Simpson Thacher

Memorandum

New Health Privacy Laws Passed by States and Proposed by the Biden Administration and Congress in Response to the *Dobbs* Decision

July 31, 2023

In the last four months, the Biden Administration and Congress have proposed, and three states have enacted, new health privacy laws and regulations governing reproductive health information. These laws and proposals seek to limit uses and disclosures of reproductive health information in ways that may pose risks to patients, health care providers and others after the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, which held that the Constitution does not confer the right to an abortion, overturning *Roe v. Wade* and *Planned Parenthood v. Casey*.

At the federal level, the U.S. Department of Health and Human Services Office for Civil Rights ("**OCR**") published a Notice of Proposed Rulemaking ("**Proposed Rule**") in April that would strengthen privacy protections for reproductive health care information. OCR noted that the *Dobbs* decision and subsequent legal developments increase the chance that an individual's reproductive health care information may be used or disclosed in ways that undermine the quality of, and/or access to, health care. OCR asserted that the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("**HIPAA**") do not adequately address uses and disclosures of such information for non-health care purposes. For example, disclosures of this information could subject individuals to criminal proceedings for obtaining or providing reproductive health care. Members of Congress have also proposed legislation that would restrict certain uses and disclosures of health data. Senators Klobuchar, Warren and Hirono introduced the Upholding Protections for Health and Online Location Data Privacy Act of 2023 ("**Uphold Privacy Act**"), which would prohibit the use of health data for commercial advertising. The bill would require certain entities to provide privacy policies related to the collection, retention, use and disclosure of health data; permit individuals to request the deletion of health and location data held by certain entities; prohibit data brokers from selling location data; prohibit the sale of location data to data brokers; require the Federal Trade Commission ("**FTC**") to issue new regulations on health data and location data; and create a private right of action.

At the state level, in June, both Connecticut and Nevada passed legislation with new protections for consumer health data, including reproductive health, sexual health and gender-affirming care data. And in April, Washington State enacted the My Health My Data Act, which similarly created requirements for the collection and sharing of such data and established a private right of action for consumers. The three state laws and, potentially, new federal laws and regulations will impose new requirements on regulated entities, necessitate analyses of current uses and disclosures of health data and subject regulated entities to additional litigation.

The Proposed Rule, Uphold Privacy Act and the three state laws address uses and disclosures of health data in ways that were not contemplated by Congress or OCR when HIPAA was enacted and implemented. For example, the Proposed Rule would prohibit uses and disclosures of reproductive health information for the purpose of prosecuting individuals obtaining or providing lawful reproductive health care in another state. The Uphold Privacy Act would define health data to include information derived or extrapolated from non-health information, such as proxy or algorithmic data. The three state laws prohibit the implementation of geofences, which use cellular or other data to establish a virtual boundary around a consumer's physical location, near certain medical facilities if the geofences will be used for certain purposes related to consumer health data, such as tracking and sending notifications to consumers. Below, we discuss each proposal and new state law.

OCR's Proposed Rule

The Proposed Rule would strengthen regulations regarding uses and disclosures of a specific type of health data for which Congress has not yet mandated additional protections. As a result, the Proposed Rule may be more vulnerable to judicial challenges than OCR's 2013 amendments to HIPAA to increase privacy protections for genetic information, which Congress required in a 2008 law.

The Proposed Rule would prohibit certain uses and disclosures of Protected Health Information ("**PHI**"), permit certain uses and disclosures of PHI only if a Covered Entity, as defined under HIPAA, has first obtained an attestation from the prospective recipient of the requested PHI, require updates to a Covered Entity's Notice of Privacy Practices and make technical corrections. If the following modifications are finalized, the Proposed Rule would prevent existing HIPAA provisions that permit certain uses and disclosures of PHI from being used to obtain an individual's PHI for a non-health care purpose that would be detrimental to the individual, the individual's health care providers or others:

- **Definition of "Reproductive Health Care":** The Proposed Rule would define "reproductive health care" as "care, services, or supplies related to the reproductive health of the individual." The definition would include reproductive health care and services furnished by a health care provider; supplies furnished in accordance with a prescription; care, services or supplies furnished by other persons; and non-prescription supplies purchased in connection with an individual's reproductive health. The Proposed Rule lists examples of health care services and supplies related to the reproductive system that would fall under the definition, including fertility treatments, prenatal care, pregnancy termination, miscarriage management and contraception.
- **Prohibition on Use and Disclosure of Reproductive Health Care PHI:** Covered Entities and their Business Associates, as defined under HIPAA, would be prohibited from using or disclosing PHI for either of the following purposes:
    - A criminal, civil or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing or facilitating reproductive health care that is:

- provided out of the state where the investigation or proceeding is authorized and is lawful in the state in which it is provided;
- protected, required or authorized by federal law; or
- provided in the state in which the investigation or proceeding is authorized and permitted in that state; or

◦ The identification of any person for the purpose of initiating these investigations or proceedings.

For example, the proposed prohibition would apply in cases where an individual travels to another state to receive an abortion that is lawful in the state where the abortion is provided.

