December 21, 2022

Protecting The Privacy of Reproductive Health Information Post-Dobbs

*Summary of Federal and California Health Privacy Laws and Recommendations to Expand Protection**

By: Andrea Frey, JD, MPH, Senior Counsel, Hooper, Lundy & Bookman, P.C.; Kerry K. Sakimoto, JD, Associate, Hooper, Lundy & Bookman, P.C.; Robby Franceschini, JD, MPH, Managing Director, BluePath Health

Background

On June 24, 2022, the Supreme Court released its decision in *Dobbs v. Jackson Women's Health Organization,* overturning *Roe v. Wade* and the constitutional right to an abortion.[1] The decision authorizes state legislatures to regulate abortion, leading states to enact a patchwork of laws that span the spectrum of prohibiting to enhancing access to abortion and related reproductive health services. In an effort to enforce restrictive laws, state prosecutors and law enforcement agencies will likely turn to patient medical records and related health-care information in the search for evidence of potential civil and criminal violations, raising questions around whether existing health information privacy laws sufficiently protect both patients and health care providers.

Although federal and state health privacy laws provide broad protection for patients regarding when and how their providers may use and share medical information, these laws are far from an absolute protection and often limited in their application. These limitations could have significant implications for patient-provider confidentiality and the delivery of healthcare, particularly if patients think that their health information, including PHI, is no longer secure and hesitate to seek necessary reproductive health

* The information, statements and recommendations in this fact sheet are general in nature, do not constitute legal advice, and should not be used as a substitute for obtaining competent legal counsel. Readers should be aware that the laws, rules and regulatory guidance are subject to change. Please contact legal counsel for any specific legal advice. Note also that this fact sheet does not provide a comprehensive overview of all applicable federal and state laws and requirements.

services. And for those who do, their reproductive health information could be used for prosecutions in states where abortion is not legally available.

This fact sheet provides an overview of federal and California legal protections governing the privacy of reproductive health information post-*Dobbs*, the impact of data sharing obligations on such privacy laws, and what policy options may be leveraged to enhance protection of individuals' medical information in California.[2]

Protection of Patient Reproductive Health Information under HIPAA

At the federal level, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") sets forth a floor of comprehensive standards for the protection of individually identifiable health information (referred to as "protected health information" or "PHI") for covered entities, including hospitals, health plans, clinicians' offices, and their business associates, that hold or transmit PHI.[3] HIPAA's implementing regulations under the Privacy Rule establish specific rules regarding the use and disclosure of PHI by these entities without a patient's knowledge or authorization.[4]

Shortly following the issuance of *Dobbs*, the Office for Civil Rights ("OCR") within HHS (the agency that enforces HIPAA) issued new guidance addressing permitted disclosures and their limitations under the Privacy Rule.[5] As detailed in the guidance, HIPAA permits (but does not require) covered entities to disclose PHI without the patient's knowledge or authorization in the following circumstances:

- Disclosures Required by Law: The Privacy Rule permits – but does not require – covered entities to make disclosures of an individual's PHI without an authorization where such disclosure is expressly required by another law, and the use or disclosure complies with and is limited to the relevant requirements of such law.[6] For example, newly enacted state laws post-*Dobbs* may require practitioners or facilities to report on post-abortion complications or whether the fetus was viable.[7] In these instances, HIPAA does not serve to protect patients from covered entities complying with such reporting requirements under state law. Where, however, a workforce member suspects that a patient may have taken medication abortion and state law does not expressly mandate reporting that patient to law enforcement, the guidance issued by HHS states that the Privacy Rule would not permit such a disclosure to law enforcement. Any disclosure made would constitute a reportable breach of that patient's PHI, requiring notice to HHS and the patient.[8]

