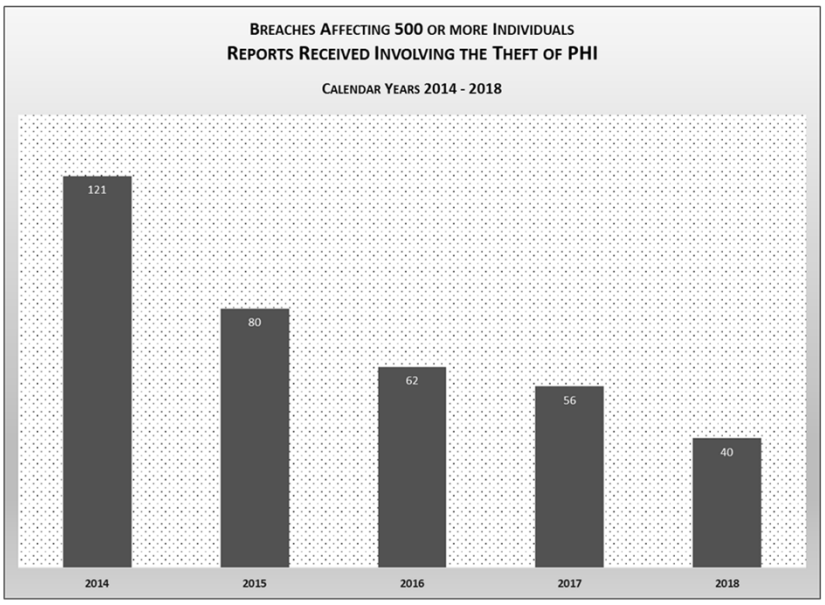
500+ Breaches by Type

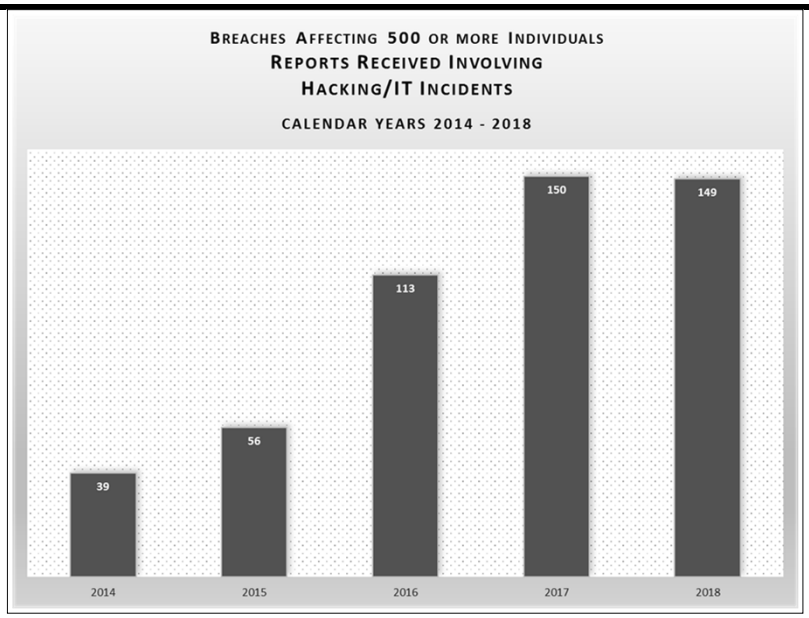


September 23, 2009 through December 31, 2018

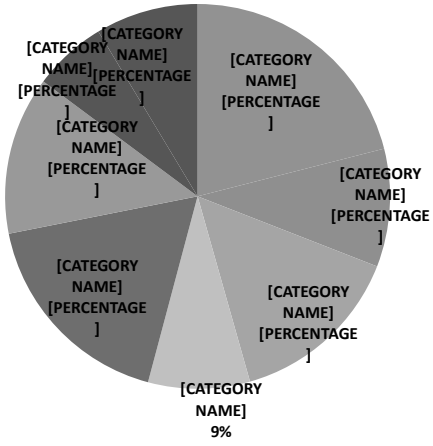


January 1, 2018 through December 31, 2018

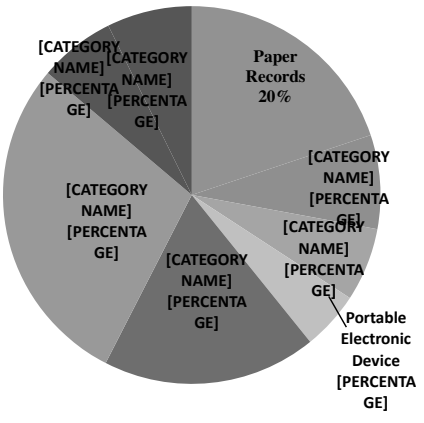




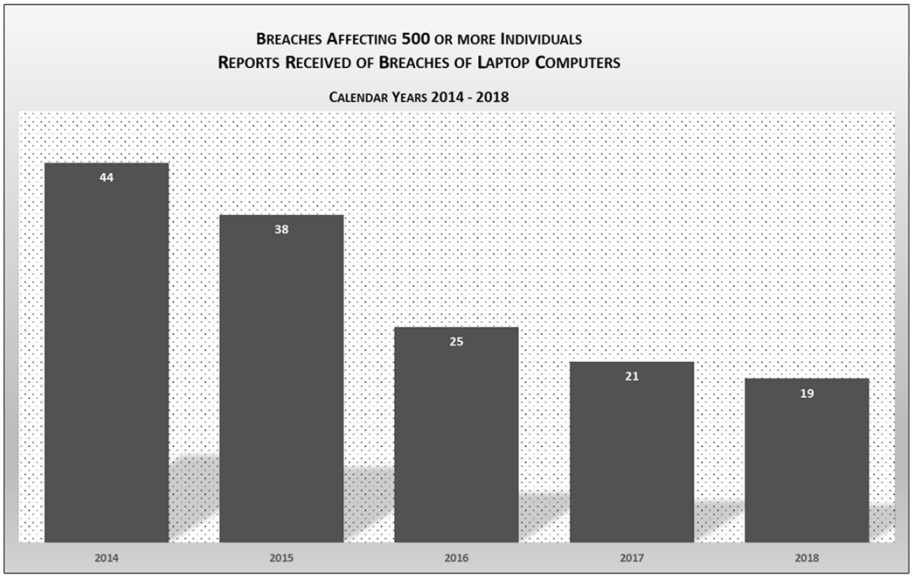
