# HIPAA Basic Slide Deck

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

Alicia Brown, Supervisor
OCR Pacific Region, San Francisco
November 8, 2019


## Updates

- Policy
- Breach Notification
- Enforcement
- Audit

# Policy



## Apps, APIs and the HIPAA Right of Access FAQs

- In April 2019, OCR issued new FAQs addressing the applicability of HIPAA to the use of software applications (apps) by individuals to receive health information from their providers.
- Provides guidance for covered entities, EHR developers and app developers.
- Reiterates the importance of HIPAA's right to access for individuals.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html

- **Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties Announced April 26, 2019**

| Enforcement Notice | | | |
|---|---|---|---|
| **Culpability** | Low/violation* | High/violation* | Annual limit* |
| **No Knowledge** | $100 | $50,000 | **$25,000** |
| **Reasonable Cause** | $1,000 | $50,000 | **$100,000** |
| **Willful – Corrected** | $10,000 | $50,000 | **$250,000** |
| **Willful – Not corrected** | $50,000 | $50,000 | $1,500,000 |

https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties

*The Department of Health and Human Services may make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. The annual inflation amounts are found at 45 CFR § 102.3.



# Direct Liability of Business Associates

Business associates are directly liable for HIPAA violations as follows:

- Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including protected health information (PHI), pertinent to determining compliance.
- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.
- Failure to comply with the requirements of the Security Rule.
- Failure to provide breach notification to a covered entity or another business associate.
- Impermissible uses and disclosures of PHI.

# Direct Liability of Business Associates

- Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement) to satisfy a covered entity's obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.
- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- Failure, in certain circumstances, to provide an accounting of disclosures.
- Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.
- Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html



# Direct Liability of Business Associates

Notably, OCR lacks the authority to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act does not apply the fee limitation provision to business associates. A covered entity that engages the services of a business associate to fulfill an individual's request for access to their PHI is responsible for ensuring that, where applicable, no more than the reasonable, cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.

- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

# BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY



## Breach Notification Requirements

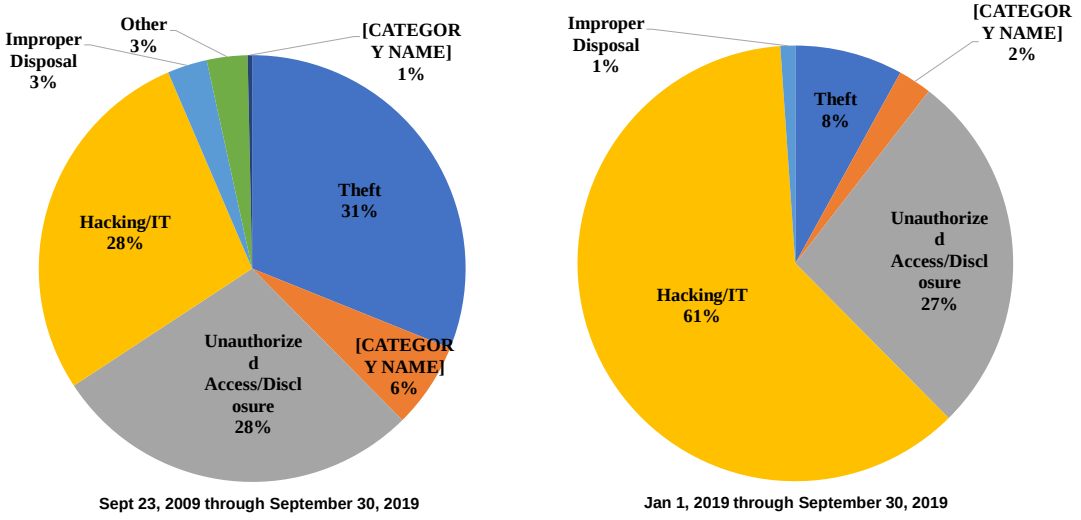
- Covered entity must notify affected individuals, HHS, and in some cases, the media
- Business associate must notify covered entity of a breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller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

