It's Midnight. Do you know where your data is?

Presenters:

Jonathan Alford, *Senior Corporate Attorney, Otsuka America Pharmaceuticals*

Michael Gaba, *Shareholder, Polsinelli PC*

Iliana Peters, *Shareholder, Polsinelli PC*

January 9, 2020

What’s your nightmare?

- Ransomware
- Email compromise
- Stolen Device
- Break-In
- Insider Attack
- Malware

CCPA

- Goes into effect Jan. 2020 with enforcement starting in July 2020
- Enacted quickly and the details are still not completely finalized
- Imposes new obligations on companies that collect personal information (PI) about CA residents
- Creates an exception for:
  - HIPAA-covered entities for their handling of PHI
  - Medical Information governed by the California Confidentiality of Medical Information Act
  - Information collected for approved clinical trial purposes
- Because of the exceptions, some data assets may be excluded but others will be covered

CCPA – Applicability

- Applies to organizations of a certain size that collect personal information about consumers based in California
  - Due to website collection and other online activities this is almost every large organization
- “Personal Information” – information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular consumer
  - Applies to information in all mediums

CCPA – Basics

Creates rights for California residents whose information a Business holds

- Transparency – business must disclose what information it collects
- Right of access to PI business maintains
- Right to opt-out of business selling PI
- Right to delete PI business maintains
- Data portability – right to get a copy of the data
- Right of equal service – Business cannot penalize people for exercising their rights

Imposes restrictions on vendors that service companies

- Limits their use of the information for purposes related to the contract

CCPA Compliance Project Plan

Phase	Phase 1	Phase 2 / Phase 3	Phase 4
	Planning	Data Gathering Activities	Assessment & Gap Analysis	Implementation & Remediation
Activities	▪ Analysis of how and why CCPA applies to your Business ▪ Draft Project Work Plan ▪ Review existing data inventories / maps for CCPA relevancy ▪ Develop interview questionnaire ▪ Identify preliminary set of questionnaires recipients and other stakeholders ▪ Schedule stakeholder meetings (in person or by phone)	▪ Conduct data mapping ▪ Submit and get responses to questionnaires ▪ Identify all vendors and third-parties that receive data and contracts for each ▪ Collect existing policies, procedures, and practices ▪ Commence onsite visits and / or stakeholder telephone interviews	▪ Cross- reference statutory requirements to current policies, procedures, and practices ▪ Assess vendor contracts ▪ Perform gap analysis ▪ Prepare Compliance & Risk Report ▪ Develop prioritized remediation plan ▪ Create an action plan and supporting documentation	▪ Update and develop new processes ▪ Update and draft new policies and procedures ▪ Update disclosures and consent documents ▪ Revise and/or put in place vendor contracts
Deliverables	1. **Meeting Materials & Work Plan** 2. **Interview questionnaire** 3. **Stakeholder interview schedule** 4. **Weekly Status Meetings and Reporting Template**	1. **Complete data map** 2. **Format gap analysis questionnaires** 3. **Stakeholder Interview Notes**	1. **Compliance-Readiness Findings** 2. **Gap Analysis Results** 3. **Compliance & Risk Report** 4. **Remediation and Action Plans**	1. **Same as above**

GDPR - Applicability

Applies to organizations which:

- Are established in the EU (i.e have offices, servers or employees in the EU);
- Offer goods and services to individuals in the EU (or to clients/customers which do so); OR
- Monitor the behavior of individuals in the EU (as a core part of their business).

Applies to “controllers” and “processors.”

- Controller – decides how and why personal information is processed. Includes HIPAA covered entities.
- Processor – processes personal information on behalf of a controller.

GDPR - Principles

Key principles:

- Lawful basis to process personal information
- Transparency
- Rights of individuals (access, correction, portability and erasure)
- Contractual flow down of obligations from Controller to Processor
- Security
- Breach notification

Fines can be substantial:

- Greater of EURO20million (approx. $23million) or 4% of global revenue.
- Portuguese hospital fined $455,000 for failing to properly secure access to patient personal information.

