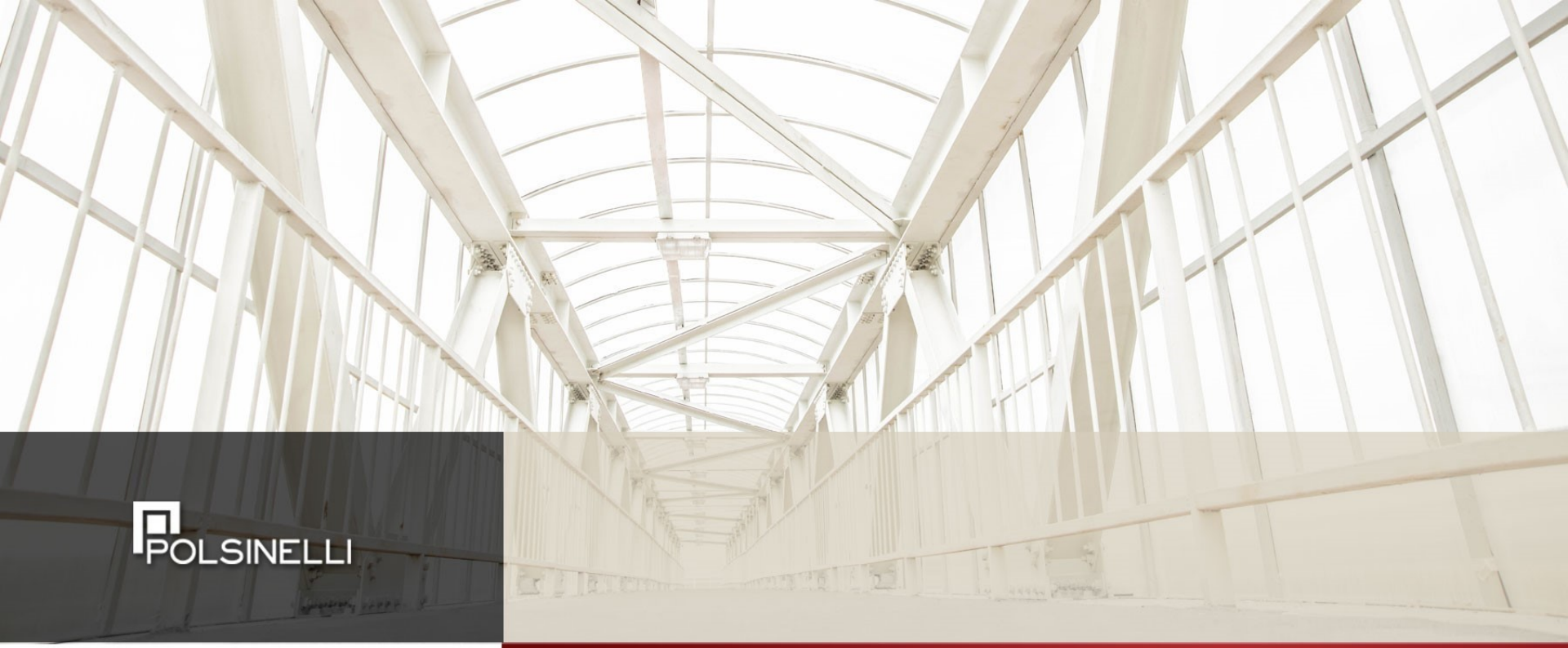


POLSINELLI

It's Midnight. Do you Know Where your Data Is?

