HEALTH DATA

NAVIGATING THE LATEST STATE AND FEDERAL TRENDS IN PRIVACY AND CYBERSECURITY ENFORCEMENT

10/25/2024

orrick

Agenda

- State Consumer Privacy Laws
- HIPAA, Part 2, and CMIA
- Overview of Consumer Health Privacy Laws
- FTC Act and FTC's Health Breach Notification Rule
- Looking Forward

Comprehensive U.S. Consumer Privacy Laws

While federal privacy legislative efforts continue to stall, twenty **U.S. states have passed** comprehensive privacy laws:

- **California** (eff. Jan. 1, 2023) – California Privacy Rights Act (amends CCPA)
- **Virginia** (eff. Jan. 1, 2023) – Virginia Consumer Data Protection Act
- **Colorado** (eff. July 1, 2023) – Colorado Privacy Act
- **Connecticut** (eff. July 1, 2023) – Connecticut Data Privacy Act
- **Utah** (eff. Dec. 31, 2023) – Utah Consumer Privacy Act
- **Florida** (eff. July 1, 2024) – Florida Digital Bill of Rights
- **Oregon** (eff. July 1, 2024) – Oregon Consumer Privacy Act
- **Texas** (eff. July 1, 2024) – Texas Data Privacy and Security Act
- **Montana** (eff. Oct. 1, 2024) – Montana Consumer Data Privacy Act
- **Delaware** (eff. Jan. 1, 2025) – Delaware Personal Data Privacy Act
- **Iowa** (eff. Jan. 1, 2025) – Iowa Consumer Data Protection Act
- **Nebraska** (eff. Jan. 1, 2025) – Nebraska Data Privacy Act
- **New Hampshire** (eff. Jan. 1, 2025) – New Hampshire Privacy Act
- **New Jersey** (eff. Jan. 15, 2025) – New Jersey Data Privacy Act
- **Tennessee** (eff. July 1, 2025) – Tennessee Information Protection Act
- **Minnesota** (eff. Jul. 31, 2025) – Minnesota Consumer Data Privacy Act
- **Maryland** (eff. Oct. 1, 2025) – Maryland Online Data Privacy Act
- **Indiana** (eff. Jan 1, 2026) – Indiana Consumer Data Protection Act
- **Kentucky** (eff. Jan. 1, 2026) – Kentucky Consumer Data Protection Act
- **Rhode Island** (eff. Jan 1, 2026) – Rhode Island Data Transparency and Privacy Protection Act

Protected Sensitive Information

California	Virginia	Colorado	Connecticut	Utah
• SSN; Driver's License #; State ID #; Passport # • Account Log in or # Plus PW (including Credit or Debit Card) • Precise Geolocation • Race/Ethnicity • Religious/Philosophical Beliefs • Union Membership • Non-Recipient Message Content • **Genetic Data** • **Biometric Data** • **Health Data** • Sexual Orientation or Sex Life	• Race/Ethnicity • Religious Beliefs • **Mental/Physical Health Diagnosis** • Sexual Orientation • Citizenship/Immigration Status • **Genetic Data** • **Biometric Data** • Data About a Known Child < 13 • Precise Geolocation Data	• Race/Ethnicity • Religious Beliefs • **Mental/Physical Health Condition or Diagnosis** • Sexual Orientation or Sex Life • Citizenship/ Citizenship Status • **Genetic Data** • **Biometric Data** • Data About a Known Child < 13 • Biological data • Neural data	• Race/Ethnicity • Religious Beliefs • **Mental/Physical Health Condition or Diagnosis** • Sexual Orientation or Sex Life • Citizenship/ Immigration Status • **Genetic Data** • **Biometric Data** • **Consumer Health Data** • Data About a Known Child < 13 • Precise Geolocation Data • Status as victim of a crime	• Race/Ethnicity • Religious Beliefs • **Medical History** • **Mental/Physical Health Condition/ Treatment/Diagnosis** • Sexual Orientation • Citizenship/ Immigration Status • **Genetic Data** • **Biometric Data** • Specific Geolocation Data

