Updates in HIPAA Enforcement

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

Danielle Archuleta, J.D.
Supervisory Equal Opportunity Specialist
OCR – Pacific Region
February 27, 2020
Alaska Region Compliance & Ethics Conference

1

Updates

- Policy
- Breach Notification
- Enforcement
- Audit

2

Policy

3

HIPAA Regulatory Sprint

RFI asked for comments on specific areas of the HIPAA Privacy Rule, including:

- Encouraging timely information-sharing for treatment and care coordination;
- Addressing the opioid crisis and serious mental illness; and
- Changing the current signature requirement on the Notice of Privacy Practices.

4

HIPAA and FERPA Joint Guidance

New clarifications and examples address:

- When can PHI or personally identifiable information (PII) from an education record be shared with the parent of an adult student?
- What options do family members of an adult student have under HIPAA if they are concerned about the student's mental health and the student does not agree to disclosures of their PHI?
- Does HIPAA allow a covered health care provider to disclose PHI about a minor with a mental health condition or substance use disorder to the minor's parents?
- When can PHI or PII be shared about a student who presents a danger to self or others?

Health App FAQs

- A covered entity cannot withhold releasing ePHI to a user-requested health app because of concerns about how the app will use the ePHI.
- A covered entity is not liable for the re-disclosure of ePHI by a health app if there is no business associate relationship.
- Buyer Beware: HIPAA Rules don't follow health data everywhere it goes.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html (April 2019)

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 of 2015. The annual inflation amounts are found at 45 CFR § 102.3.

7

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

8

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

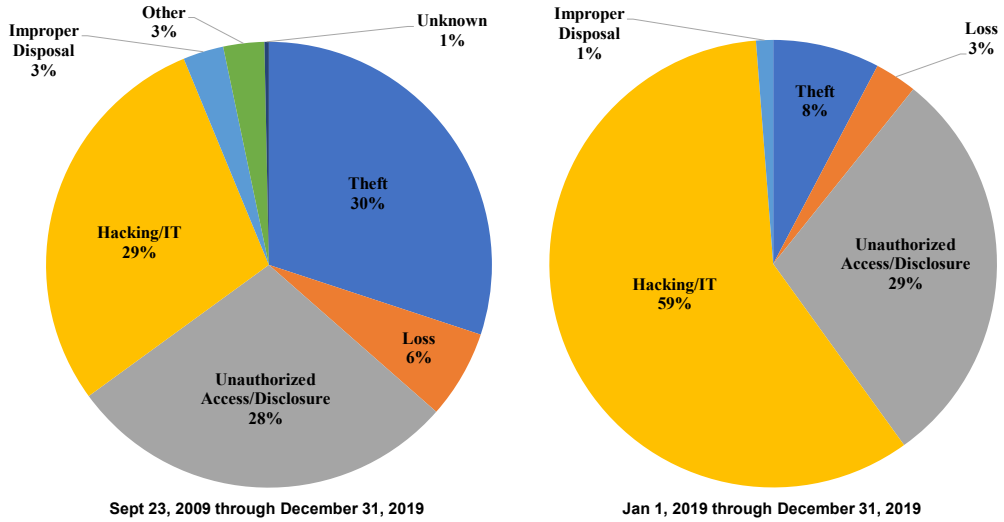
9

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
- OCR breach investigations examine:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity's compliance prior to the breach

