

The Patchwork of Federal & State Privacy Rules for Health Information

What Providers, Plans, & Vendors Need to Know

29th HIPAA Summit, Mini Summit 6
March 4, 2020

David Holtzman, JD, CIPP/US/G
Executive Advisor
CynergisTek
240.720.1365
david.holtzman@cynergistek.com

Thora Johnson, Esq.
Chair, Healthcare Practice
Venable LLP
410.244.7747
tajohnson@venable.com

Erika Riethmiller, CPHRM, CHC,
CHPC, CISM, CIPP/US
Chief Privacy Officer
University of Colorado Health
303.752.8242
erika.riethmiller@uchealth.org

State Data Protection Laws

- Trend in new state laws setting standards for data protection of PII
- Require organizations to have in place reasonable security safeguards
- States setting their own standards to define reasonable security
- No national standard defining reasonable security leading to patchwork of standards
 - NY SHIELD Law
 - Oregon Consumer Information Protection Act
 - Consumer protection standards outlawing deceptive and unfair trade practices

What is Reasonable Security?

Administrative

- Security official
- Risk based management of security
- Training
- Vendor security management

Technical

- Assess risk in network design, information processing, and Storage
- Detect, prevent, and respond to attacks and system failures
- Regular testing and monitoring

Physical

- Assess risk of information storage and disposal
- Detect, prevent, and respond to intrusions
- Protect against unauthorized access or use of PII



**Secure disposal of PII or storage media after its no longer needed

NJ AG Example of Aggressive Enforcement


- NJ AG fined medical group \$418,000 for 2016 breach involving BA
- Medical transcription vendor misconfigured the medical group's FTP server that exposed PHI of 1,600 patients on Internet
- AG's investigation found that:
 - The vendor failed to notify the medical group of the incident resulting in failure to timely notify impacted individuals and the state of the breach
 - Medical group failed to exercise appropriate oversight of the vendor's security practices in safeguarding PHI

<https://nj.gov/oag/newsreleases18/Virtua-Medical-Group-Consent-Judgment.pdf>

What is CCPA?

- Gives California consumers certain rights with respect to their personal information.
- A consumer is defined broadly to include employees/families, prospective customers contacting a covered entity through their job, and applicants for employment.
- Applies to **for-profit** businesses with California presence that:
 - Have gross revenue in excess of \$25 million;
 - Buy, receive, sell, or share for commercial purposes the personal information of 50,000+ California consumers, households, or devices; or
 - Derive 50% or more of its revenues from selling personal information.

4 Basic Consumer Rights



Right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom

Right to “opt out” of allowing a business to sell their personal information to third parties

Right to have a business delete their personal information

Right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act

HIPAA

- Covered Entities: (1) a health plan (2) healthcare clearing house, or (3) healthcare provider that transmits health information in electronic form to another party to carry out financial or administrative activities related to healthcare.
- Privacy Rule: Most uses and disclosures of protected health information (PHI)- other than those for treatment, payment of treatment, and health care operations-must be authorized by the patient/Enrollee
- Security Rule: Covered entities must “protect against reasonably anticipated threats and vulnerabilities ” that compromise e-PHI in ways that are not permitted by the Privacy Rule
- Breach Notification: Obligation to assess incidents of unauthorized uses and disclosures of unsecured PHI to determine probability of compromise to the data and make notifications to individuals, government or the media within 60 days when a breach has been discovered

CMIA

- **Scope:** Individually identifiable information is medical information that includes or contains any element of personal identifying information such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
- **Privacy:** Subject to specified exceptions, disclosure of covered information must be authorized by the patient, enrollee, or subscriber.
- **Enforcement:** California Department of Public Health
- **Private Right of Action**
 - Unauthorized disclosure or use of records.
 - Negligent release of records—it is not necessary to demonstrate that plaintiff suffered actual damages.

Health Care Largely Exempt



HIPAA COVERED
ENTITIES



ENTITIES
COVERED BY
CALIFORNIA
HEALTH CARE
PRIVACY LAW
(CMIA)