HIPAA (and Health Data) Exemptions

California	Virginia	Colorado	Connecticut	Utah
• **Data Level Exemption** • Exempts protected health information ("PHI") collected by a covered entity or business associate governed by HIPAA. • Exempts covered entities, to the extent the covered entity maintains patient information in the same manner as PHI. • Clinical trial personal information subject to the Common Rule. • Does not expire.	• **Data & Entity Level Exemption** • Exempts covered entities and business associates subject to HIPAA, as well as PHI. • Also exempts certain other patient and health-care related information. • Does not expire.	• **Data Level Exemption** • Exempts PHI collected, stored, and processed by a covered entity or its business associates. • Exempts information and documents created by a covered entity for purposes of complying with HIPAA and its implementing regulations. • Exempts information maintained in the same manner as PHI by a covered entity or business associate, as well as certain other health-related information. • Does not expire.	• **Data & Entity Level Exemption** • Exempts covered entities and business associates subject to HIPAA, as well as PHI. • Also exempts certain other patient and health-care related information. • Does not expire.	• **Data & Entity Level Exemption** • Exempts covered entities and business associates subject to HIPAA, as well as PHI. • Also exempts certain other patient and health-care related information. • Does not expire.

Virginia, Connecticut, and Utah exempt covered entities and business associates in their entirety.

AG Enforcement/Private Right of Action

- Attorneys General have power to enforce state privacy laws
- Civil penalties for violations of comprehensive state privacy laws
  - $2,500 per violation under CPRA, $7,500 per intentional violation
  - $7,500 per violation for VCPDA
- CPRA also has limited private right of action
- Multiple states can investigate the same activity under their own state laws, leading to companies facing numerous CIDs

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

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.

HIPAA Privacy Rule – Reproductive Health Regulations

- In April 2024, the Office for Civil Rights (OCR) in the Department of Health and Human Services (HHS) issued a Notice of Final Rulemaking modifying the HIPAA Privacy Rule to strengthen reproductive health privacy.
- The Final Rule prohibits the use or disclosure of PHI by a regulated entity to:
    - Conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care;
    - Impose criminal, civil, or administrative liability on a person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; and
    - Identify any person for the purpose of initiating such investigations or proceedings.

HIPAA Liability

State Attorneys General have HIPAA enforcement authority

Civil Money Penalty

- Calculated by culpability tier and number of violations (see next slide)

Corrective Action Plan

- Develop, maintain, and/or revise HIPAA policies and procedures
- Employee training
- Security Risk Assessment
- Risk Management Plan
- Third-party oversight, auditing, and/or monitoring
- Submit reports to HHS summarizing status of corrective action plan compliance

HIPAA Civil Money Penalties

OCR Enforcement

45 C.F.R. §§ 160.300 – 160.552

Violation Due To:	Penalty Range (Per Violation):
Unknown cause	$137 - $68,928
Reasonable cause and not willful neglect	$1,370 - $68,928
Willful neglect (violation corrected within 30 days)	$13,700 - $68,928
Willful neglect (violation not corrected within 30 days)	At least $50,000

- A $1.5M annual cap applies for violations of an identical privacy or security requirement
- Subject to periodic inflation increases

State AG Enforcement

42 U.S. Code § 1320d–5(d)(2)

- State AGs may assess damages on behalf of state residents by multiplying the number of violations by a maximum of $100 per violation
- A $25,000 cap applies for all violations of an identical privacy or security requirement during a calendar year

California Confidentiality of Medical Information Act (CMIA)

- A mini "HIPAA" law that:
  - Applies to, among others, certain healthcare providers and apps that process "medical information"
    - Medical Information is individually identifiable information in the possession of or derived from a provider of health care, healthcare service plan, pharmaceutical companies, or contractor regarding a patient's medical history, mental health application information, mental or physical condition or treatment.
  - Places safeguards around use and disclosure of medical information
- Note, it does not include a breach reporting requirement but does include a private right of action and provides for statutory damages

California Assembly Bill 352 (AB 352)