500+ Breaches by Location

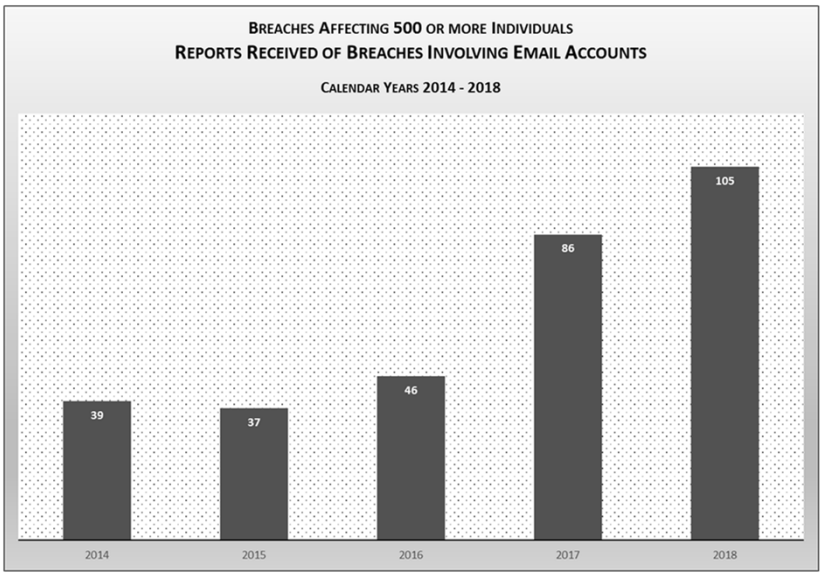


September 23, 2009 through December 31, 2018



January 1, 2018 through December 31, 2018


BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES OF LAPTOP COMPUTERS
CALENDAR YEARS 2014 - 2018
44
38
25
21
19
2014
2015
2016
2017
2018

