



# The New Health Privacy and Security

**January 16, 2020**

*Presenters:*

Thora Johnson

Jami Mills Vibbert

Shannon Yavorsky

**VENABLE** LLP

# Agenda

Regulatory  
Landscape

CCPA - HIPAA  
and the CMIA

Reasonable  
Security and IoT

Data Sharing,  
Interoperability,  
and More

Key  
Takeaways

# Regulatory Landscape

- Time of focus and change on both federal and state levels
- Federal level, including:
  - New proposed HIPAA regulations
  - New Part 2 regulations regarding SUD
  - Finalized interoperability regulations expected
  - New federal privacy law?
- State level, including
  - California Consumer Privacy Act
  - New York SHIELD Act
  - Texas Medical Records Privacy Act
  - More to come?

# Scope of CCPA

Any company that does business in California and meets one or more of these standards:

Annual gross revenue over \$25 million

Collects or shares personal information annually from 50,000 consumers, households, or devices

Derives at least 50% of annual revenue from sale of personal information

Plus any entity that controls or is controlled by a business and that shares common branding

Control = power to exercise a controlling influence over the management of a company and

Common Branding = shared name, service mark, or trademark

# CCPA Key Requirements

- Consumer right to request certain information about practices, *and specific pieces of personal information*
- Consumer right to request deletion of personal information, with some exceptions
- Consumer right to opt out of “sales” of personal information
  - “Do Not Sell My Personal Information” link and webpage
- Business must not discriminate against consumers who exercise rights
- Implementation requirements

# Implementing Consumer Rights

- Must provide at least a toll-free telephone number and a web portal
- Must provide consumers reason for not taking action
- Must provide information, free of charge, and generally within 45 days of receipt
- May charge a reasonable fee or refuse to act on repetitious, "manifestly unfounded or excessive" requests
- Must train employees who handle consumer inquiries
- Cannot require consumers to create an account to exercise their rights

# Health Insurance Portability and Accountability Act (HIPAA)





- **Covered Entities:** (1) A health plan, (2) a healthcare clearing house, or (3) a healthcare provider that transmits any 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 disclosures for treatment, payment for treatment, and healthcare operations – must be authorized by the patient/participant.
- **Security Rule:** Covered entities must “protect against reasonably anticipated threats or hazards to the security or integrity of such information” and “protect against reasonably anticipated” uses and disclosures that are not permitted under the Privacy Rule.
- **Security Breach Notification:** 60 days to notify affected individuals of a security breach affecting their unencrypted PHI.

# Confidentiality of Medical Information Act (CMIA)

- **Scope:** “Individually identifiable information” means 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.
- **Confidentiality:** Subject to specified exceptions, confidentiality of the medical information must be preserved.
- **Private Rights of Action**
  - Unauthorized disclosure or use of records.
  - Negligent release of records – it is not necessary that the plaintiff suffered actual damages.



# Individual Rights Comparison

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

# HIPAA and CMIA Carve-Outs from the CCPA

- **Information Carve-Out**

- HIPAA: All “protected health information” (PHI) collected by “covered entities” and “business associates” subject to HIPAA is exempted from the CCPA.
- CMIA: All “medical information” subject to the CMIA is exempted from the CCPA.
- Research and safety data?

- **Entities Carve-Out**

- HIPAA: Other patient information (i.e., non-PHI) that is maintained by a covered entity is also exempted from the CCPA to the extent the covered entity maintains that “patient information” in the same manner as PHI.
  - “Patient information” is not defined.
  - “Business associates” are not expressly exempted.
- CMIA: A “provider of healthcare” covered by the CMIA is exempted from the CCPA to the extent the provider maintains “patient information” in the same manner as “medical information.”
  - “Patient information” is not defined.

# The Scope of the Entity Carve-Out Is Not Clear

- The entity carve-out ostensibly exempts the entire entity as long as the entity maintains all personal information in compliance with what HIPAA and the CMIA require.
- However, the language of the carve-out creates a risk that certain buckets of personal information (e.g., non-patient information) will fall outside the carve-out and trigger CCPA protection.
  - The language of the carve-out uses the term “patient information,” which may limit the scope of the carve-out.
  - “Business associates” are not expressly carved out.

# Key Risks Under the CCPA

- California Attorney General may read the carve-outs narrowly and bring enforcement actions to bring entities in line with the CCPA.
- Private Right of Action: In the event of unauthorized access to personal information, private individuals may sue under the CCPA.