- **Attestation Requirement:** The Proposed Rule would permit Covered Entities and their Business Associates to use and disclose PHI as otherwise permitted under HIPAA so long as the requested use or disclosure is for a permitted purpose. OCR recognizes that it would be difficult for regulated entities to ascertain whether a request for PHI is for a permitted purpose, so the Proposed Rule would require signed attestations from persons requesting PHI that the PHI will not be used or disclosed for the prohibited purposes described above. The Proposed Rule's requirements for a valid attestation are modeled after HIPAA's existing authorization requirements for certain uses or disclosures of PHI.

- **Revised Notice of Privacy Practices:** Finally, the Proposed Rule would require minor revisions to and a redistribution of a Covered Entity's Notice of Privacy Practices. The revised Notice of Privacy Practices would describe the new attestation requirement and the two prohibited uses and disclosures of PHI discussed above in enough detail for an individual to understand the prohibited uses and disclosures.

In the Proposed Rule, OCR repeatedly cites the potential harmful effects on health care and individuals that may result from uses or disclosures of PHI for non-health care purposes and outside of the patient/health care provider relationship. OCR describes the potential impact of such disclosures of PHI on individuals' medical conditions and willingness to seek lawful treatment, as well as on health care providers' ability to correctly diagnose patients and provide information about treatment options. For example, OCR noted that individuals may not seek emergency care or other health care for fear that their records may be disclosed. Similarly, health care providers may withhold information about treatment options for fear of prosecution or liability arising from disclosure of an individual's PHI. This is not the first time that OCR has cited fears related to the use or disclosure of PHI in its rulemakings; OCR has cited fear of discrimination, abuse and retaliation in other proposed rules on substance use disorder patient records and coordinated care.

The Proposed Rule is one of several Biden Administration actions that would provide additional privacy protections for patients post-*Dobbs*. The Proposed Rule would considerably change how Covered Entities and their Business Associates are permitted to use and disclose PHI related to reproductive health care. To date, the Proposed Rule has received almost 26,000 comments, including comments from health plans, hospitals and health systems, electronic medical records companies, state Medicaid agencies, providers of reproductive health

care, Members of Congress, state and local government officials, health policy and privacy organizations, religious and social justice organizations, individuals and associations representing physicians and physician practices, health plans, health care information systems and managed care pharmacies. The comment period has closed, and we anticipate that the Administration will move to finalize the Proposed Rule expeditiously. Once finalized, the rule would take effect 60 days after publication in the *Federal Register*, and regulated entities would then have 180 days after the effective date to comply. Some commenters, such as health plans that send Notices of Privacy Practices on an annual basis, noted that additional time may be required to implement the regulation. Aspects of the final rule will almost certainly be challenged in court.

The Uphold Privacy Act

In a press release introducing the Uphold Privacy Act, Senator Klobuchar cited reports of companies and data brokers that collect and sell location data of individuals who visit health care facilities that offer abortions and family planning services. The bill would prohibit data brokers that collect, buy, license or infer data about an individual and that sell, license or trade this data from selling, reselling, licensing, trading, transferring, sharing or otherwise providing or making available location data, including data that individuals volunteer and data from wearable fitness trackers, web browser histories and other sources. The Uphold Privacy Act also includes a number of other protections for health data, which the bill defines much more broadly than HIPAA. Under the bill, "health data" would include:

- data that relates to searches for, attempts to obtain and the receipt of *any* health services;
- efforts to research or obtain health services or supplies, including location data that might indicate an attempt to acquire or receive such services or supplies; and
- information regarding health services, health conditions and treatments of such conditions that is derived or extrapolated from non-health information, such as proxy, derivative, inferred, emergent or algorithmic data.

The bill would apply to any entity engaged in activities in or affecting commerce, other than HIPAA Covered Entities and Business Associates, and would prohibit such entities from using individuals' health data for commercial advertising. The Uphold Privacy Act would require such entities to obtain an individual's express consent to collect, retain, use or disclose health data, unless the entity is collecting, retaining, using or disclosing health data to provide the individual with a product or service that the individual has requested from the entity. If enacted, the bill would require such entities to publish privacy policies on the collection, retention, use and disclosure of health data that list the specific third parties to which the entities disclose such data and that list the specific third parties from which the entities have collected such data. These privacy policies would need to include the purposes for which the health data is being disclosed and how the health data may be used by each third party, as well as the purposes for which the entity collects the data. The bill does not specify whether the third parties would be listed by name or in another manner, such as by categories of data recipients.

The FTC has recently increased its scrutiny of uses of health data and enforcement of its health breach notification rule under its existing authority. The legislation would grant the FTC the authority to treat certain violations as unfair or deceptive acts or practices under the FTC Act, including violations of its prohibitions on the sale of location data by data brokers and the sale of location data to data brokers. The bill would not preempt state laws that offer greater privacy protections than those provided in the Uphold Privacy Act. Additionally, the Uphold Privacy Act would grant the FTC the authority to bring civil actions to enjoin violations by regulated entities and data brokers and to obtain civil penalties and damages, restitution, disgorgement of unjust enrichment, other compensation and equitable relief. If passed, the legislation would enable individuals to bring civil actions and obtain damages, restitution, attorney's fees and other relief.