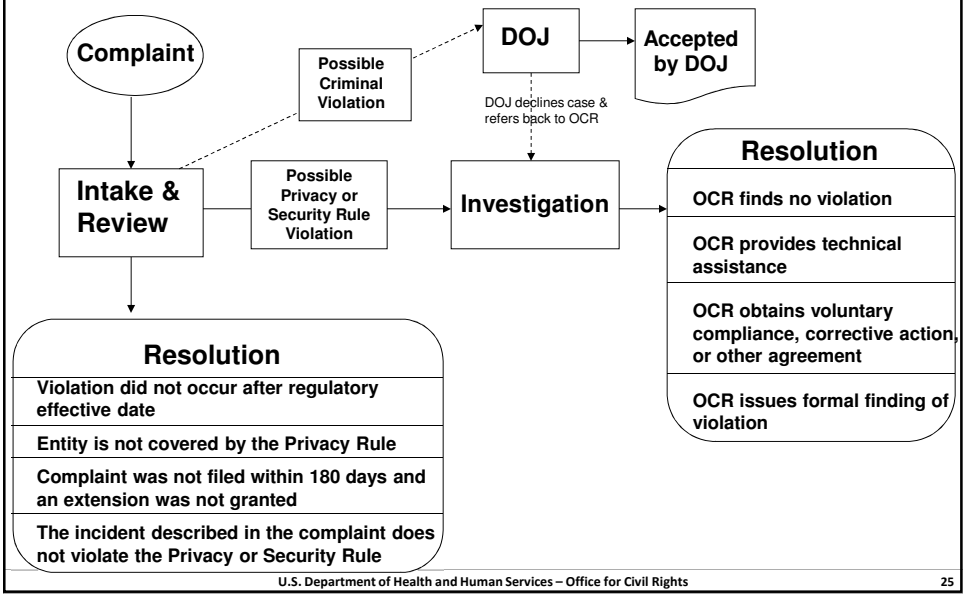

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES INVOLVING EMAIL ACCOUNTS
CALENDAR YEARS 2014 - 2018
39
37
46
86
105
2014
2015
2016
2017
2018

Breach Reports

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
    - 340 total 500 + breach reports 2016
    - 360 total 500 + breach reports 2017
    - 376 total 500 + breach reports 2018
- 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

UPDATE ON OCR COMPLIANCE AND ENFORCEMENT ACTIVITIES

HIPAA Complaint Process



General Enforcement Highlights

- Expect to receive over 26,000 complaints this year
- Receive over 350 500+ breach reports per 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 January 31, 2019

Enforcement and Compliance Activities

- Complaint Investigations
- Compliance Reviews
  - Including all 500+ breach reports
- Letters of Finding
- Settlement Agreements
- Formal Enforcement
- Outreach and Public Education
- Audits

2018 Enforcement Actions

2/2018	Fresenius Medical Care North America	$3,500,000
2/2018	Filefax	$100,000
6/2018	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

2018 Enforcement Actions and Settlements

- **Fresenius Medical Care North America** – Multiple breaches lead to findings of failure to conduct adequate risk analysis and risk management -- $3,500,000
- **Filefax** – PHI liability for mishandling of PHI survives closure of business -- $100,000
- **MD Anderson** – ALJ rules in favor of OCR following thefts of unencrypted media affecting over 33,500 individuals-- $4,348,000