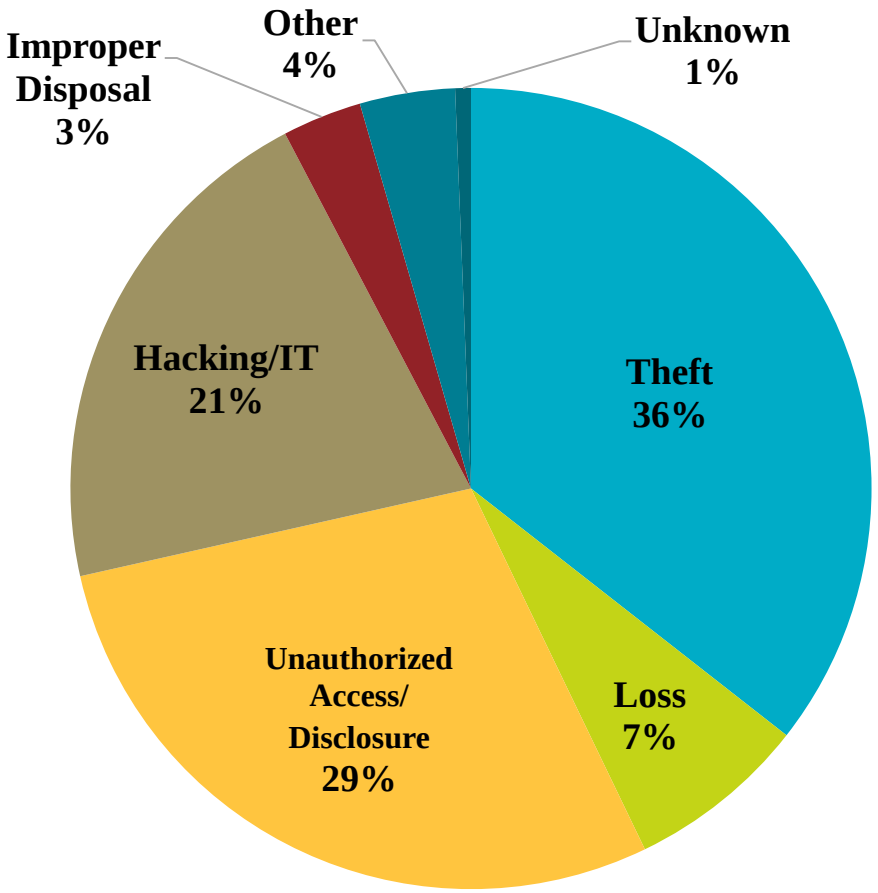
Cyber Threats to Health Data and Regulatory Requirements in a Cyber Incident