GDPR - Questions

Does GDPR apply to my organization?

YES – if you have facilities physically located in the EU

YES – if you advertise services to individuals in the EU, use country specific website domains (.fr, .eu, .uk), offer payment in EUROs or GBP.

Yes – if you monitor the behavior of individuals in the EU (i.e monitoring of medical device information).

YES – if you perform services on behalf of an EU company which involve storing, accessing, anonymizing, deleting, or otherwise using personal information.

NO – if you just provide medical treatment for people from the EU whilst they are visiting the US

NO – if you are a US company and one of your employees visits the EU on vacation

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
  - 64 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 5 civil money penalties

As of October 15, 2019

Notice of Enforcement Discretion

Regarding HIPAA Civil Money Penalties

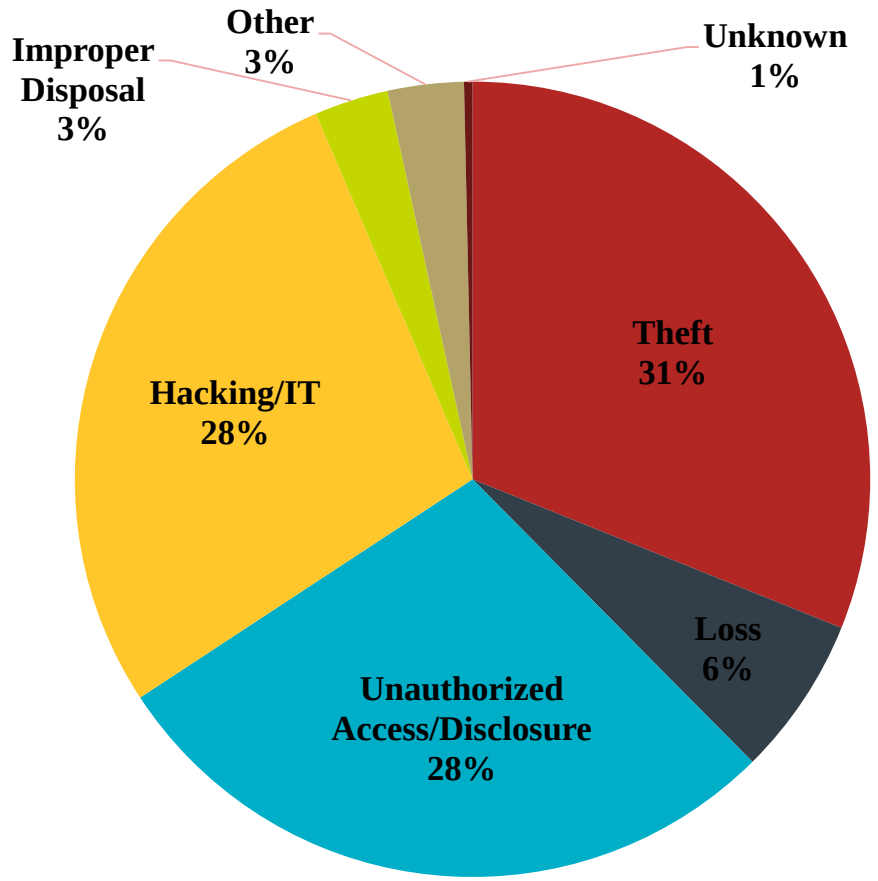
Announced April 26, 2019

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

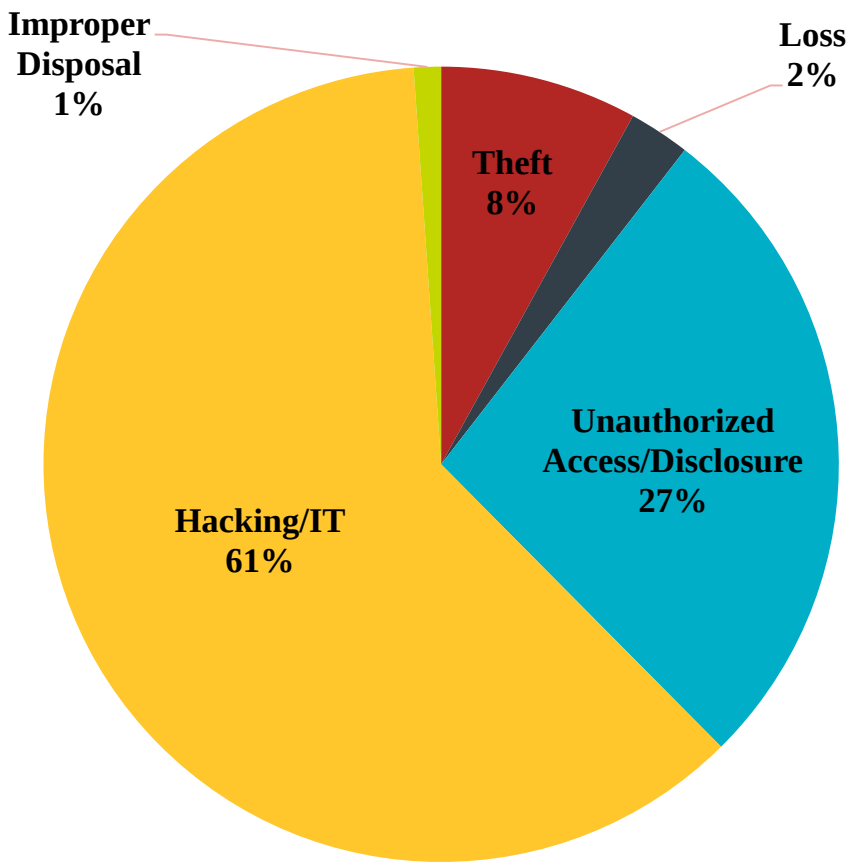
https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties

*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.

