



HIPAA Breach Notification and Enforcement Rules

Iliana Peters, JD, LLM, CISSP

February 3, 2020



THE HIPAA BREACH NOTIFICATION RULE

HIPAA & the HITECH Act

Health Insurance Portability and Accountability Act (HIPAA) (1996)

Privacy Rule

Security Rule

Enforcement Rule

HITECH, short for the *Health Information Technology for Economic and Clinical Health Act (2009)*:

Breach Notification Rule

HIPAA Rules for *Business Associates*

Limited certain uses and disclosures of PHI

Increased individual rights with respect to PHI

Increased enforcement of, and penalties for, HIPAA violations



KEY DEFINITIONS

PHI Defined

Individually
Identifiable Health
Information

- Any information, including demographic information, collected from an individual, that is created by a CE.

Protected Health
Information (PHI)

- Individually identifiable health information held or transmitted in any form or medium by . . . HIPAA covered entities and business associates, subject to certain limited exceptions.”

PHI includes

- Information that relates to all of the following:
 - The individual’s past, present, or future physical or mental health or condition
 - The provision of health care to the individual
 - The past, present, or future payment for the provision of health care to the individual
- PHI includes many common identifiers, such as name, address, birth date, and Social Security number

Covered Entities & Business Associates

“Covered Entities” include:

- Health plans
- Health care clearinghouses
- Health care providers who (i) transmit any health information in electronic form (ii) in connection with a transaction covered by the HIPAA Privacy Rule.

“Business Associates”:

- Persons or entities that perform a service for, or on behalf of, a Covered Entity which involves the use or disclosure of PHI
- *Need written Business Associate Agreement*

Breach Defined

“[B]reach means the **acquisition, access, use, or disclosure** of **[unsecured] protected health information** in a manner not permitted under HIPAA which compromises the security or privacy of the protected health information.” 45 C.F.R. §164.402 (2013).

Breach Defined (cont.)

Secured PHI

Using encryption or an encryption algorithm specified in HHS guidance to safeguard PHI

Risk Assessment NOT Required

Notification NOT Required

Unsecured PHI

NOT using encryption or an encryption algorithm specified in HHS guidance to safeguard PHI

Risk Assessment Required

Notification Required

Breach Notification Rule – Requirement Overview

WHO:

Covered Entities

Business Associates

Subcontractors

WHAT:

Risk Assessment

Notification

WHEN & WHOM:

As soon as reasonable

No longer than 60
days from discovery

To affected individuals

HHS

Media

WHY:

Civil Penalties up to
\$1.5 million

Criminal Penalties,
including
imprisonment

Breach Notification – Notify

Whom

Affected Individuals

HHS Secretary

- Notify HHS within a year plus 60 days – fewer than 500 individuals
- Notify HHS & the Individuals contemporaneously – greater than 500 individuals (reasonable time and no later than 60 days)

Media

- Great than 500 individuals

When

Without unreasonable delay:

- Outer limit is 60 days

Discovery:

- Knew vs. should have reasonably known

Breach:

- Discovered vs. completed investigation confirming breach

Covered Entity:

- Business associate's discovery imputed if agent vs. independent contractor

How

In writing and delivered by first-class mail at last known address, or next of kin if deceased

- (email if agreed to by individual);

Reasonable substitution as necessary to reach individual

Lack contact information for more than 10 individuals


- Conspicuous notice for 90 days on CE's homepage website, or
- Notice in major print or broadcast media in geographic areas of affected individuals (include toll-free phone no.)

In case of urgency, may use telephone or other means

Print or Broadcast Media if more than **500** affected individuals (in a jurisdiction)

HHS Web Portal

Contents of Notice – Written in Plain Language



A brief description of what happened, including the date of both the breach and discovery;

A description of the types of unsecured protected health information involved;

A description of any steps that the subjects of data breaches should take to protect themselves from potential harm resulting from the breach;

A brief description of investigative and mitigating actions taken since the breach;

Contact information for individuals to ask questions or learn additional information, including a toll-free phone number, postal address, or e-mail address.