Iliana L. Peters, JD, LLM, CISSP

HIPAA Breach Highlights

500+ Breaches by Type of Breach

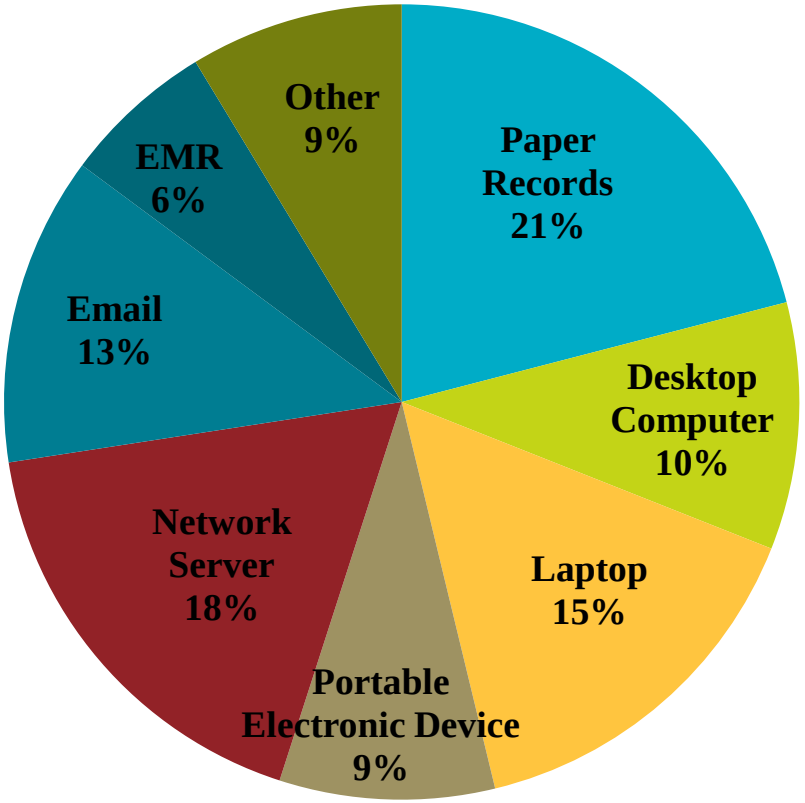
September 23, 2009 – August 31, 2018



HIPAA Breach Highlights

500+ Breaches by Location of Breach

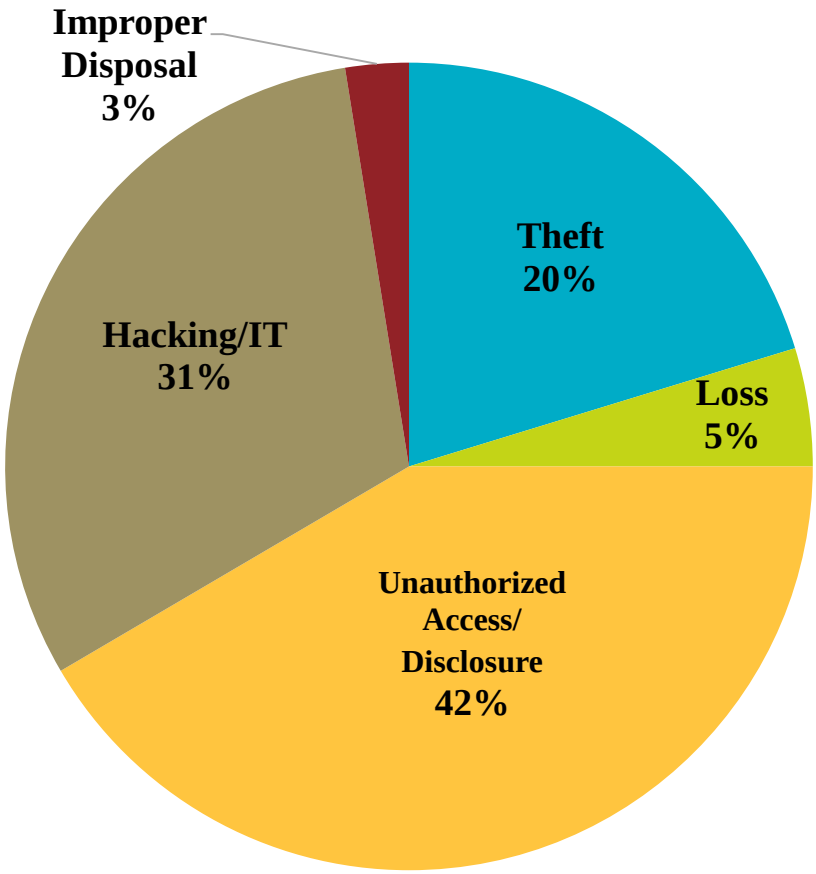
September 23, 2009 – August 31, 2018



HIPAA Breach Highlights

500+ Breaches by Type of Breach

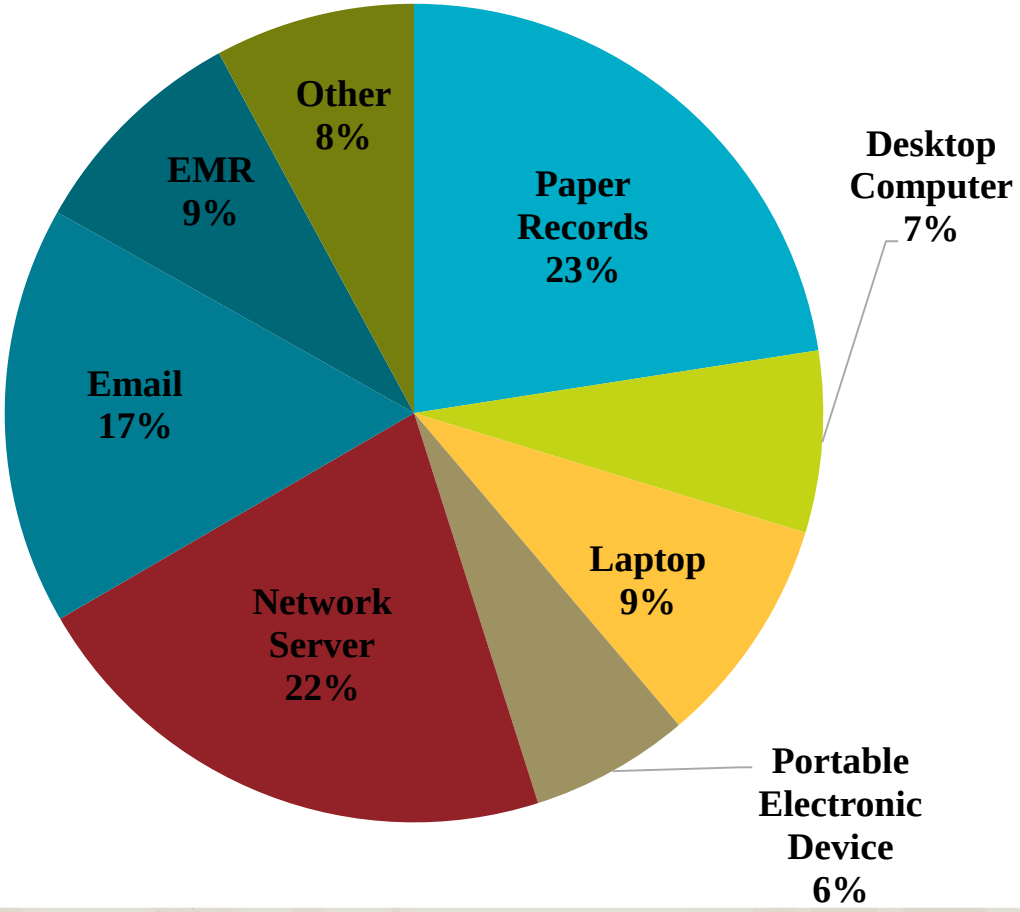
September 1, 2015 – August 31, 2018



HIPAA Breach Highlights

500+ Breaches by Location of Breach

September 1, 2015 – August 31, 2018



GDPR Breaches

- Approx. 60,000 breaches reported since May 25, 2018.
- Notify within 72 hours of becoming aware.
- Broad definition of breach:
  - *a **breach** of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

HIPAA Enforcement Case 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
- 4 civil money penalties

Recent HHS Enforcement Actions

- "OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement – February 7, 2019 OCR has concluded an all-time record year in HIPAA enforcement activity. In 2018, OCR settled 10 cases and secured one judgment, together totaling $28.7 million. This total surpassed the previous record of $23.5 million from 2016 by 22 percent. In addition, OCR also achieved the single largest individual HIPAA settlement in history of $16 million with Anthem, Inc., representing a nearly three-fold increase over the previous record settlement of $5.5 million in 2016."

2018 HHS Enforcement Actions

Date	Name	Amount
Jan. 2018	Filefax, Inc (settlement)	$100,000
Jan. 2018	Fresenius Medical Care North America (settlement)	$3,500,000
June 2018	MD Anderson (judgment)	$4,348,000
Aug. 2018	Boston Medical Center (settlement)	$100,000
Sep. 2018	Brigham and Women's Hospital (settlement)	$384,000
Sep. 2018	Massachusetts General Hospital (settlement)	$515,000
Sep. 2018	Advanced Care Hospitalists (settlement)	$500,000
Oct. 2018	Allergy Associates of Hartford (settlement)	$125,000
Oct. 2018	Anthem, Inc (settlement)	$16,000,000
Nov. 2018	Pagosa Springs (settlement)	$111,400
Dec. 2018	Cottage Health (settlement)	$3,000,000
