Articles + Publications | October 6, 2025

Reproductive Health Data Privacy Laws in Flux – Compliance in an Ever-Changing Landscape

WRITTEN BY

Brent T. Hoard | David J. Navetta | Erin S. Whaley | Kaitlin J. Clemens | Timothy Shyu | Emma E. Trivax

Influenced by advancements in AI and wearable technology, and fueled by privacy concerns, reproductive health data is at a pivotal intersection of federal and state regulations. Traditionally, the Health Insurance Portability and Accountability Act (HIPAA) has served as the primary framework for protecting patient information and regulating health care providers and insurers.

Recently, however, a federal judge in Texas overturned the Reproductive Health Care Privacy rule, which amended HIPAA to impose stricter limitations on the use and disclosure of reproductive health-related protected health information (PHI). This ruling leaves covered entities uncertain about compliance, as states like California, Washington, and Virginia are enacting laws to fill these gaps and protect reproductive health data across various platforms and technologies. These laws often apply beyond traditional health care entities regulated by HIPAA, yet may still apply to HIPAA-covered entities if they collect data outside their medical provider role. This post summarizes some of the key developments and requirements in this area.

Federal Protections – A Federal Court Vacates the Final Rule

In April 2024, the U.S. Department of Health and Human Services (HHS) amended the HIPAA Privacy Rule to support reproductive health care privacy in the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization.* A majority of the final rule prohibits covered entities from disclosing or using PHI potentially related to reproductive health care for certain purposes, including criminal or administrative investigations or penalties. It also requires covered entities to attest that they would not use or disclose reproductive health care PHI for a prohibited purpose. The final rule also updated 42 CFR Part 2, requiring covered entities to revise their Notice of Privacy Policies to inform individuals of these changes.

In *Purl v. U.S. Department of Health and Human Services*, a Texas physician challenged the final rule on the grounds that it prevented her from complying with state reporting requirements related to child abuse and participating in public health investigations. On June 18, 2025, the court agreed and struck down those portions of the final rule related to reproductive health care privacy protections finding that they impermissibly limit state law on child abuse reporting, unlawfully redefine terms, and exceed HHS's authority to implement such a rule.

Accordingly, the court vacated the reproductive health care privacy protections set forth in the final rule, leaving intact only those requirements relating to modifications in notices of privacy practices related to substance abuse disorder to reflect changes in Section 3221(i) of the Coronavirus Aid, Relief, and Economic Security Act. HHS let the August 18, 2025, appeal deadline pass without challenging the *Purl* decision, thus telegraphing its agreement

with the court's decision. HIPAA-regulated entities must continue protecting reproductive health care information under existing HIPAA rules and regulations, but the enhanced reproductive protections under the final rule are no longer in effect.

State Law Fills in the Gaps

Even with the court-imposed limitations on the HIPAA final rule, several important states have regulated in this space. California, Virginia, and Washington have enacted data privacy laws that expand upon the federal requirements, with New York closely following suit with their pending New York Health Information Privacy Act (NYHIPA). These laws are broadly written and may apply to traditional HIPAA-regulated covered entities, health care-adjacent companies (*e.g.*, fitness trackers), and organizations that likely do not consider themselves to be health care-oriented at all (*e.g.*, retailers, advertisers, and tech companies that process geolocation data). Below are some considerations for businesses collecting reproductive health data.

California:

California's Assembly Bill No. 352 (AB 352), effective January 1, 2024, amended California's Confidentiality of Medical Information Act (CMIA) and introduced significant changes to the handling and sharing of sensitive health information, particularly regarding reproductive health services. The law applies broadly to both traditional and nontraditional health care entities. These nontraditional entities include electronic health record (EHR) developers, digital health companies, and other entities that store or maintain medical information on behalf of health care providers, health plans, pharmaceutical companies, contractors, or employers.

Although AB 352 does not create a new private right of action, it continues to allow individuals to seek remedies under the CMIA for negligent release of their confidential information or records. Administrative fines and civil penalties for negligent disclosure or mishandling of medical information can range from $2,500 to $25,000 per violation. Penalties for willful violations can amount to $250,000 per violation, and criminal penalties may also apply if the violation results in economic loss or personal injury to a patient. Key requirements include:

1. **Enhanced Security Measures:** As of July 1, 2024, businesses storing medical information on gender-affirming services, abortion, and contraception must implement security measures such as limiting access privileges and preventing sharing outside California.
2. **Prohibition on Cooperation With Out-of-State Inquiries**: Entities are prohibited from cooperating with out-of-state inquiries that could identify individuals seeking abortion services lawful in California.
3. **Prohibition on Disclosure of Medical Information:** Entities must not disclose medical information related to lawful abortion services to out-of-state individuals or entities unless authorized.
4. **Exclusion From Automatic Data Sharing:** Health information related to abortion services is excluded from automatic sharing on California's Health and Human Services Data Exchange Framework.

This law does not include a HIPAA exemption and therefore applies to HIPAA-covered entities.

Virginia:

Virginia's Senate Bill 754, amending the Virginia Consumer Protection Act (VCPA), took effect on July 1, 2025. It prohibits "suppliers" from processing reproductive and sexual health information (RSHI) without consumer

consent.

"Suppliers" include any entity involved in consumer transactions that obtain RSHI, including small businesses and nonprofits. Non-health care organizations, such as retailers, search engines, and companies using geolocation data, may fall under the act's scope due to its broad definitions. The law includes the carveouts under the Virginia Consumer Data Protection Act (VCDPA), explicitly exempting PHI covered by HIPAA or similar federal or state regulations.