Takeaways

Plan

- Privacy policies and procedures up to date that accurately reflect practices/business
- Understand consequences of breach
- Responsible vendor contracts

Train

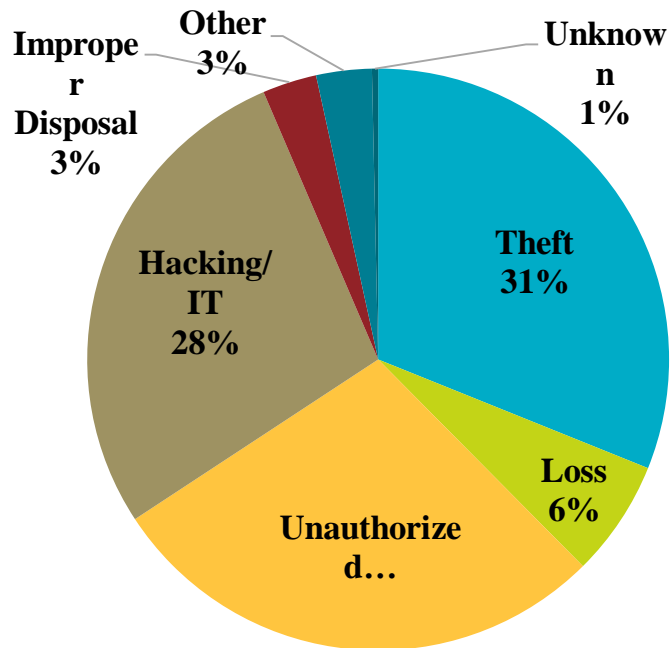
- Identify risks through discussions with IT, management, HR
- Protect against biggest risks
- Detection systems
- Run through response to breach

Prepare for a breach incident

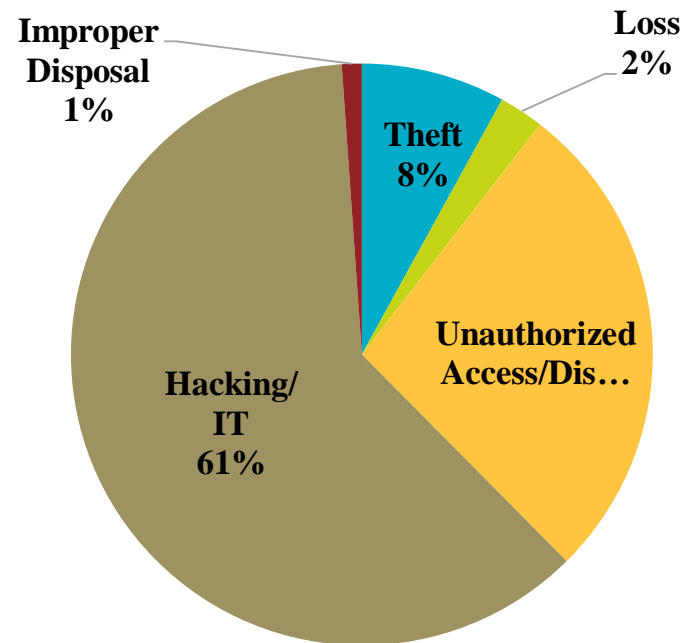
- Pre-draft PR/notice statements
- Identify experts needed if incidence of breach
- Understand notification requirements/deadlines