- Disclosures for Law Enforcement Purposes: Covered entities are also permitted, but not required, to disclose PHI for law enforcement pursuant to legal process such as a warrant, subpoena or summons and "as otherwise required by law," provided all other conditions outlined in the Privacy Rule for such disclosures are satisfied.[9] To illustrate, a law enforcement official may requests that a clinic turn over records regarding all abortions performed on-site. If the request is not accompanied by a court order or other mandate enforceable in a court of law, the Privacy Rule would preclude disclosure of PHI by the clinic in response to such a request.[10] However, where the law enforcement official presents a court order mandating the clinic to produce PHI about an identified individual who has obtained an abortion, the Privacy Rule "would permit but not require the clinic to disclose the requested PHI," and it may disclose only the PHI expressly authorized by the court order.[11]

- Disclosures to Avert a Serious Threat to Health or Safety: Covered entities may disclose PHI if they believe in good faith that disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and consistent with applicable law and standards of ethical conduct.[12] However, OCR finds that disclosures of PHI to law enforcement or others regarding a patient's interest, intent, or prior experience with reproductive health care would be inconsistent with professional standards of ethical conduct, as such disclosure compromises the integrity of the physician-patient relationship and may increase risk of harm to the patient.[13] HHS notes that HIPAA would not permit a health care provider to disclose an individual's intent to get a legal abortion, as this would not qualify as a serious and imminent threat to the health and safety of a person or the public, and would be inconsistent with the provider's ethical standards.[14]

Ultimately, OCR's guidance makes clear that while there are limited circumstances in which a covered entity is permitted to disclose PHI regarding an abortion or reproductive health services to law enforcement or others who might use the information to enforce restrictive laws, any such disclosure is never required by HIPAA itself.

Limitations of HIPAA

Although HIPAA sets an integral foundation for the protection of patient information maintained or transmitted by most health care providers and their business associates, concerns regarding the protection of reproductive health information remain post-*Dobbs* in the face of new state laws limiting or restricting abortion. For example:

- Permissive Disclosures: While HIPAA itself may not prohibit certain disclosures without an authorization from the patient, other laws that support criminal or civil

action against those seeking an abortion or facilitating the performance of an abortion may be used as the basis for a permissive disclosure of PHI "for law enforcement purposes," by compelling providers and other covered entities to disclose abortion-related PHI to law enforcement and other state officials. For example, state law can impose penalties on providers for failing to comply with a warrant or subpoena for abortion-related information. Even though disclosing abortion-related PHI would not be required under HIPAA, the law is limited in its ability to fully protect the rights of patients seeking abortion-related care.

- Limited Applicability: HIPAA only protects PHI maintained or transmitted by certain entities that are considered covered entities or their business associates.[15] This means that sensitive information collected by certain technology companies or mobile health applications, for example those that access a person's internet search history or track a user's menstrual cycle, is typically not protected by HIPAA. These data are generally entitled only to the privacy protections provided by the company in its terms of service or privacy policy, and the Federal Trade Commission ("FTC") rather than HHS oversees the relationship between consumers and service providers.[16] (See also this additional guidance issued by OCR directed at warning individuals that their sensitive health information collected on personal devices and/or mobile applications generally falls outside of HIPAA's protections.[17])

California's Confidentiality of Medical Information Act

California's analog to HIPAA, known as the Confidentiality of Medical Information Act or CMIA, is the state's primary law addressing privacy of medical information and expands upon HIPAA's protections. The CMIA and its restrictions on the use and disclosure of medical information apply to health care providers and plans, and more broadly to businesses organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care upon request.[18] Unlike HIPAA, the CMIA applies to companies that offer devices or mobile applications designed to maintain medical information, such as certain fertility trackers, or other products that store details about a user's sexual activity, ovulation, or fertility test results.[19]

Notably, the CMIA does not apply to medical information "sought" by a law enforcement agency; rather the California Penal Code applies, which considerably narrows the instances in which disclosures may be made to law enforcement without patient authorization. Providers may generally only disclose a patient's medical information to law enforcement if – *and only if* – the disclosure is: (i) in accordance with the patient's

prior written consent; (ii) authorized by an appropriate order by a court in the county where the records are located, granted after application showing good cause; or (iii) authorized by a valid search warrant.[20] However, the CMIA does not prevent covered entities from making unsolicited reports to law enforcement agencies when otherwise permitted.[21]