Breach Update
500+ Breaches by Type of Breach

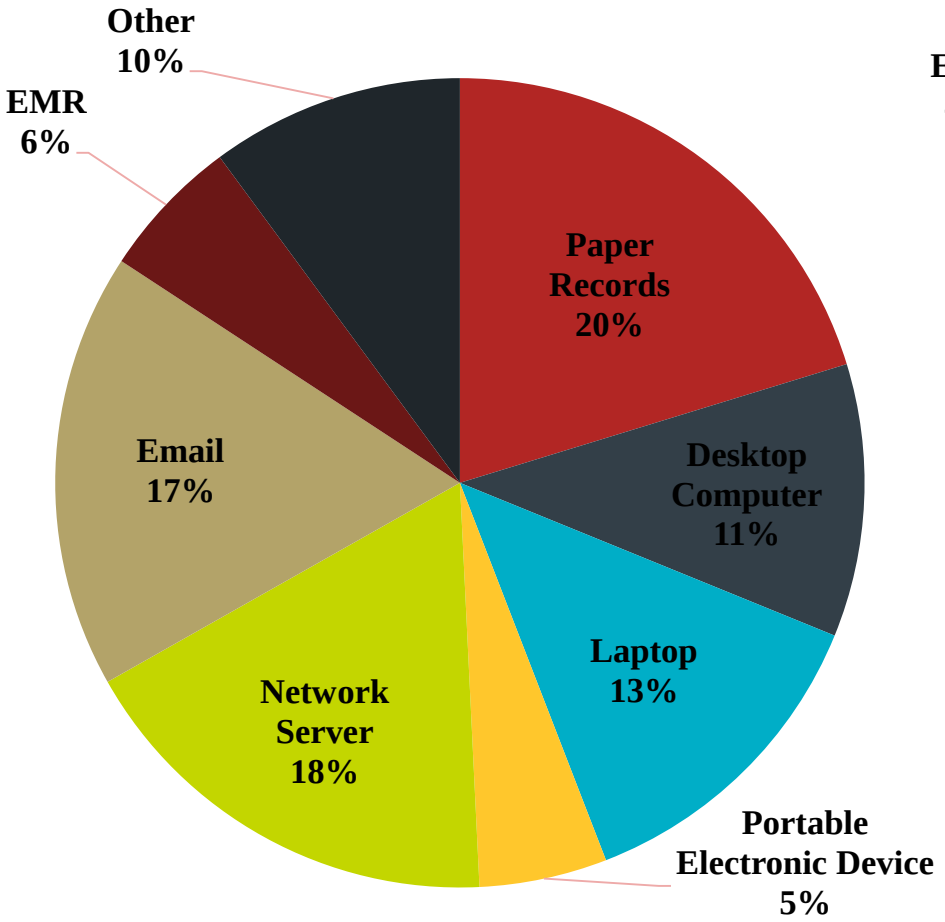


Sept 23, 2009 through September 30, 2019

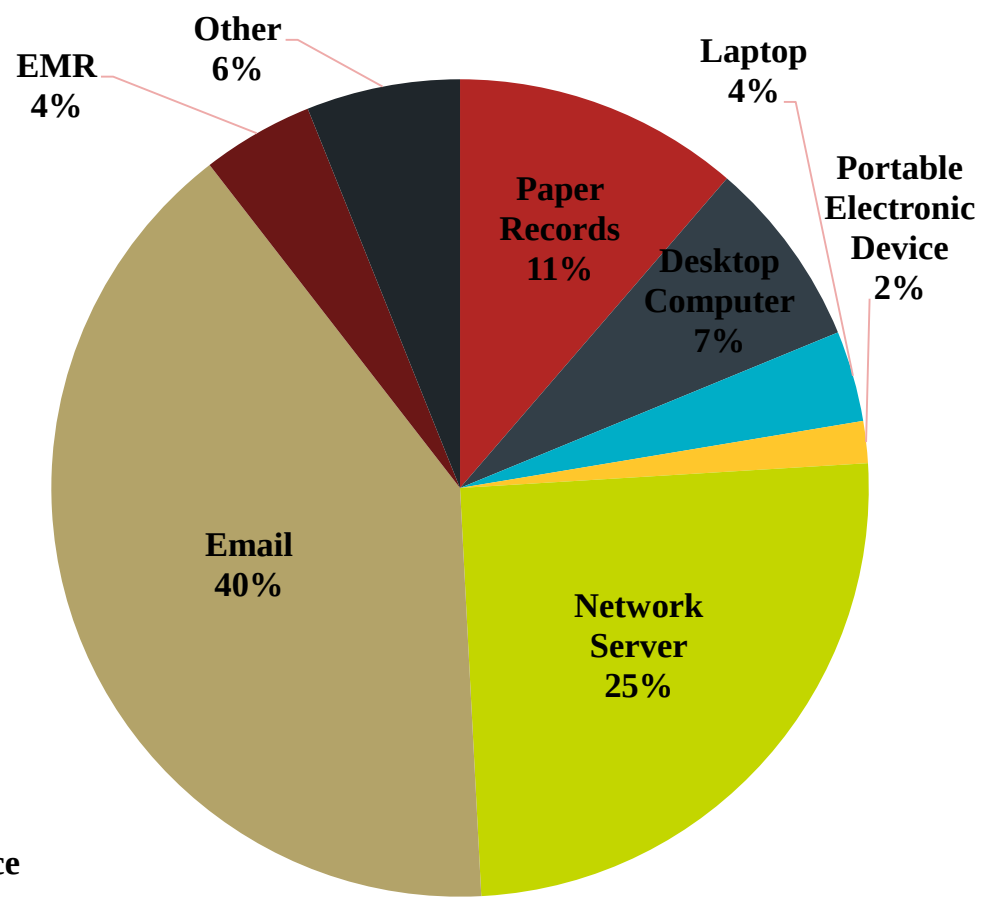


Jan 1, 2019 through September 30, 2019

Breach Update
500+ Breaches by Location of Breach



Sept 23, 2009 through September 30, 2019



Jan 1, 2019 through September 30, 2019

Recent Enforcement Actions

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
9/2019	Elite Dental	$10,000
10/2019	Jackson Health System	$2,154,000

Disclosure and Safeguards

Impermissible Disclosure and Safeguards

- 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. See 45 C.F.R. § 164.502(a)
- A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c).