- AB 352 amended the CMIA to require certain businesses that electronically store or maintain medical information on the provision of **sensitive services** to enable certain security controls
- Prohibits entities subject to the CMIA from cooperating in an investigation originating from another state by disclosing certain information **related to an individual seeking, obtaining, providing, supporting, or aiding in the performance of an abortion that is lawful under the laws of California to any individual or entity from another state**, unless the disclosure is authorized under specific, enumerated conditions or subject to specific exceptions
- Provides for limitations on user access privileges to systems containing medical information related to gender affirming care, abortion, abortion related services and contraception
- Requires segregation of medical information related to gender affirming care, abortion, abortion-related services and contraception from the rest of a patient's medical record

Consumer Health Data Privacy Laws Overview

- **Three U.S. states** have passed comprehensive consumer health data privacy laws:
  - **Connecticut** (eff. October 1, 2023) – Amendments to Connecticut Data Privacy Act
  - **Washington** (generally eff. March 31, 2024) – My Health My Data Act
  - **Nevada** (eff. March 31, 2024) – Nevada SB 370.
- **Enforcement**: All three laws can be enforced by the state AGs. Washington's law also contains a ***private right of action***.

Applicability and Scope

Regulated Entity

- **Washington / Nevada**: ***Any*** legal entity that:
  - (a) conducts business in the state or targets its products or services to the state's consumers, **and**
  - (b) alone or jointly with others, determines the purposes and means of collecting, processing, sharing, or selling consumer health data.

- **Connecticut**: ***Any*** consumer health data controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

There are NO applicability thresholds for coverage.

Consumer Health Data

- **Washington**: PI that is linked or reasonably linkable to a consumer and that ***identifies the consumer's past, present, or future physical or mental health status***.

- **Nevada**: PI that is linked or reasonably capable of being linked to a consumer and that *a Regulated Entity* ***uses to identify*** the past, present, or future health status of the consumer.

- **Connecticut**: PI that ***a controller uses to identify*** a consumer's physical or mental health condition or diagnosis.

Requirements

- **Health Data Privacy Notice:** Washington and Nevada each require regulated entities to develop and maintain a consumer health data privacy notice.
- **Privacy Rights:** Washington and Nevada require regulated entities to provide right to confirm and access, right to withdraw consent, and right to deletion.
- **Consent Required:** Washington and Nevada require consent before collecting or sharing consumer health data. In Connecticut, the opt-in consent requirements applicable to "sensitive data" apply to "consumer health data."
- **Authorization to Sell:** Under the Nevada and Washington laws, Regulated Entities must obtain valid authorization prior to selling or offering to sell consumer health data. Such authorization must be separate and distinct from the consent to collect or share. Connecticut requires opt-in to collect and process (including share or sell) health data.

FTC Background

- Independent law enforcement agency
- 2-part mandate:
  - Consumer protection
  - Competition
- Privacy and data security are consumer protection priorities
  - Enforcement
  - Policy initiatives
  - Consumer education and business outreach

orrick

FTC Section 5 Powers and Remedies

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices"

- **Deceptive Acts** – representations, omissions, or practices that are likely to mislead consumers
  - Evaluated from the perspective of a reasonable consumer or targeted audience
  - Representation, omission, or practice must be material
- **Unfair Acts** – practice which causes or is likely to cause substantial injury, which is not reasonably avoidable, and not outweighed by countervailing benefits to consumers

Remedies can include:

- $50,120 per violation penalties for violation of Rule or previous consent decree
- Conduct restrictions relating to certain business/marketing practices
- Disgorgement and consumer redress
- Creation of comprehensive compliance program
- 20-year compliance audits and compliance reporting
- Burdensome or awkward consumer notifications

HIPAA & the FTC Act

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

- Section 5 authority extends to both HIPAA and non-HIPAA covered entities
- OCR and FTC enforce sister health breach notification rules
- Joint Guidance (Sept. 2023): Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule
- Joint cases: CVS and Rite Aid

FTC Health Breach Notification Rule (HBNR)

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), and in some cases, the media
- Notifications to individuals, by third party service providers, to the media, and to the FTC should be made no later than 60 calendar days after discovery of a breach of security.