California Constitutional Right to Privacy

The California Constitution, Article 1, Section 1 expressly protects the right of privacy, and this right extends to a patient's medical and psychiatric history.[22] Providers have raised this constitutional right to protect patient records from disclosure, often pursuant to requests from state agencies like the Medical Board of California, and courts have balanced the privacy rights of the patient to the need for the information in the litigation (*e.g.*, can the agency show a compelling interest to overcome the patients' right to privacy).[23] Additionally, the recent voter-approved Senate Constitutional Amendment No. 10 amends the state constitution to explicitly protect the right to abortion and contraception.

New State Legislative Privacy Measures: AB 2091 and AB 1242

Two recently enacted state laws enhance privacy protections for medical information of individuals seeking abortions in the state. Both are explicitly intended to counter restrictive abortion laws in other states, leaving some providers and companies caught in the middle between compliance with conflicting state laws:

- Assembly Bill 2091, in part, seeks to enhance privacy protections under the CMIA for patients' medical records related to abortion care by prohibiting disclosures to law enforcement and out-of-state parties seeking to enforce abortion bans in other states. It would also prohibit a person from being compelled to identify or provide information that would identify an individual who has sought or obtained an abortion, if the information is being requested based on either: (i) another state's laws, which interfere with an individual's rights to choose or obtain an abortion; or (ii) a civil action authorized by another state's law to punish an offense against the public justice of that state.[24]

- Assembly Bill 1242 prohibits certain California-based technology corporations from providing records or information pursuant to a warrant, subpoena or other legal process relating to an investigation or enforcement of another state's abortion law, where the abortion is lawful under California law.[25]

Impact of Federal and State Data Sharing Obligations

ONC Information Blocking Rule

The 21st Century Cures Act Information Blocking Rule prohibits certain practices by health care providers, health information technology developers, and health information exchanges and networks that are likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI).[26] Thus, "the information blocking provision may operate to require that actors provide access, exchange, or use of EHI in situations that the HIPAA Rules would not require access of similar information"—unless an exception such as to prevent harm or comply with another law applies.[27]

The Information Blocking Rule could be implicated where, for example, a law enforcement official requests electronic health information from a provider that includes reproductive health information, and the provider denies or delays turning the requested information over. While the regulations contemplate exceptions to information blocking for preventing harm to the patient, the applicability of the exception is not clear when the requestor is a third party, such as a law enforcement official. Another potentially applicable exception is the privacy exception, under which a denial of access is not considered information blocking based on a request from the patient that the health care provider not provide such access, among other requirements.

It should be noted that, even where permitted by HIPAA, if a disclosure is impermissible under state law, then compliance with the state law would not be information blocking. In California, a provider could point to the new protections under AB 2091 as a basis for denying a request for a patient's EHI from an out-of-state law enforcement agency. Further, an actor only violates the Information Blocking Rule if it knows the practice is unreasonable and likely to interfere with the access, exchange, or use of electronic health information. A health care provider or other entity like a health information exchange could take the position that it acted reasonably in withholding access to law enforcement.[28]

California's New Data Exchange Framework

Following the passage of Assembly Bill 133 in July 2021, enacting California Health and Safety Code Section 130290, California became the first state focused on implementing a statewide data exchange framework (also referred to as the DxF), and mandating "real-time" access to, or exchange of health information by required DxF participants.

In particular, AB 133 will require most health plans, hospitals, physician organizations, and clinical laboratories in California to begin sharing by January 1, 2024 what is called "Health and Social Services Information" for treatment, payment and health care operations.[29] Reproductive health information would be subject to the data sharing mandate as the DxF and the implementing Data Sharing Agreement and policies and procedures do not offer patients a choice to opt out of having their sensitive data shared over the exchange. Forthcoming policies are expected on topics that include information blocking, monitoring and auditing, and enforcement, and further consideration may be warranted by the DxF around ensuring appropriate protections are in place for information relating to reproductive health services.