Risk Analysis/Risk Assessment

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).

Recent Settlement: Medical Informatics Engineering

- Breach report received through breach portal
- Hackers used user ID and password to get ePHI of 3.5 million people
  - Including names, addresses, DOB, SSN, email addresses, clinical information and health insurance information
- Included information held by subsidiary - NoMoreClipboard
- Impermissible disclosure to hackers
- No comprehensive risk analysis
- $100,000 settlement
- 2 year corrective action plan

Recent State AG Settlement: Medical Informatics Engineering

- 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.

Recent Settlement: Anthem

- 78.8m individuals affected
  - Largest health data breach in U.S.
- Gained access through spear fishing in Feb. 2014
- Data extracted from Dec. 2014 to Jan. 2015
  - Included names, addresses, dates of birth, email addresses, SSNs, medical ID numbers and employment information
- Issues with risk analysis, information system activity review, security incident response and reporting, and access controls
- 2 other settlements –
  - National Association of Insurance Commissioners (December 2016)
  - Class Action (August 2018)

Recent CMP: Jackson Health System

- $2,154,000 civil money penalty
- 3 investigations
  - Paper Records
  - Media acquisition of PHI
  - Employee theft of PHI
- 3 violations
  - Breach Notification to the Secretary
  - Risk Analysis
  - Information Access Management

Recent Settlement: Elite Dental

- Originated as a complaint
- PHI discussed on Yelp Review page
  - Last name
  - Treatment plan
  - Insurance
  - Treatment cost
- Review found multiple patients' PHI discussed on Yelp Review page
- Failed to implement policies and procedures with respect to PHI
- Notice of Privacy Practices also deficient
- $10,000 settlement
- 2 year corrective action plan

Recent Settlement: Bayfront St. Petersburg

Privacy Rule Right of Access Requests

- [An] individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set…. See 45 C.F.R. §164.524(a)(1).
- [T]he covered entity must act on a request for access no later than 30 days after receipt of the request.... See 45 C.F.R. §164.524(b)(2).
- Includes the right to inspect records. 45 C.F.R. §164.524(b)(1).
- The provision of access must be provided in the form and format requested. 45 C.F.R. §164.524(c)(2).
- Can be directed to a person designated by the individual at the individual's signed written request. See 45 C.F.R. §164.524(c)(3).
- Only reasonable, cost-based fees may be assessed. See 45 C.F.R. §164.524(c)(4).
- OCR Right of Access guidance – www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Recent Settlement: Bayfront St. Petersburg

1st Right of Access Initiative case

- Originated as a Complaint
- Records requested related to child's birth
- October 2017- 2 requests due to confusion about which designated record set contained the requested information
  - Immediately corrected by Complainant
- January and February 2018 – attorney requested records
- March 2018 – partial records delivered to attorney
- August 2018 – full records delivered to attorney
- February 2019 – full records delivered to Complainant
- $85,000 settlement
- 1 year corrective action plan

Recent State AG Settlement: Premera

- As a result of an Attorney General's Office investigation, Premera Blue Cross will pay $10 million nationwide for "failing to secure sensitive consumer data and for misleading consumers before and after a data breach affecting millions across the country."
- Attorney General Bob Ferguson led a coalition of 30 state attorneys general investigating the company's practices.
- The data breach affected the information of more than 10.4 million individuals nationwide, including more than 6.4 million Washingtonians.
- Under the consent decree, Premera will pay $5.4 million of the total recovery to the Washington State Attorney General's Office, which will go towards continued enforcement of state data security and privacy laws, and nearly $4.6 million to the coalition of states that joined Ferguson's legal action.
- The consent decree also legally requires Premera to implement specific data security controls to protect personal health information, annually review its security practices and provide data security reports to the Washington State Attorney General's Office.
- https://www.atg.wa.gov/news/news-releases/attorney-general-ferguson-s-investigation-premera-data-breach-results-premera

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

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

Feel free to contact me for more information:

Iliana Peters:
ipeters@polsinelli.com

Polsinelli PC 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.

POLSINELLI

polsinelli.com