Breach Update

500+ Breaches by Type of Breach



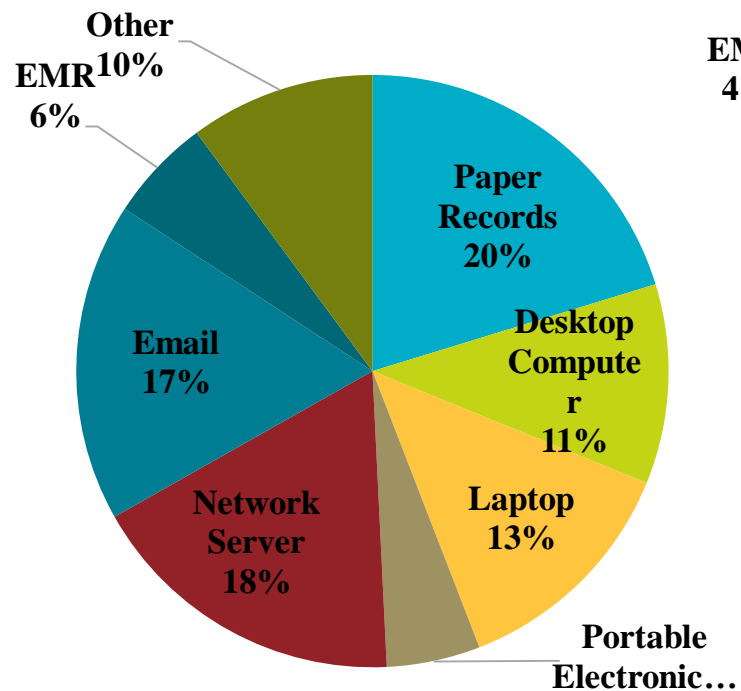
Sept 23, 2009 through September 30, 2010



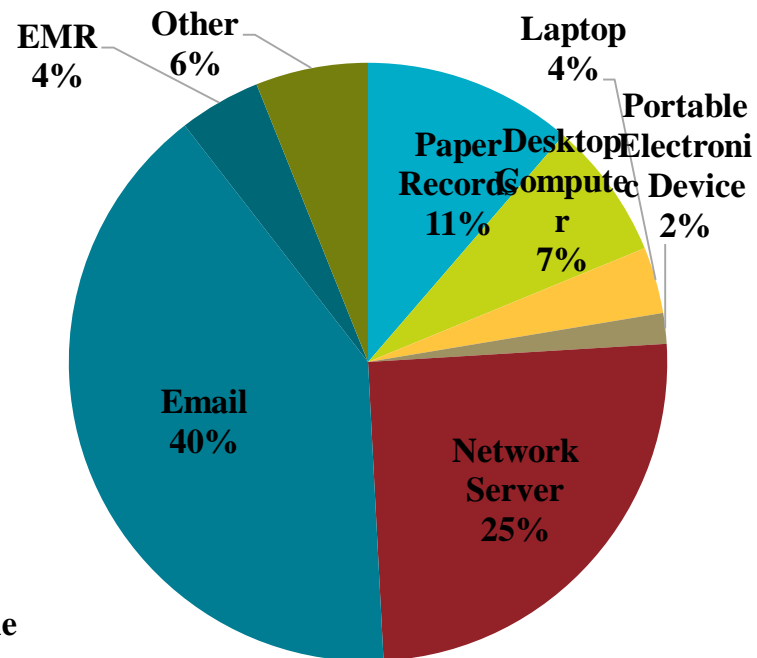
Jan 1, 2019 through September 30, 2019

Breach Update

500+ Breaches by Location of Breach



Sent 23. 2009 through September 30. 20



Jan 1, 2019 through September 30, 2019



HIPAA ENFORCEMENT RULE



Preemption of State Law

- **45 C.F.R. § 160.203 General rule and exceptions.**
- A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law.



Investigations

- **45 C.F.R. § 160.310 Responsibilities of covered entities and business associates.**
- (a) Provide records and compliance reports.
- (b) Cooperate with complaint investigations and compliance reviews.

Subpoenas

- **45 C.F.R. § 160.314 Investigational subpoenas and inquiries.**
- (a) The Secretary may issue subpoenas in accordance with 42 U.S.C. 405(d) and (e), 1320a7a(j), and 1320d-5 to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review pursuant to this part. For purposes of this paragraph, a person other than a natural person is termed an “entity.”