HBNR Amendments

- Final rule amendments announced in May 2024
- Eight Main Take-aways:
  1. Rule applies to health apps and similar technologies not covered by HIPAA
  2. Breach includes data security breaches + unauthorized disclosures
  3. Clarification regarding what it means to draw PHR identifiable health information from multiple sources
  4. Revised definition of “PHR related entity”
  5. Expanded use of electronic notice to consumers
  6. Expanded content of notice to consumers
  7. Altered timing requirement for notice to FTC
  8. Adding cross-references, citations, and more information about penalties for non-compliance

GoodRx

- First enforcement action under HBNR
- Telehealth and discount drug provider allegedly shared personal information with third parties for advertising without consent and contrary representations
- Complaint alleges:
  - Failed to notify consumers and FTC of unauthorized disclosures of health info to third parties for advertising
  - Misrepresented disclosure of health information to third parties
  - Failed to limit third party use
  - Misrepresented HIPAA and DAA compliance
  - Failed to implement policies to protect health information

BetterHelp

- Mental health and telehealth counseling service allegedly shared personal information with third parties for advertising without consent and contrary representations to consumers
- Complaint alleges:
  - Failed to use reasonable measures to protect consumers' health information, resulting in unauthorized disclosure to third parties for advertising
  - Failed to obtain affirmative express consent
  - Failure to disclose + privacy misrepresentations

Easy Healthcare Corp. (Premom)

- Fertility app allegedly shared users' personal information with third parties, including two China-based firms, and failed to notify consumers
- Complaint alleges:
  - Failure to disclose + privacy misrepresentations
  - Unfair privacy and data security practices
  - Unfair sharing of health information for advertising without affirmative express consent
  - Failed to notify consumers as required by HBNR

Cerebral

- Mental health and pain management subscription service turned over sensitive health data of nearly 3.2 million consumers to third-parties like LinkedIn, Snapchat, and Tiktok
  - Complaint alleges:
    - Failed to clearly disclose sharing consumers' sensitive data with third parties
    - Failed to have adequate protections in place for data collected and engaged in unreasonable security
    - Violated OARFPA by engaging in unfair and deceptive practices with respect to substance use disorder treatment services
    - Violated Restore Online Shoppers' Confidence Act (ROSCA) by failing to clearly disclose all material terms of Cerebral's cancellation policies before charging consumers

Monument

- First privacy enforcement action alleging violations of Opioid Addiction Recovery Fraud Prevention Act of 2018 (OARFPA)
- FTC jurisdiction extends to HIPAA-covered entities
- Alcohol addiction treatment service shared consumers' health data for advertising purposes with third parties, contrary to promises and without consumer consent
- Complaint alleges:
  - Deceived users about sharing practices with third parties
  - Misrepresented HIPAA compliance
  - Violated OARFPA by misstating its practices regarding disclosure of users' personal information, including health information

1Health.io (Vitagene)

- Genetic testing firm allegedly left health data unsecured in the cloud, misled consumers about privacy and security (data deletion and sample destruction), and made material retroactive privacy policy changes without consent (reserving rights is not enough)
- Complaint alleges:
  - Privacy misrepresentations
  - Security misrepresentations
  - Unfair adoption of material retroactive privacy policy changes regarding sharing of consumers' sensitive personal information with third parties

Joint FTC-HHS Letters

- July 2023 letters to 130 hospital systems and telehealth providers
- Cautions them about the privacy and security risks related to the use of online tracking technologies, which may disclose consumers' sensitive personal health data to third parties.
- Highlights that this tech gathers identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid

July 2023 Health Privacy Guidance Takeaways

1. Understand the breadth of “health information”
2. Your obligation to protect the privacy of health information is a given.
3. Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.
4. Don’t share consumers’ health information improperly – and don’t receive it either.
5. Insist your technology people and compliance staff communicate about your company’s privacy practices.
6. "HIPAA Compliant,” “HIPAA Secure,” and similar claims may deceive consumers.
7. Companies that provide HIPAA seals and certifications also may be liable for deceptive claims.
8. Reserving the right to make big changes to your privacy policy isn’t real consent.
9. Hidden euphemisms don’t cut it.
10. You may be liable under the FTC Act for what you say and for what you *don’t* say.
11. The FTC Act protects biometric data.
12. Reproductive information should be protected from prying eyes.
13. There’s a lot at stake.