# 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



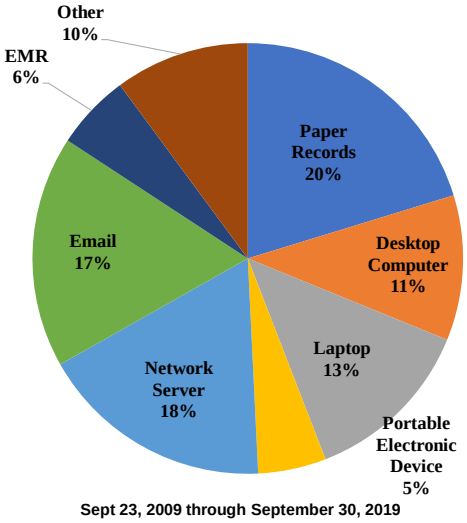
## 500+ Breaches by Type of Breach



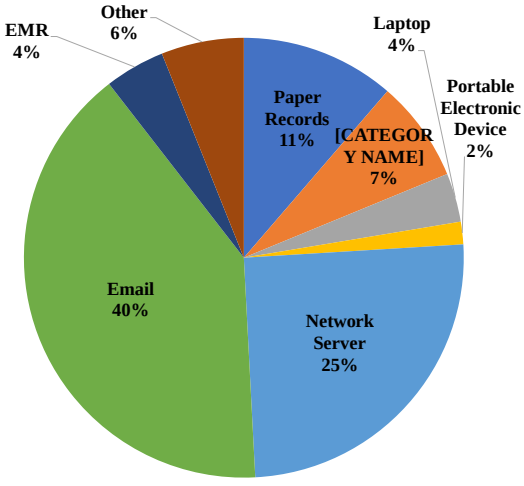

Sept 23, 2009 through September 30, 2019

Jan 1, 2019 through September 30, 2019

## 500+ Breaches by Location of Breach

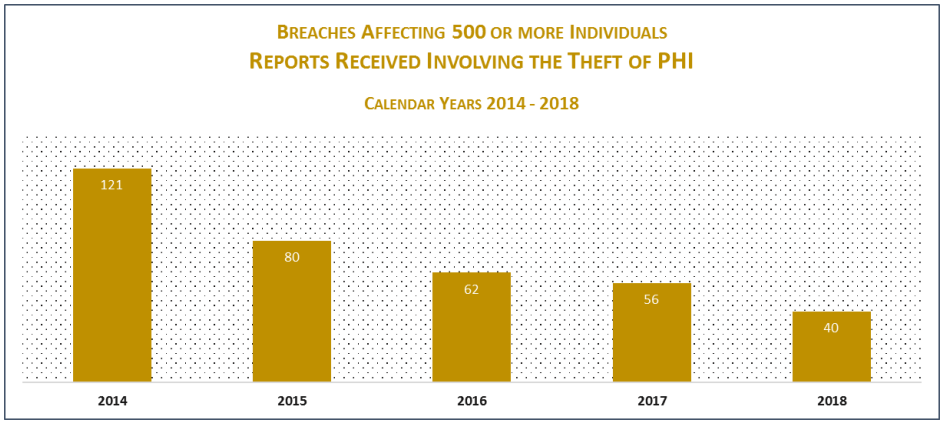


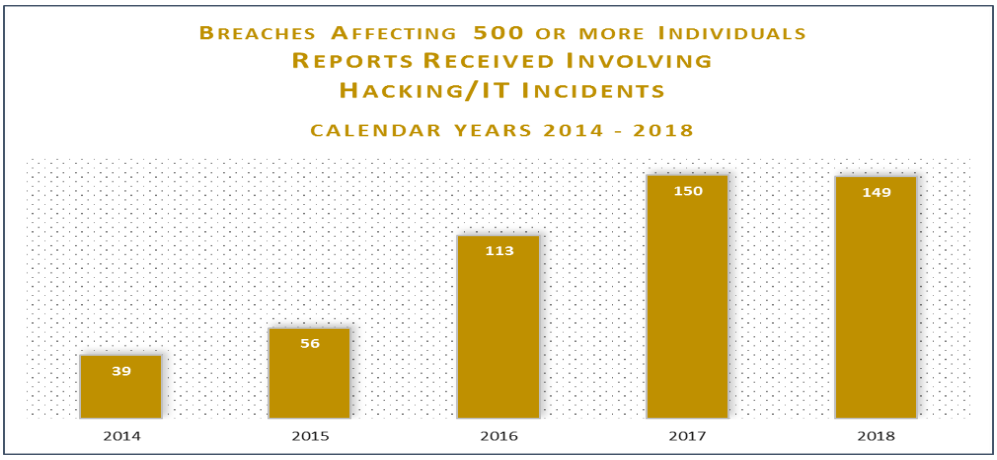

Sept 23, 2009 through September 30, 2019



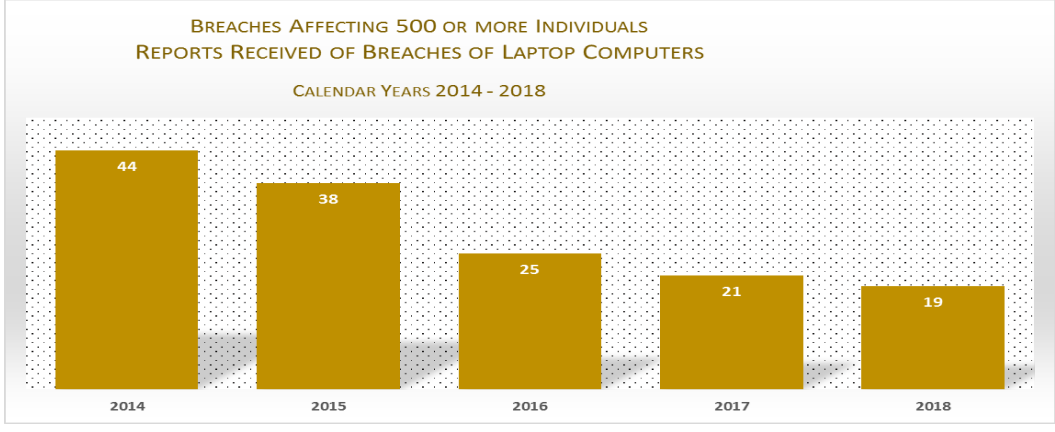