Imposition of Civil Money Penalties¹

BEFORE NOTIFICATION OF ENFORCEMENT DISCRETION

Culpability	Minimum Penalty/ Violation	Maximum Penalty/ Violation	Annual Limit
No Knowledge	\$100	\$50,000	\$1,500,000
Reasonable Cause	\$1,000	\$50,000	\$1,500,000
Willful Neglect - Corrected	\$10,000	\$50,000	\$1,500,000
Willful Neglect - Not Corrected	\$50,000	\$50,000	\$1,500,000

AFTER NOTIFICATION OF ENFORCEMENT DISCRETION

Culpability	Minimum Penalty/ Violation	Maximum Penalty/ Violation	Annual Limit
No Knowledge	\$100	\$50,000	\$25,000
Reasonable Cause	\$1,000	\$50,000	\$100,000
Willful Neglect - Corrected	\$10,000	\$50,000	\$250,000
Willful Neglect - Not Corrected	\$50,000	\$50,000	\$1,500,000

¹<https://www.ecfr.gov/cgi-bin/text-idx?SID=62698974ad3e15d8181d2eae0152961&mc=true&node=pt45.1.160&rgn=div5#sp45.2.160.d>

Annual Civil Money Penalties Inflation Adjustment¹

CMP for HIPAA violations in accordance with the Inflation Adjustment Act

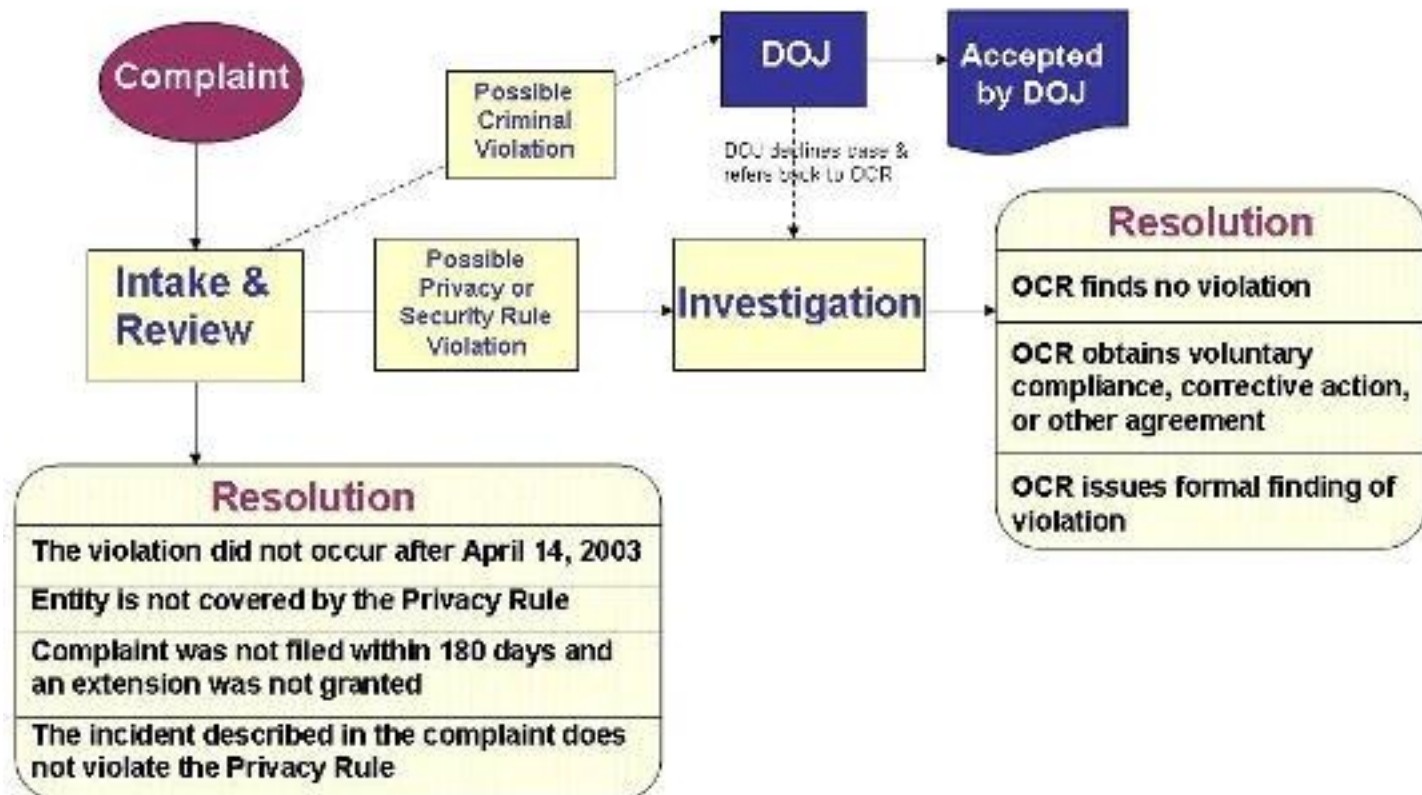
Penalty Tier	Level of Culpability	Minimum Penalty per Violation (2018 - 2019)	Maximum Penalty per Violation (2018 - 2019)	New Maximum Annual Penalty (2018 - 2019)*
1	No Knowledge	\$114.29 - \$117	\$57,051 - \$58,490	\$1,711,533 - \$1,754,698
2	Reasonable Cause	\$1,141 - \$1,170	\$57,051 - \$58,490	\$1,711,533 - \$1,754,698
3	Willful Neglect: Corrective Action Taken	\$11,140 - \$11,698	\$57,051 - \$58,490	\$1,711,533 - \$1,754,698
4	Willful Neglect: No Corrective Action Taken	\$57,051 - \$58,490	\$1,711,533 - \$1,754,698	\$1,711,533 - \$1,754,698