	Total (settlements and judgment)	$28,683,400

"Start With Security:" FTC Enforcement Actions

- mResource LLC (Loop Works LLC), In the Matter of (November 19, 2018)
- VenPath, Inc., In the Matter of (November 19, 2018)
- SmartStart Employment Screening, Inc., In the Matter of (November 19, 2018)
- LabMD, Inc. v. Federal Trade Commission (November 19, 2018)
- Uber Technologies, Inc. (October 29, 2018)
- IDmission LLC, In the Matter of (October 11, 2018)
- BLU Products and Samuel Ohev-Zion, In the Matter of (September 11, 2018)
- PayPal, Inc., In the Matter of (May 24, 2018)
- VTech Electronics Limited (January 8, 2018)
- TaxSlayer (November 8, 2017)
- Ashley Madison (September 27, 2017)
- Lenovo, Inc. (September 13, 2017)
- D-Link (May 22, 2017)
- LabMD, Inc., In the Matter of (September 29, 2016)
- ASUSTeK Computer Inc., In the Matter of (July 28, 2016)
- Henry Schein Practice Solutions, Inc., In the Matter of (May 23, 2016)
- Oracle Corporation, In the Matter of (March 29, 2016)
- LifeLock, Inc., a corporation (January 5, 2016)
- Wyndham Worldwide Corporation (December 11, 2015)
- Cornerstone and Company, LLC (April 21, 2015)

State AG/OCR Case

- Indiana Attorney General leading a multi-state federal lawsuit against Medical Informatics Engineering Inc. and NoMoreClipboard LLC, which sustained a data breach which compromised the data of more than 3.9 million people.
- “Hackers infiltrated a web application called WebChart, which is run by MIE, between May 7 and May 26, 2015. The hackers stole electronic Protected Health Information, including names, phone numbers, mailing addresses, Social Security numbers, and usernames and passwords, among other types of information.”
- Alleges violations of HIPAA Rules, along with state claims including Unfair and Deceptive Practice Laws, Notice of Data Breach statutes, and state Personal Information Protection Acts.
- “Hill's office says it is the first time state attorneys general have joined to pursue a HIPAA-related data breach case in federal court.” See http://www.insideindianabusiness.com/story/39579639/hill-files-multi-state-data-breach-lawsuit.