Security of Health Information

Vitagene - Company claimed to exceed industry-standard security practices, while storing health and DNA information in plain text in publicly accessible cloud repositories

PreMom - Alleged that app developer didn't employ reasonable security, including by failing to assess the risks of third-party SDKs

Chegg - Alleged that ed tech provider failed to protect personal information collected from users and employees, resulting in exposure through 4 data breaches of health, financial, and other information of millions

Security of Health Information

SkyMed - Alleged that provider of travel emergency services didn't use reasonable measures to secure personal information, leaving a cloud database with health info unsecured and misled consumers about its response to the incident

Henry Schein - Alleged that provider of dental office management software misrepresented industry-standard encryption of patient info to help dentists meet regulatory obligations under HIPAA

Remedies

- Ban on disclosing health information for advertising
  - E.g., Cerebral, Monument, Premom, BetterHelp, GoodRx
- Third Party Deletion
  - E.g., Premom, BetterHelp, GoodRx, ~Vitagene, Flo Health
- Deletion of algorithms or data product
  - E.g., Kurbo/Weight Watchers, Everalbum, CRI Genetics, Amazon/Alexa, Ring
- Money
  - Penalties (e.g., Monument, Cerebral, Premom, GoodRx)
  - Consumer redress (e.g., Cerebral, BetterHelp, Henry Schein)

Remedies

- Notice to consumers
  - E.g., Cerebral, Premom, BetterHelp, GoodRx, Vitagene, Flo Health
- Affirmative Express Consent for Disclosures
  - E.g., Cerebral, Premom, BetterHelp, GoodRx, Vitagene ~Flo Health
- Privacy programs
  - E.g., Cerebral, Premom, BetterHelp, GoodRx, Vitagene ~Flo Health
- Security programs
  - E.g., Cerebral, Premom, Vitagene, Chegg, SkyMed, Henry Schein

Remedies

- Data minimization - detail and limit data collection or retention
  - E.g., Chegg, Drizly, Premom, GoodRx, Kurbo
- Individual liability
  - E.g., Drizly, InfoTrax, PaymentsMD
- Deletion of data product / prohibition of generating data product
  - E.g., Kurbo, Everalbum, Facebook, Ring, Amazon/Alexa

Commercial Surveillance & Data Security ANPR

- Public comments address health extensively, e.g.,
  - Carve-outs for HIPAA-covered data
  - Same protections for all health data
  - Public health / research implications of restricting data use
  - De-identification
- Next steps

Artificial Intelligence (AI)

- AI/privacy enforcement actions
  - Rite Aid (face)
  - Amazon/Alexa (voice)
  - Ring (video)
- Policy – e.g., Biometric Policy Statement, Report to Congress on Combatting Online Harms Through Innovation, Voice Cloning Challenge, Summit on AI

AI Guidance

- Digital ownership & creation
- Watching the detectives: Suspicious marketing claims for tools that spot AI-generated content
- Hey, Alexa! What are you doing with my data?
- Chatbots, deepfakes, and voice clones: AI deception for sale
- Keep your AI claims in check
- The Luring Test: AI and the engineering of consumer trust
- Aiming for truth, fairness, and equity in your company’s use of AI

Takeaways

- What is health information?
- Risks associated with ad tech
- DTC tech – apps, telehealth, genetic testing
- HIPAA claims
- Biometric data
- Using every tool in the toolbox
- Serious consequences for violating Section 5, HBNR, and OARFPA
  - Ban on sharing health data for advertising
  - $$$

Speakers

Hannah Levin

Senior Associate, Cyber Privacy & Data Innovation

Orrick

hlevin@orrick.com

Erik Jones

Attorney, Division of Privacy & Identity Protection

Federal Trade Commission