Jan 1, 2019 through September 30, 2019



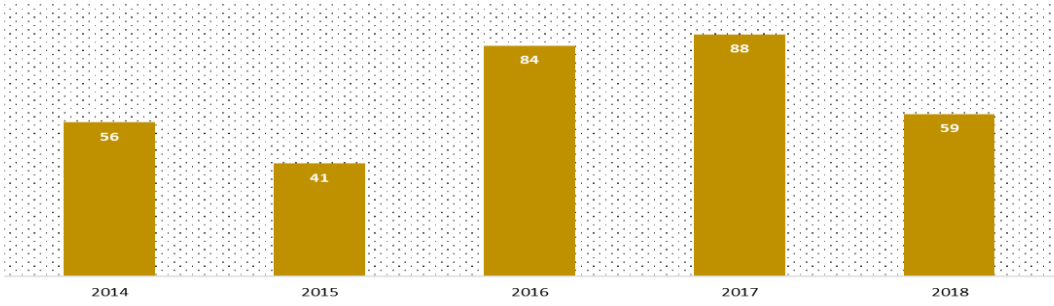



BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED INVOLVING
HACKING/IT INCIDENTS
CALENDAR YEARS 2014 - 2018
39
56
113
150
149
2014
2015
2016
2017
2018



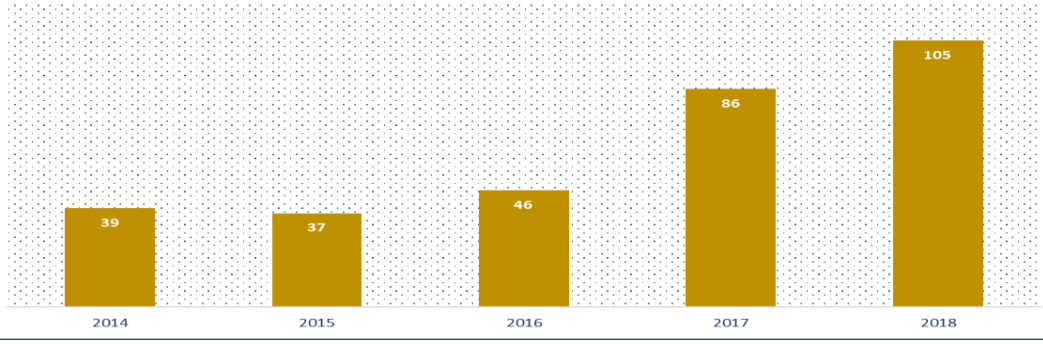

BREACHES AFFECTING 500 OR MORE INDIVIDUALS
REPORTS RECEIVED OF BREACHES OF LAPTOP COMPUTERS
CALENDAR YEARS 2014 - 2018
44
38
25
21
19
2014
2015
2016
2017
2018