10

500+ Breaches by Type of Breach

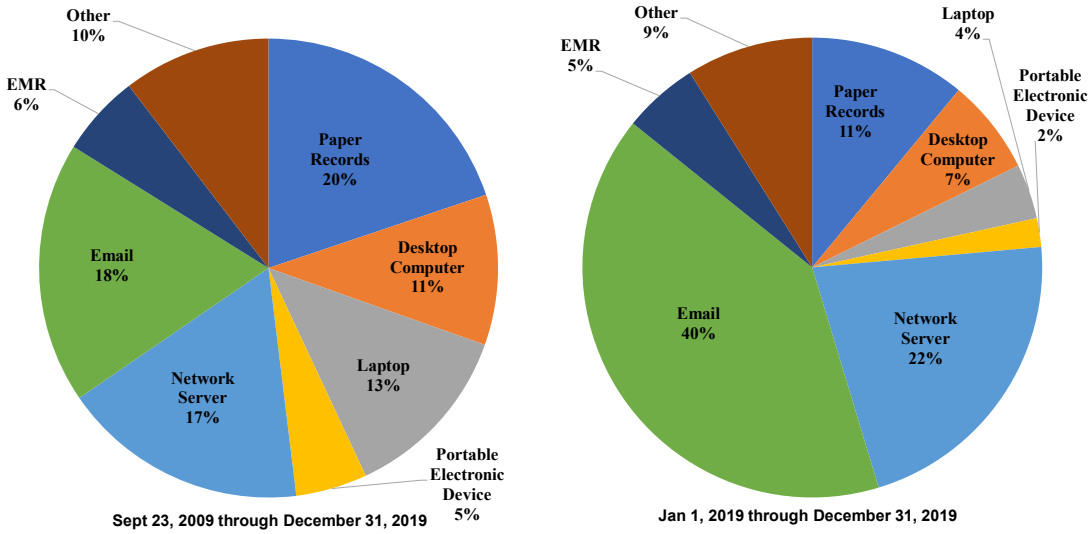


Sept 23, 2009 through December 31, 2019

Jan 1, 2019 through December 31, 2019

11

500+ Breaches by Location of Breach



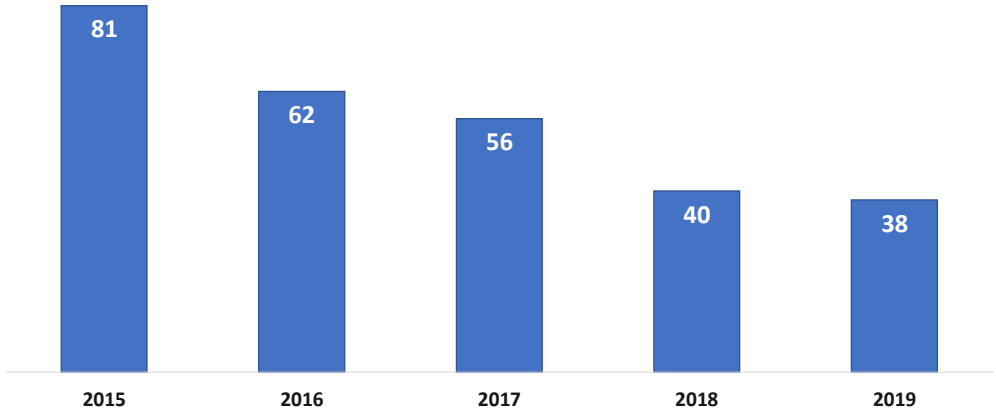
Sept 23, 2009 through December 31, 2019

Jan 1, 2019 through December 31, 2019

12

Breaches Affecting 500 or More Individuals
Reports Received Involving the Theft of PHI

Calendar Years 2015 - 2019



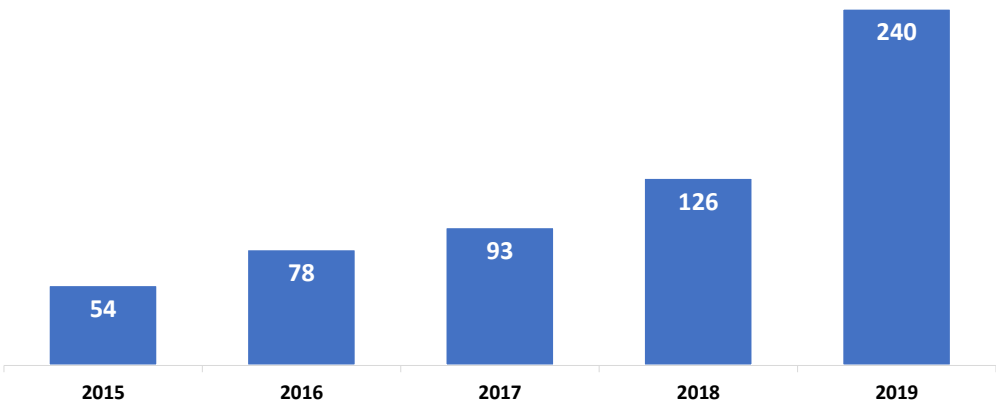
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