Washington, Connecticut and Nevada Laws on Consumer Health Data

In the absence of congressional action on health privacy laws post-*Dobbs*, beyond the introduction of the Uphold Privacy Act, three states have enacted or revised their own health privacy laws. The new state laws address the ways that consumers seeking health care are being identified and targeted by entities that are not subject to HIPAA. For example, Washington and Nevada define "consumer health data" to include information that is derived from algorithms and machine learning, which is a type of artificial intelligence. The Washington Attorney General recently issued guidance explaining that information that is derived or extrapolated from non-health data and used by a regulated entity to associate a consumer with consumer health data is considered "consumer health data." The Washington Attorney General noted that a retailer's "pregnancy prediction score," based on the purchase of certain products, would be consumer health data even though it was inferred from non-health data. Given the increased focus on the use of reproductive health data post-*Dobbs*, we expect additional states to pass consumer health privacy laws.

On April 27, 2023, Washington State enacted the My Health My Data Act. This consumer health privacy law makes it unlawful for any person to implement a geofence around an entity that provides in-person health care services where the geofence is used for certain purposes, such as identifying or tracking consumers seeking health care services and collecting consumer health data. The My Health My Data Act establishes affirmative consent requirements for the collection and sharing of consumer health data and prohibits the sale or offer to sell consumer health data without a consumer's valid authorization. The law also requires regulated entities that conduct business in the state or produce or provide products or services targeted to Washington consumers to implement consumer health data privacy policies. Regulated entities may be subject to new civil penalties for violations and or civil actions from consumers seeking to enjoin further violations and recover actual damages and litigation costs. The law provides that violations are *per se* violations of Washington's Consumer Protection Act, which is enforced by the Washington Attorney General and through private actions. The law's restrictions on implementing geofencing took effect on July 23, 2023, and regulated entities that are not small businesses must comply by March 31, 2024.

On June 2, 2023, Connecticut amended its Data Privacy Act to add new provisions related to consumer health data. Similar to Washington's law, the law prohibits the use of geofences near mental, reproductive and sexual health facilities for the purpose of identifying, tracking or collecting data from or sending notifications to a consumer regarding the consumer's health data. Connecticut's law expands the definition of "sensitive data" to include "consumer health data," which is any personal data that a data controller uses to identify a consumer's physical or mental health condition or diagnosis, including gender-affirming health data and reproductive or sexual health data. The law also requires any controller that determines the purpose and means of processing consumer health data to, among other things, obtain consent to sell, or offer to sell, such consumer health data. The law's provisions apply to persons that conduct business in Connecticut and persons that produce products or services that are targeted to residents of Connecticut. The law does not create a private right of action.

A few days later, on June 5, 2023, Nevada passed its consumer health data privacy law. As with Washington and Connecticut, the Nevada law applies to persons who conduct business in the state or produce products or services that are targeted to consumers in the state. The law broadly defines "consumer health data" to include personally identifiable information 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, including any information derived through an algorithm, machine learning or any other means. Nevada's law requires regulated entities to obtain affirmative, voluntary consent from consumers to collect their consumer health data and prohibits persons from selling or offering to sell consumer health data without a consumer's written authorization. The law provides certain privacy rights to consumers who provide health data to regulated entities (which do not include entities subject to HIPAA, the Gramm-Leach-Bliley Act or other laws that govern certain types of data, such as patient safety, clinical trial and public health data). For example, the law provides consumers with the right to request the deletion of their consumer health data. While the law does not create a private right of action, Nevada's deceptive trade practices laws provide for $5,000 per-violation civil penalties for those who willfully engage in deceptive trade practices.

In addition to these states, California's existing consumer privacy law, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "**CCPA**"), defines "sensitive personal information" to include "personal information collected and analyzed concerning a consumer's health." CCPA allows consumers (any California resident) to direct covered businesses to limit the use and disclosure of their sensitive personal information. However, the CCPA does not apply to medical information collected by a Covered Entity under HIPAA, such as a health care provider.

Although the majority of the provisions in the new Washington, Connecticut and Nevada state laws do not take effect until 2024, regulated entities will need to begin drafting privacy and technical policies and procedures to address the new rights granted to consumers with respect to their consumer health data under these laws. Regulated entities must also start collecting affirmative consents for certain uses and disclosures of consumer health data and implementing restrictions on the collection, use, disclosure and sale of consumer health data.

For further information regarding this memorandum, please contact one of the following authors:

WASHINGTON, D.C.

Vanessa K. Burrows
+1-202-636-5891
vanessa.burrows@stblaw.com

Sara Y. Razi
+1-202-636-5582
sara.razi@stblaw.com

Nawa Lodin
+1-202-636-5980
nawa.lodin@stblaw.com

NEW YORK CITY

Jessica N. Cohen
+1-212-455-7736
jessica.cohen@stblaw.com

John C. Ericson
+1-212-455-3520
jericson@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Mark D. Pflug
+1-212-455-7239
mpflug@stblaw.com

Arthur D. Robinson
+1-212-455-7086
arobinson@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com