The act defines RSHI broadly, including information related to reproductive health services, conditions, surgeries, contraceptive use, and any data derived from non-health-related sources. It does not differentiate between data controllers and processors, arguably requiring vendors to obtain consent for processing RSHI.

Violations can result in civil penalties enforced by the Virginia attorney general, ranging from $2,500 to $5,000 per violation. The act also provides a private right of action for consumers, allowing recovery of actual damages or statutory damages, with potential for treble damages and attorney fees for willful violations.

Key requirements include:

1. **Clear Consent:** Suppliers are required to obtain explicit consent before sharing RSHI, including abortion care or contraceptive use.
2. **Prohibition on Data Brokers:** The bill blocks data brokers from selling or sharing RSHI that could be used to track people seeking reproductive health care.
3. **No Processing Necessary Exemption:** SB 754 lacks an exemption for data processing necessary to deliver a product or service. Suppliers cannot process RSHI even when providing a related product or service unless the consumer provides explicit, clear, opt-in consent.
4. **No Entity-Level Exemptions:** The bill does not include the exemptions found in the VCDPA, and instead applies to a wide range of suppliers, even those who do not meet the VCDPA thresholds (*i.e.*, processing the personal data of 100,000 or more consumers during the calendar year). Accordingly, small businesses and nonprofits are included under the definition of supplier.

For more information on the Virginia law, please visit our FAQ series on Virginia's Protection of Reproductive Health Information Law.

Washington:

The My Health My Data Act (MHMDA), effective on April 27, 2023, imposes a variety of restrictions on the use of "consumer health data" by companies operating in Washington or engaging with its residents. Consumer health data includes any personal information linked to a consumer's health status, and explicitly includes cookie IDs. The law is broad and applies to both traditional health care entities (like doctors or hospitals) as well as digital health companies (*e.g.*, fitness trackers, telehealth apps). However, HIPAA-regulated PHI is not regulated by the statute. As with California's and Virginia's laws, the MHMDA covers a wide range of organizations, including small businesses and nonprofits, and applies to data collected in Washington.

Investigations into and penalties for violations of MHMDA can be brought by the Washington attorney general, with a maximum fine of $7,500 per violation. If the violation is deemed willful or intentional, the attorney general can, in their discretion, seek higher penalties. Further, the statute allows consumers to pursue a private right of action for

noncompliance, including seeking declaratory relief, injunctive relief, actual damages, and statutory damages of up to $7,500 per violation.

Key aspects of the MHMDA include:

1. **Granular Consent**: Companies need to obtain specific, detailed, and explicit consent from individuals before collecting, using, or sharing their health data. For example, individuals need to know exactly what data is being collected and how it will be used, including whether it will be used for health care purposes, whether it will be shared with third parties, and the specific purpose the company is using the data.
2. **Consumer Authorization to Sell Data**: Prohibits selling consumer health data without a signed authorization, valid for one year and revocable at any time.
3. **Expanded Data Subject Rights**: Includes rights of access and deletion, extending to all third parties and backups.
4. **Limitation on Geofencing**: Prohibits the use of health data collected through location-based data to target individuals for advertising or marketing based on their location in a health care setting or in relation to health care services.

New York:

The NYHIPA will also seek to fill in the gaps and protect data not typically falling under HIPAA, requiring reasonable safeguards to protect the security, confidentiality, and integrity of regulated health information.

Similar to the other states, the NYHIPA applies broadly to both traditional health care entities like health care providers, and health insurers, but also nontraditional entities, such as apps and digital platforms that collect health data (*e.g.*, wearable devices and digital health tools). The NYHIPA covers any health-related data that can identify an individual, including data related to medical conditions, treatment, prescription information, mental health data, and genetic information.

Although the NYHIPA does not offer a private right of action, the New York attorney general has enforcement power, and can bring both investigations and civil enforcement actions against organizations that fail to comply. Fines for violation can amount to $5,000, and up to $10,000 per violation if the violation was willful or resulted in harm to individuals.

Key aspects of the NYHIPA will include:

1. **Explicit Consent:** Organizations must obtain explicit, informed consent from individuals before collecting, using, or sharing their health information. This means consent must be specific, clear, and obtained prior to any data collection.
2. **Limited Use:** Health data may only be used for specified purposes as disclosed at the time of consent. It cannot be used for marketing or advertising purposes without the individual's consent.
3. **Security Safeguards:** Sensitive health data must be encrypted, particularly when it is transmitted electronically or stored in digital systems.
4. **Data Minimization:** Organizations must only collect and retain health data that is necessary for the specific purpose outlined in the consent agreement. Data that is no longer needed should be deleted or anonymized.

There are consistent themes across these state laws: entities not traditionally viewed as health care providers, such as digital health trackers and fitness apps, are now subject to stringent privacy regulations with significant

penalties for noncompliance. Organizations should reassess the data they collect, the methods of collection, and its intended use to determine if they are governed by these statutes. Given the complexity and potential impact of these regulations, it is crucial for organizations to consult with experienced privacy counsel who can provide tailored guidance to ensure compliance and help mitigate risks associated with these new laws.

RELATED INDUSTRIES + PRACTICES

- Data + Privacy
- Health Care + Life Sciences
- Health Care Regulatory
- Privacy + Cyber