13

13

Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

Calendar Years 2015 - 2019



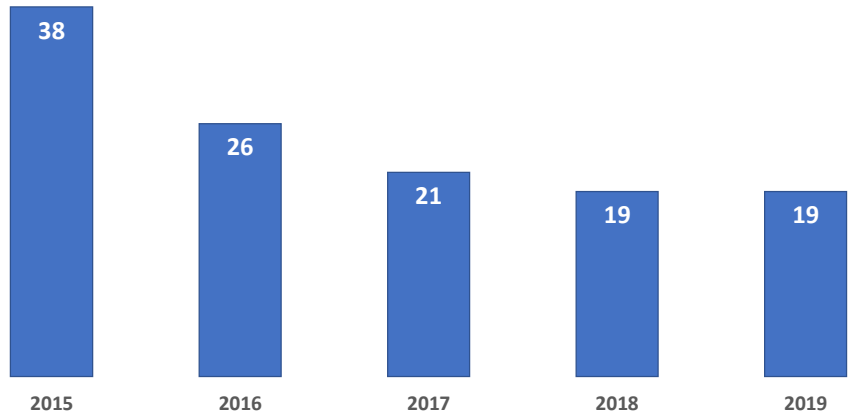
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

14

14

Breaches Affecting 500 or More Individuals
Reports Received of Breaches of Laptop Computers

Calendar Years 2015 - 2019



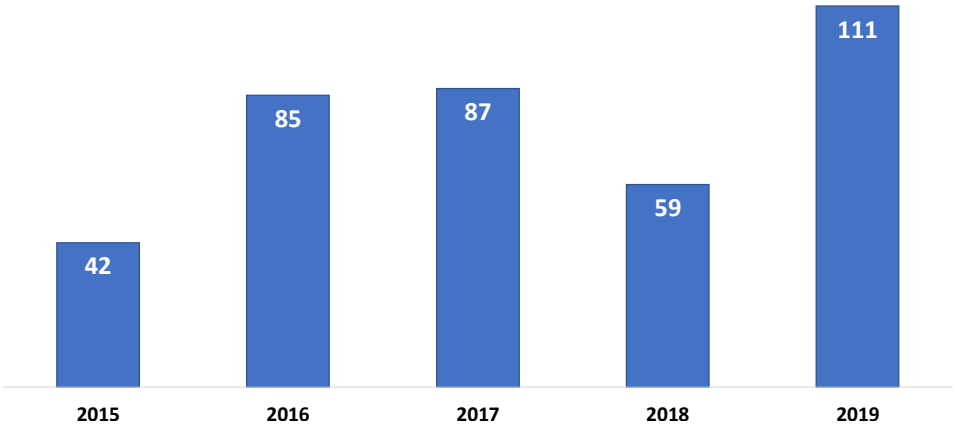
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

15

15

Breaches Affecting 500 or More Individuals
Reports Received of Breaches of Network Servers

Calendar Years 2015 - 2019



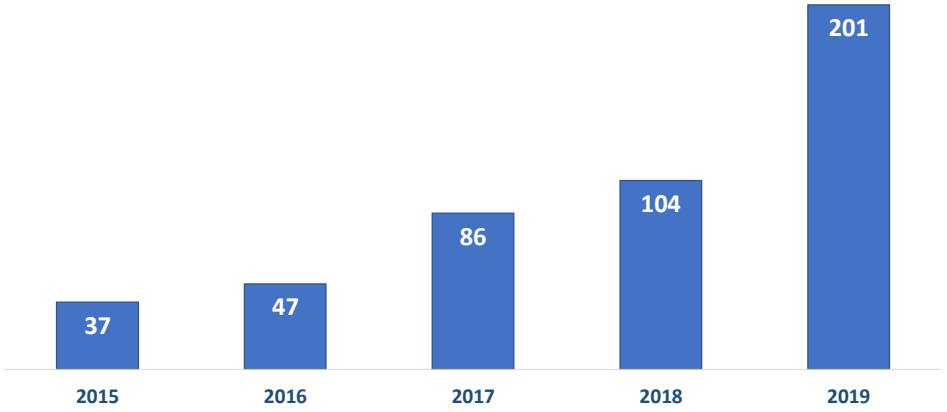
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