Options to Enhance Legal Protections for Reproductive Health Information

In the wake of *Dobbs*, a renewed focus on ensuring the privacy of reproductive health information is critical to ensure patients are comfortable seeking needed care and that when they do, their information is not used to prosecute them or someone involved in their care. Below are a number of proposed legislative and regulatory measures that could enhance legal protections for such information.

- Federal-Level Legislative & Regulatory Measures:
    - HIPAA Privacy Rule amendments: HHS could enact specific rules or clarify the Privacy Rule to provide for special treatment for the use and disclosure of PHI relating to abortion-related care and other reproductive health services – similar to how it carves out psychotherapy notes. In so doing, the agency could further restrict providers and others from sharing an individuals' reproductive health information without their explicit authorization, particularly to law enforcement and for civil and criminal proceedings involving penalties for abortion care, including investigations and enforcement pursuant to another state's abortion law.
    - Limits to allowable disclosures: Federal officials could also enact new legislation calling for the special protection of such records (*i.e.*, as with genetic information under the federal law, GINA). For example, such legislation could limit the ability of companies and businesses, including those not currently subject to HIPAA or other federal or state patient privacy laws, from disclosing reproductive health information without authorization from the consumer.

- Information Blocking Rule amendments: HHS could revise the Information Blocking Rule to include an exception for disclosing reproductive health information to third parties, or revise the "preventing harm exception" to allow a denial of access to a third party where there is a reasonable belief that providing access would cause substantial harm—rather than endangerment of life or safety—to the patient or others. Such action would bolster similar recommendations from health information technology experts recommending that institutions explicitly add pregnancy and abortion-related care to their information blocking policies under the preventing harm exception.[30]

- Technical assistance and compliance guidance: Federal officials could dedicate resources to assist companies handling reproductive health policy in developing more robust privacy and security policies and procedures, in addition to detailed guidance clarifying obligations under federal law with respect to disclosure of reproductive health information.

- California-Level Legislative & Regulatory Measures:

  - Limits to allowable disclosures: State officials could likewise enact new legislation or provisions under the Data Sharing Agreement calling for the special protection of reproductive health information (much like the state's Lanterman-Petris-Short Act, which protects certain mental health records). Such legislation could limit the ability of companies and businesses from disclosing such reproductive health information without authorization from the consumer.

  - Technical assistance and compliance guidance: California officials could likewise dedicate resources to assist providers in developing more robust privacy policies and procedures, in addition to detailed guidance clarifying obligations under state law with respect to disclosure of reproductive health information.

Endnotes

[1] Dobbs, 142 S.C. 2228 (2022).

[2] Note that this fact sheet does not cover institutional recommendations for protecting reproductive health information. *See* Raman R. Khanna et al., *Protecting reproductive health information in the post-Roe era: interoperability strategies for healthcare institutions*, J Amer Med Inform Assoc (2022) for recommendations for institutions to protect such information.

[3] *See* 45 C.F.R. § 164.104.

[4] *See generally* 45 C.F.R. §§ 164.500 *et seq.*

[5] U.S. Dep't Health & Hum. Serv's, HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care (last rev. Jun. 29, 2022), available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html.

[6] 45 CFR § 164.512.

[7] *See, e.g.*, Guttmacher Institute, Abortion Reporting Requirements (Aug. 1, 2022), available at: https://www.guttmacher.org/state-policy/explore/abortion-reporting-requirements.

[8] This guidance appears to contradict prior interpretation by OCR with regard to the ability of a covered entity to disclose PHI under the Privacy Rule in response to an "administrative request" (such as an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process). Per 45 CFR § 164.512(f)(1)(i)(C), a covered entity may disclose PHI pursuant to an administrative request as long as the PHI sought "is relevant and material to a legitimate law enforcement inquiry," the "request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought," and "de-identified information could not reasonably be used." Prior OCR guidance regarding permissive disclosures for such an administrative request suggested that as long as there was a written statement with the above elements, no "judicial involvement" was necessary.