Key Takeaway: The revised Annual Limits have yet to be made official,
so OCR can legally use the new maximum Annual Penalty Limit
increased for inflation across all penalty tiers: **\$1,754,698**

¹<https://www.govinfo.gov/content/pkg/FR-2019-11-05/pdf/2019-23955.pdf>

OCR Investigation Process

HIPAA Privacy & Security Rule Complaint Process



Informal v. Formal Resolution

Settlements and Corrective Action Plans

- Remediate HIPAA compliance programs

Civil Penalties

- Up to **\$1.5 million/\$1.7** for each violation of an identical HIPAA provision over the course of a calendar year

Criminal Penalties

- Start with fines of \$50,000 and/or **imprisonment** for not more than one year



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 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
 - 59 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- Four civil money penalties

Summary of 2019 OCR Settlements & CMPs¹


Type of Violation	Number	Collected
• Unencrypted laptop and mobile devices	3	\$3,165,000.00
• Not notifying OCR or victims of the breach	1	\$3,000,000.00
• Lack of BA Agreement	1	\$2,175,000.00
• Not discovering a breach in a timely manner	1	\$2,154,000.00 - CMP
• Lack of access credentials on public server	1	\$1,600,000.00 - CMP
• Failing to provide right of access	2	\$170,000.00
• Disclosing PHI on Yelp reviews	<u>1</u>	<u>\$10,000.00</u>
	10	\$12,274,000.00

¹<https://www.hhs.gov/civil-rights/for-providers/compliance-enforcement/agreements/index.html>

Questions?

Iliana Peters: ipeters@polsinelli.com





Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

*© 2017 Polsinelli PC. In California, Polsinelli LLP.
Polsinelli is a registered mark of Polsinelli PC*