BUSINESS
ASSOCIATES FOR
ACTIVITIES
COVERED BY
HIPAA







NON-HIPAA
COVERED PII
HELD BY A
COVERED ENTITY
SAFEGUARDED
TO SAME EXTENT
AS PHI

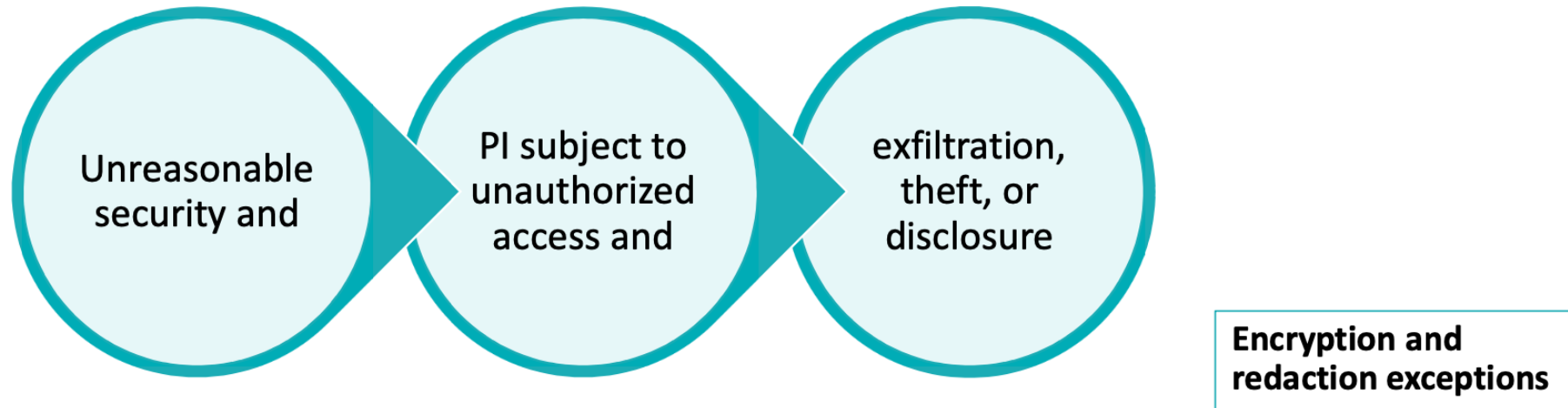


UNDERSTANDING
OF IMPACT IS
EVOLVING

Individual Rights Comparison

	Access	Portability	Erasure	Amend/Correct	Complaint	Restrict Processing	Opt-In/Consent	Private Right of Action
 CCPA	✓	✓	✓			✓	✓	✓
 CMIA	✓	✓					✓	✓
 HIPAA	✓	✓		✓	✓	✓	✓	
 GDPR	✓	✓	✓	✓	✓	✓	✓	

CCPA Private Right of Action



Different definition of personal information for this section, limited to individual's first name/initial, plus last name, plus:

Social security number	Driver's license or state identification card number	Financial account number, credit or debit card number in combination with access code	Medical information	Health insurance information
-------------------------------	---	--	----------------------------	-------------------------------------

Private Right of Action

Limited Opportunity to Cure

Prior to lawsuit for statutory damages, consumers must provide written notice of specific violations

Defendant then has 30 days to cure

No notice required for an action for actual pecuniary damages

Remedies

Statutory damages of \$100–\$750 per consumer, per incident, or actual damages (whichever is higher)

Injunctive or declaratory relief

Any other relief the court finds appropriate

Federal Activity Ramping Up?

- Data sharing, Interoperability, and Donations for Cybersecurity
 - Breaking down siloed health data with permissive or required data sharing putting the consumer at the center
 - Potential for revised HIPAA Privacy Rule and 42 CFR Part 2 regulations to further sharing for patient care and response to opioid epidemic
 - Look to guidance documents for agencies that share responsibility for data use and protection standards
 - Information Blocking and Interoperability regulations will
 - Require entities that maintain personal information in treatment & payment for health care provide patients access to information
 - Patient and authorized 3rd party access to PII through APIs
 - Revise conditions of participation for hospitals to include electronic notice of admissions, transfers and discharges
 - Prohibition on Information Blocking (21st Century Cures Act)
 - Stark revisions to permit donations of services and hardware to bolster cybersecurity safeguards

Operational Challenges

- Data Classification Enhancements/Re-evaluations
- Data Inventory and Mapping
- Records Retention
- Consumer Right of Access and Deletion Requests; Data Portability
- Privacy Notice reviews/updates and key decisions associated with them
- Technology/tools and other resources necessary to comply ensuring adequate privacy choice mechanisms/consent and preference platforms
- Authentication Protocols
- Reviewing vendors to ensure sufficient access, deletion and incident response provisions

The Future of Privacy



States will continue to expand data protection and consumer privacy standards for health information outside of HIPAA



Will Congress be able to agree on a federal privacy and data protection standard?



Healthcare marketplace changes will drive increasing demand by ever larger organizations needing to assess and comply with HIPAA and state privacy standards



CMS will seek to force providers to give patients access to treatment records in real-time and prohibit EHR information blocking



Questions?

David Holtzman

david.holtzman@cynergistek.com

Thora Johnson

tajohnson@venable.com

Erika Riethmiller

erika.riethmiller@uchealth.org