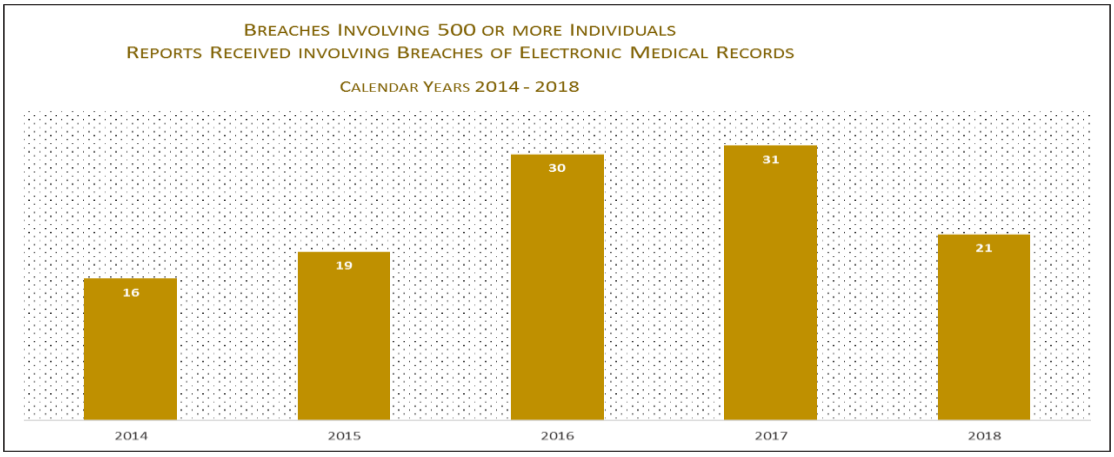
## Breaches Affecting 500 or more Individuals
## Reports Received of Breaches of Network Servers
### Calendars Years 2014 - 2018






## Breaches Affecting 500 or more Individuals
## Reports Received of Breaches Involving Email Accounts
### Calendar Years 2014 - 2018








## 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
  - 63 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

**As of September 30, 2019**

## *Recent Enforcement Actions*

| | | |
|---|---|---|
| 9/2018 | Brigham and Women's Hospital | $384,000 |
| 9/2018 | Massachusetts General Hospital | $515,000 |
| 9/2018 | Advanced Care Hospitalists | $500,000 |
| 10/2018 | Allergy Associates of Hartford | $125,000 |
| 10/2018 | Anthem | $16,000,000 |
| 11/2018 | Pagosa Springs Medical Center | $111,400 |
| 12/2018 | Cottage Health | $3,000,000 |
| 4/2019 | Touchstone Medical Imaging | $3,000,000 |
| 4/2019 | Medical Informatics Engineering | $100,000 |
| 9/2019 | Bayfront Health St. Petersburg | $85,000 |



## 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 Action

## Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- CAPs may include 3rd party or outside monitoring



# Best Practices

## 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

# 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

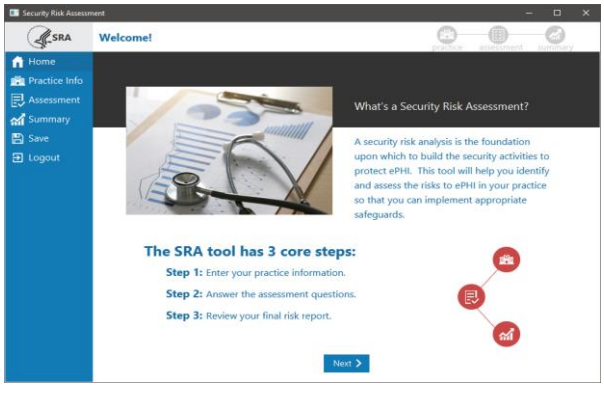
- For Covered Entities:
  - Security Rule: risk analysis and risk management; and
  - Breach Notification Rule: content and timeliness of notifications; **or**
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management **and**
  - 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
- Report to Industry planned for 2019



# SRA Tool




https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Designed to assist small to medium sized organizations in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule and the CMS EHR Incentive Program.

The SRA tool guides users through a series of questions based on standards identified in the HIPAA Security Rule. Responses are sorted into Areas of Success and Areas for Review.

Not all areas of risk may be captured by the tool. Risks not identified and assessed via the SRA Tool must be documented elsewhere.

## Provider Education:
## 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
- 70,000+ health care providers and allied health professionals trained

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



## Cybersecurity Newsletters

- Began in January 2016
- Past Topics Include
  - Risk Analyses v. Gap Analyses
  - Workstation Security
  - Software Vulnerabilities and Patching
  - Guidance on Disposing of Electronic Devices and Media
  - Considerations for Securing Electronic Media and Devices
  - Sign up for the OCR Listserv:

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

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr




# Contact Us

**Office for Civil Rights**
U.S. Department of Health and Human Services

ocrmail@hhs.gov
**www.hhs.gov/ocr**

**Voice:** (800) 368-1019
**TDD:** (800) 537-7697
**Fax:** (202) 519-3818

200 Independence Avenue, S.W.
H.H.H Building, Room 509-F
Washington, D.C. 20201