16

16

Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Email Accounts

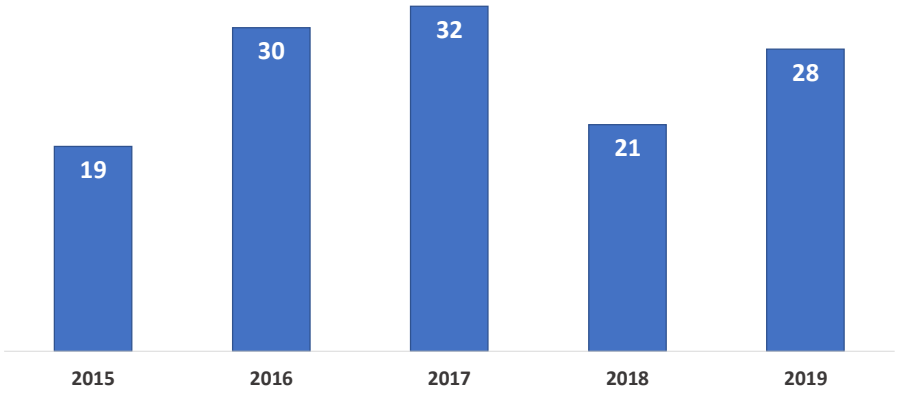
Calendar Years 2015 - 2019



17

Breaches Involving 500 or more Individuals
Reports Received Involving Breaches of Electronic Medical Records

Calendar Years 2015 - 2019



18

General HIPAA Enforcement Highlights

- OCR expects to receive over 28,000 complaints this year.
- In most cases, entities are 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
  - 68 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 6 civil money penalties

As of December 31, 2019

19

2019 Enforcement Actions

4/2019	Touchstone Medical Imaging	$3,000,000
4/2019	Medical Informatics Engineering	$100,000
9/2019	Bayfront Health St. Petersburg	$85,000
9/2019	Elite Dental Associates, Dallas	$10,000
10/2019	Jackson Health System (CMP)	$2,154,000
10/2019	Texas Health and Human Services Commission (CMP)	$1,600,000
10/2019	University of Rochester Medical Center	$3,000,000
11/2019	Sentara Hospitals	$2,175,000
12/2019	Korunda Medical	$85,000
12/2019	West Georgia Ambulance	$65,000

Total: $12,274,000

20

Recurring Compliance Issues

- Individual Right of Access
- Risk Analysis
- Business Associate Agreements
- Access Controls
- Audit Controls
- Information System Activity Review

21

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

22

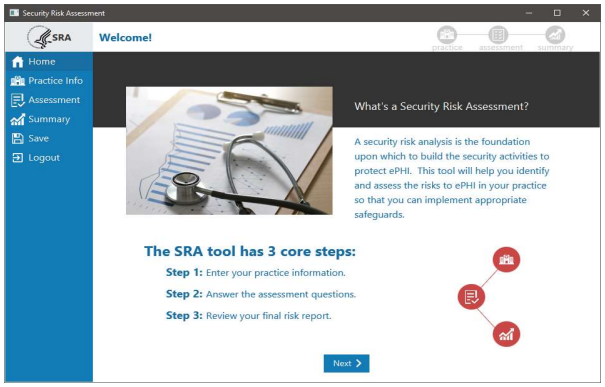
Best Practices

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

23

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.

24

2019 Cybersecurity Newsletters

- Began in January 2016
- Recent Topics Include:
  - Preventing, Mitigating, and Responding to Ransomware
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats
  - Phishing
  - Software Vulnerabilities and Patching
  - Securing Electronic Media and Devices
- Sign up for the OCR Listserv:
  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

25

Right of Access

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

80,000+ health care providers and allied health professionals trained

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

26

AUDIT

27

HITECH Audit Program

Purpose:

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

28

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 2020

31

Connect with Us

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

www.hhs.gov/hipaa

Join our Privacy and Security listservs at
https://www.hhs.gov/hipaa/for-professionals/list-serve/

@HHSOCR

32

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

33

33