HIPAA 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

Recurring Compliance Issues - GDPR

- Data Processing Agreements
- Vendor management failures
- Lack of Appropriate Auditing
- Security issues
- Improper Disposal
- No lawful basis for processing
- Failure to comply with ‘accountability principal’

HHS Risk Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
- https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf

FTC Resources

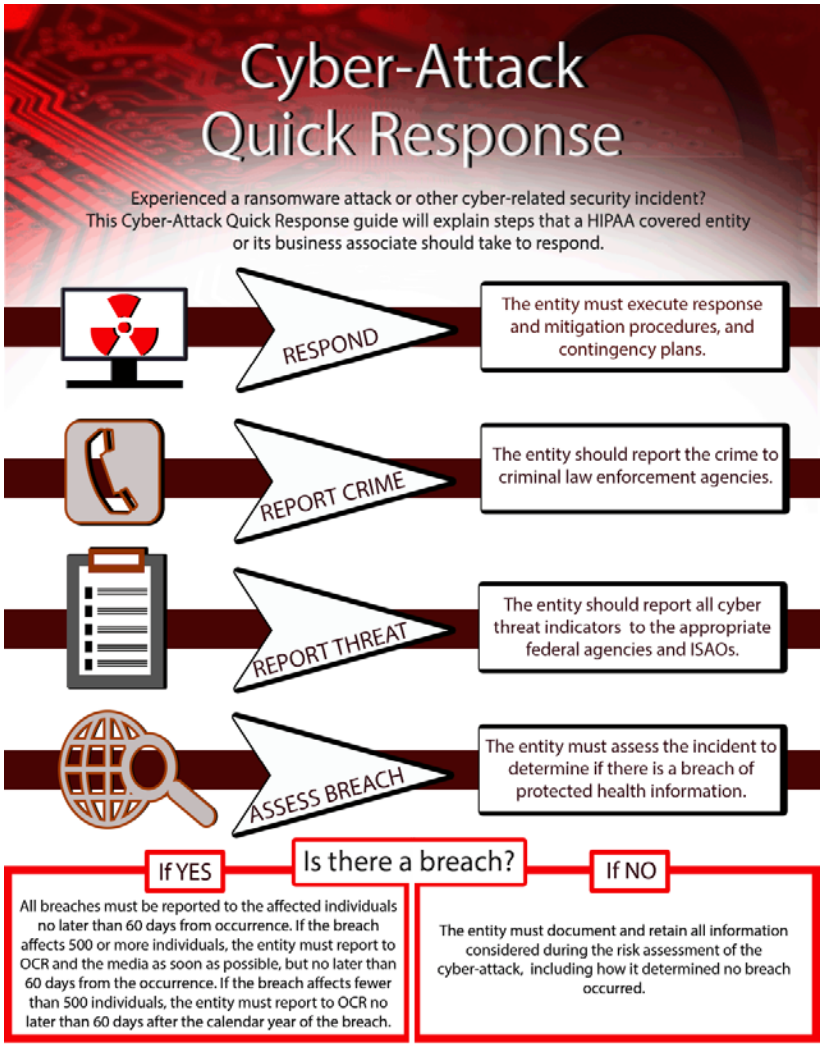
- https://www.ftc.gov/
- https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-report-finds-some-small-business-web-hosting-services-could

Vendor Cyber Risk Management

- FTC Guidance: https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series
- NIST Guidance: https://www.nist.gov/cyberframework
- HHS Cloud Guidance: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- HHS Business Associate Guidance: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es
- Remote Access Issues

Ransomware Attacks

- Phishing and Ransomware
  - Security Awareness and Training and Security Reminders
  - Be Prepared
  - Practice!



Training

- Most settlements include a training requirement
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- OCR Published a Monthly Cybersecurity Newsletter
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html
- OCR YouTube Page
  - https://www.youtube.com/user/USGovHHSOCR

Questions?

- Feel free to contact me for more information:
  - Iliana Peters: ipeters@polsinelli.com