[9] 45 CFR § 164.512(f).

[10] See fn. 8 above. Here again, the latest guidance appears to revise OCR's previous interpretation of lawful disclosures of PHI pursuant to an "administrative request" by removing the reference to a lack of judicial involvement, in stating that, "[i]n the absence of a mandate enforceable in a court of law, the Privacy Rule's permission to disclose PHI for law enforcement purposes does not permit a disclosure to law enforcement where a hospital or other health care provider's workforce member chose to report an individual's abortion or other reproductive health care."

[11] 45 CFR § 164.512(f)(5). Note that the permissive exception or disclosure to law enforcement also permits covered entities to make disclosures of PHI without an authorization for the purpose of reporting criminal conduct that occurred on the covered entity's premises. Thus, even in the absence of a legal mandate, HIPAA may still permit – but again, not require – reporting of abortion-related care in states that criminalize the procedure.

[12] 45 CFR § 164.512(j).

[13] U.S. Dep't Health & Hum. Serv's, Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet (last rev. Jun. 29, 2022), available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

[14] *Id.*

[15] *See* 45 C.F.R. § 164.104.

[16] However, the FTC issued guidance related to the topic of protecting the privacy of individuals seeking reproductive services, stating that it will continue to "vigorously enforce the law" under the FTC Act related to misuse of individuals' location, health, and other sensitive data. Fed. Trade Comm'n, Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data (July 11, 2022), available at

https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use.

[17] U.S. Dep't Health & Hum. Serv's, Protecting the Privacy and Security of Your Health Information When using Your Personal Cell Phone or Tablet (last rev. Jun. 29, 2022), available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

[18] Cal. Civ. Code § 56.06.

[19] "Attorney General Bonta Emphasizes Health Apps' Legal Obligation to Protect Reproductive Health Information," *Cal. Dep't of Justice*, *Office of the Att'y Gen.* (May 26, 2022), available at: https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect.

[20] Cal. Penal Code §§ 1543 – 1545.

[21] Note also that the CMIA allows disclosures of medical information if "in good faith" the disclosure is believed "necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat" but this expectation is only available to psychotherapists, as the term is defined in Section 1010 of the Evidence Code (e.g., psychiatrist, CSW, psychologist). Cal. Civil Code, § 56.10(c)(19). Additionally, disclosures of medical information to report a crime on the premises is permitted pursuant to Civil Code, § 56.10(c)(14), which generally allows disclosures "otherwise specifically authorized by law."

[22] *See, e.g.*, Pettus v. Cole (1996) 49 Cal.App.4th 402, 440.

[23] *See, e.g.,* Cross v. Superior Court (2017) 11 Cal.App. 5th 305, 325; Grafilo v. Soorani (2019), 41 Cal.App. 5th 497, 254.

[24] Cal. Assem. Bill 2091, 2021-2022 Reg. Sess. (2022).

[25] Cal. Assem. Bill 1242, 2021-2022 Reg. Sess. (2022).

[26] 45 C.F.R. part 171.

[27] 85 Fed. Reg. 25642, 25845 (May 1, 2020).

[28] The risk is also currently minimal because, even though the Information Blocking Rule took effect April 2021, regulations setting forth enforcement mechanisms with respect to health care providers have yet to be released as of October 2022.

[29] "Health and Social Services Information" broadly includes both PHI and medical information under HIPAA and CMIA as well as information related to the provision of social services even when it would not otherwise be PHI, in addition to de-identified data, anonymized data, pseudonymized data, metadata, digital identities, and schema.

[30] Raman R. Khanna et al., *Protecting reproductive health information in the post-Roe era: interoperability strategies for healthcare institutions*, J Amer Med Inform Assoc (2022).