HEALTH INFORMATION DATA BREACHES

RISKS, REGULATIONS, AND PROTECTING YOUR DATA

THORA JOHNSON
Partner
Cyber, Privacy, and Data Innovation
Orrick, Herrington & Sutcliffe

JENNY BARNES
Vice President, Legal and Privacy Officer
Quantum Health

SAORI KAJI
Senior Product and Privacy Counsel
NVIDIA

KAYE CYRUS
Corporate Counsel and Privacy Officer
HealthEdge

March 25, 2022

orrick

Agenda

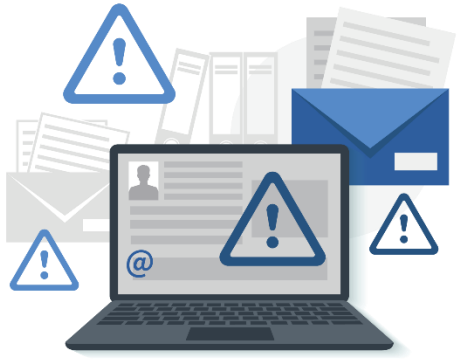
- The Legal Framework
- The Risk Landscape and Enforcement Trends
- Panel Discussion

THE LEGAL FRAMEWORK

U.S. "Cybersecurity Law"

Laws imposing civil or criminal liability for hacking

Laws requiring reasonable investigation and implementation of security measures



Laws requiring notification of security breaches

Contractual duties for security and/or breach notification

Regulator enforcement consent decrees and related requirements

Regulator and industry standards, guidelines, and frameworks

Sources of U.S. Notice Obligations for Health Data

Health Insurance Portability and Accountability Act (HIPAA) and state law equivalents

The FTC Health Breach Notification Rule for non-HIPAA covered health data

U.S. state breach notification laws

(Often carves out HIPAA-covered data or entities)

Breach Notification Obligations

Contracts that an entity has signed agreeing to notify of incidents within a certain timeline

(e.g., BAAs)

U.S. state insurance laws

(e.g., NYDFS)

HIPAA

Office for Civil Rights

Applies to protected health information (PHI) in the hands of Covered Entities and their Business Associates.

Privacy Rule

- Privacy Officer
- Written HIPAA Policies and Procedures, including permitted uses and disclosures, individual rights (access, amendment, accounting, restriction, alternative comms), complaint process and sanctions policy
- Notice of Privacy Practices (for covered entities)
- Training
- Maintenance of (Up and) Downstream Business Associate Agreements

Security Rule

- Covered Entities and Business Associates must ensure confidentiality, integrity, and security of ePHI and protect against reasonably anticipated threats by conducting periodic risk assessments.

Breach Notification Rule

- Covered Entities must notify individuals, HHS Office for Civil Rights, and prominent media outlets (if 500 or more individuals in one state or jurisdiction) following discovery of a breach of unsecured PHI.
- Business Associates must notify their Covered Entities

FTC Health Breach Notification Rule

Applies to non-HIPAA entities – vendors of Personal Health Records and PHR – Related Entities, including health apps, connected devices, and similar products.

Trigger

- Acquisition of unsecure PHR, identifiable health information caused by
- Cybersecurity intrusion
- Unauthorized disclosure of sensitive information

Breach Notification

- Must notify individuals, FTC (if over 500 individuals, within 10 business days), and in some cases, the media

Enforcement

- Restored Vigor
- New guidance
- To date, only 5 – most recent dates back to Oct. 2020

U.S. State Breach Notification Laws

All **50 states** have state breach notification laws

Applies to personal information which is defined as name combined with SSN, driver's license or state ID, account numbers, etc. Some states include medical and health insurance information in the definition of personal information.

Trigger

- A "breach of security" is defined as unauthorized acquisition / access / loss / use of PI that compromises the confidentiality, integrity or security of data.

Breach Notification

- States have various timeframes for notifying Attorney Generals or other regulators and individuals
  - Some states include specific content requirements for notifications
  - Some states also require companies to provide credit monitoring to individuals with affected personal information
- Some states have reporting exemptions for HIPAA-regulated entities.

Enforcement

- AGs can investigate incidents. The typical outcome of these investigations is a consent decree with requirements related to reasonable security measures.

NYDFS Cybersecurity Regulation (23 NYCRR 500)

Applies to any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Insurance, Banking, or Financial Services Laws.

Trigger

- Any act or attempt, successful or unsuccessful, to gain unauthorized access to disrupt or misuse an Information System or information stored on such Information System that either:
  - (1) requires notice to any government body, self-regulatory agency or any other supervisory body; OR
  - (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity

Breach Notification

- Covered entities must notify NYDFS no later than 72 hours from determination that a cybersecurity event has occurred

Enforcement

- Aggressive enforcement: In 2021, NYDFS settled with three companies for violations of cybersecurity requirements for $1.5M, 1.8M, and $3M, respectively

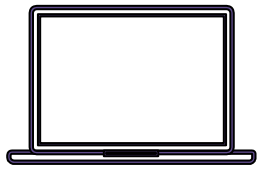
Additional Regulators

- **State Departments of Insurance**
  - Many states have breach notification laws that are specific to entities regulated by state departments of insurance
- **Securities and Exchange Commission**
  - Disclosure of material cybersecurity incidents
  - Proposed periodic disclosure of cybersecurity risk management, strategy, and governance

THE RISK LANDSCAPE AND ENFORCEMENT TRENDS

Trends in Health-Related Cybersecurity Events

The following trends emerged in 2021:



INITIAL ATTACK VECTOR

Compromised credentials were responsible for 20% of breaches across all industries, followed by phishing, cloud misconfiguration, vulnerabilities in third party software, and business email compromise

HEALTHCARE HAD THE HIGHEST INDUSTRY BREACH COSTS

Healthcare data breach costs increased from an average of $7.13 million to $9.23 million, a 29.5% increase from 2020

ENCRYPTION

The use of strong encryption was a top mitigating factor to reduce breach cost

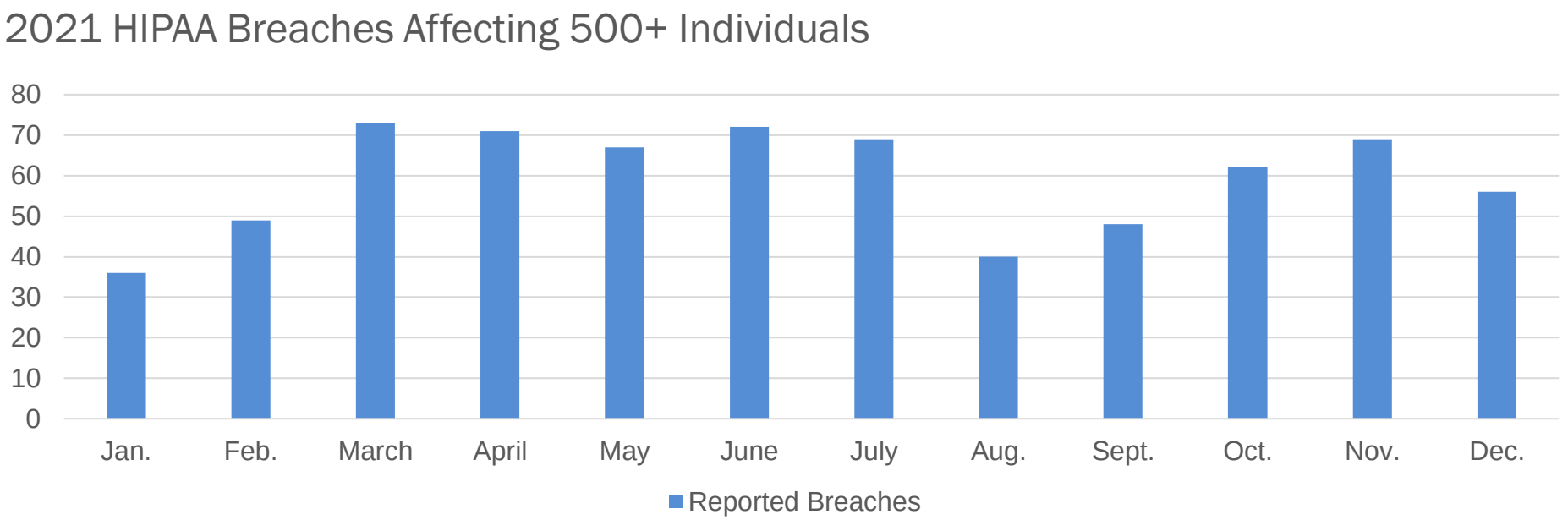
REGULATORY COMPLIANCE FAILURES

Failure to comply with regulatory requirements amplified average cost of a breach

See IBM, *Cost of a Data Breach Report 2021*, https://www.ibm.com/security/data-breach.

2021 OCR Breach Statistics

- In 2021, a total of 714 breaches affecting 500 or more individuals were reported to OCR
  - This is an average of 59 data breaches each month and represents a 10.9% increase in the number of reported data breaches from the prior year



See HIPAA Journal, *2021 Healthcare Data Breach Report*, https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/.

Trends in FTC Enforcement

- **New Health Breach Notification Rule Policy Statement**
  - Clarified that a breach of security under the Rule is not limited to cybersecurity intrusions, but also includes unauthorized access to covered information including the disclosure of covered information without the individual's authorization.
- **Flo Health, Inc.** (Jan. 2021)
  - Arose from Flo's failure to disclose in its Privacy Policy that it shared users' health information with third parties

Trends in State AG Enforcement

- Increase in State AG enforcement of HIPAA in OCR's place
- Collaboration between AG offices across multiple states

Action Items for Entities Handling Health Data

Determine applicability of the various federal and state laws.	**Advise senior management** on the potential impact of these laws.	Designate a **compliance team** and appoint team leader; schedule regular meetings; and ensure security compliance costs are built into the budget.	Develop a compliance **roadmap** and begin implementation on the new requirements.
Determine whether **software development work** will be required and incorporate into roadmap.	Update **data inventories** to address any repositories of health data.	Identify and update **contracts** to address security obligations.	Review and update **privacy notices** to ensure that all third-party disclosures are adequately disclosed.
Review and revise agreements with **vendors** as needed to ensure appropriate security controls are in place.	Review the organization's current **security** posture, identify potential security enhancements to be implemented, and prepare for cybersecurity audit and risk assessment requirements.	Make applicable **changes to websites, apps, and related online properties** to address new obligations.	Monitor forthcoming **regulations and enforcement actions**.

PANEL DISCUSSION

THORA JOHNSON
Partner
Cyber, Privacy, and Data Innovation
Orrick, Herrington & Sutcliffe

JENNY BARNES
Vice President, Legal and Privacy Officer
Quantum Health

SAORI KAJI
Senior Product and Privacy Counsel
NVIDIA

KAYE CYRUS
Corporate Counsel and Privacy Officer
HealthEdge

orrick


orrick