# Attorney General Enforcement



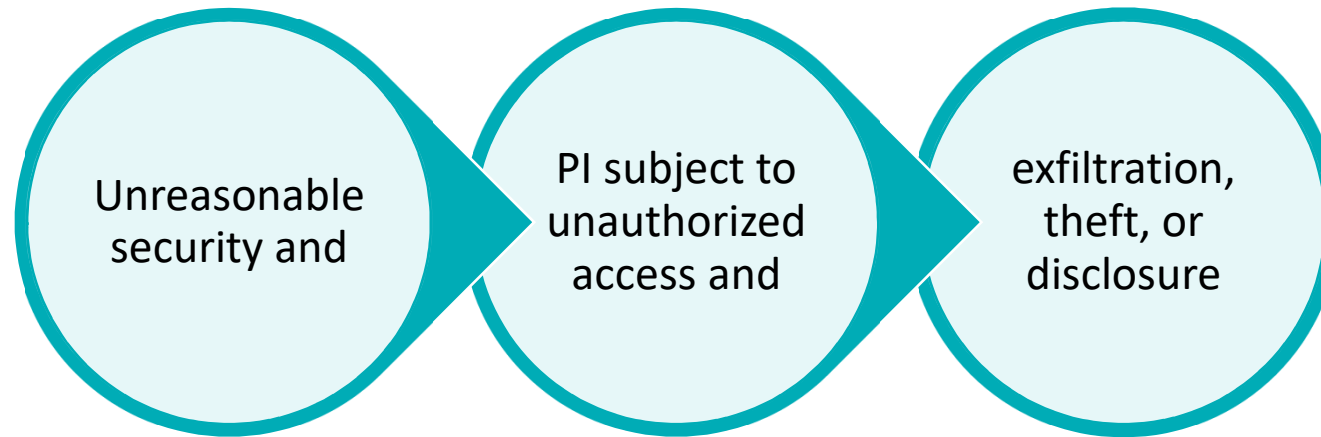
## California Attorney General enforcement

- Businesses have a 30-day cure period after being notified.
- Can seek an injunction plus civil penalties of up to \$2,500 per violation and up to \$7,500 per intentional violation

## Considerations

- No cap on civil penalties.
- Attorney General is incentivized to seek enforcement – penalties and settlement proceeds placed in state fund.
- Attorney General has urged expanded private right of action.
- No liability for CCPA violations of service providers, or other entities that receive personal information under specific contract restrictions, as long as company did not have "actual knowledge...or reason to believe...that the person intends to commit such a violation."

# What About Security? CCPA Private Right of Action



**Encryption and redaction exceptions**

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

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

# 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

# Reasonable Security

- States
  - Breach notification laws
  - “Reasonable security” procedures, guidelines, and laws
  - Unfair and deceptive acts laws
  - Specific requirements
    - New York SHIELD Act
  - Internet of Things “reasonable security”



# Risk Management Recommendations for Health Data Entities

- Conduct a security risk assessment
  - Assess security measures to confirm compliance with HIPAA security rule and whether the security measures are “reasonable” under the CCPA.
- Maintain all personal information in compliance with CCPA, HIPAA, and/or CMIA requirements.
- Prepare 30-day cure plan in the event the Attorney General provides notice of non-compliance with the CCPA.

# Data Sharing, Interoperability, and More

- Breaking down siloed health data with required and encouraged data sharing and putting the consumer at the center.
- Potentially new HIPAA and Part 2 regulations to permit greater sharing to further patient care and combat the opioid epidemic.
- More guidance documents, such as FERPA and HIPAA.
- OCR enforcement actions focused on access rights.
- Interoperability regulations will
  - Require APIs
  - May revise conditions of participation for hospitals to include electronic notice of admissions, transfers, and discharges
  - Prohibit “information blocking”

# Key Takeaways

- More data sharing required and encouraged
- More individual rights
- Need to identify applicable regimes to various categories of data
- Continued importance of security risk assessments
- Privacy and security as a competitive edge
- Continued government enforcement
- Data litigation on the rise
- No time to be complacent – change is constant

# Thank You



**Thora Johnson**

Partner

+1 410.244.7747

[tajohnson@Venable.com](mailto:tajohnson@Venable.com)



**Jami Vibbert**

Partner

+1 212.370.6288

[jvibbert@Venable.com](mailto:jvibbert@Venable.com)



**Shannon Yavorsky**

Partner

+1 415.343.4486

[skyavorsky@Venable.com](mailto:skyavorsky@Venable.com)



© 2020 Venable LLP.

This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address.

**VENABLE** LLP