2018 Enforcement Actions and Settlements

- **ABC Cases (3)** – PHI disclosed during filming of Boston Med-- $999,000
- **Anthem** – Largest U.S. PHI breach in history. OCR investigation find inadequate safeguards to prevent and address spearphishing attacks- $16,000,000
- **Allergy Associates of Hartford, PC** – Doctor discloses PHI to reporter in response to dispute with patient – $125,000

2018 Enforcement Actions and Settlements

- **Advanced Care Hospitalist** – Physicians group shares PHI with unknown vendor without a BAA – $500,000
- **Pagosa Springs Medical Center** – Hospital failed to terminate former employee remote access leading to impermissible disclosure – $111,400
- **Cottage Health** – Failures to configure security settings correctly led to exposure of 62,500 individuals' ePHI in 2 separate breaches – $3,000,000

Recurring Compliance Issues

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)).

The HIPAA Omnibus Rule, issued in January 2013, changed the standards for BAAs

- –Modified BAA requirements
- –Must execute a BAA that includes the modified provisions
- –Compliance date: September 23, 2013

Case Example: Advanced Care Hospitalists

- A contractor physician group
- ACH filed a breach report confirming that ACH patient information was viewable on a medical billing services' website
- ACH never had a BAA with the individual providing medical billing services to ACH
- ACH failed to adopt any policy requiring business associate agreements until April 2014
- ACH had been in operation since 2005
  - No risk analysis or implemented security measures
  - No HIPAA policies or procedures before 2014.
- Settlement with RA/CAP - September 2018 for $500,000

Risk Analysis: Incomplete or Inaccurate

- 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
- Found inadequate safeguards to prevent and address spearphishing attacks
- Settlement with RA/CAP – October, 2018 for $16,000,000

Impermissible Disclosures: Media

- 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.
- OCR Media Guidance
  - https://www.hhs.gov/hipaa/for-professionals/faq/2023/film-and-media/index.html

Case Example: Allergy Associates

- Dispute regarding care
- Impermissible Disclosure to reporter
- Advised by Privacy Officer and attorney not to discuss matter
- Disregarded advice
- Settlement with RA/CAP - November 2018 for $125,000

Case Example: ABC Cases

- Involved in filming of ABC television network documentary series
- Failed to first obtain authorization from patients

3 Separate Settlements - $999,000:

- Boston Medical Center ($100,000)
- Brigham and Women's Hospital ($384,000)
- Massachusetts General Hospital ($515,000)

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

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Evaluating vendor/contractor relationships and updating BAAs
- Training of workforce
- External monitoring

Compliance Best Practices

- Review vendor/contractor relationships to ensure required BAAs are in place 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

Right of Access – Provider Education

56,000+ Trained on Right to Access from July 2017 – December 2018

Credits Available

Physicians - maximum of 0.50 *AMA PRA Category 1 Credit(s)™*

You Are Eligible For

- AMA PRA Category 1 Credit(s)™

Accreditation Statements

For Physicians

Medscape

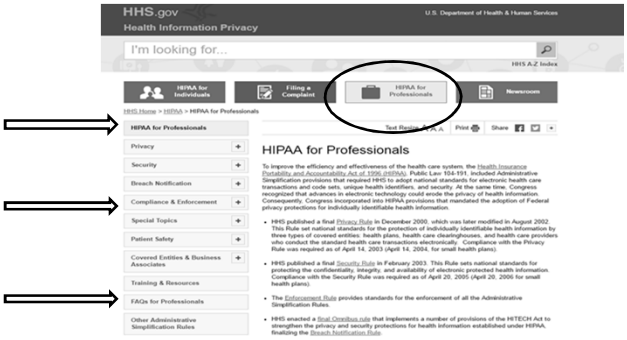
Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

An Individual's Right to Access and Obtain their Health Information Under HIPAA

Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape

http://www.medscape.org/viewarticle/876110

For More Information



- OCR's website at https://www.hhs.gov/hipaa
- Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/
- Find us on Twitter @hhsocr