Employee Relations
LAW JOURNAL

Navigating Data Privacy Questions Post-*Dobbs*

By Scott A. Weinstein, Jayda Greco, David Quinn Gacioch, Daniel F. Gottlieb and Carolyn V. Metnick

The authors examine the protections under the Health Insurance Portability and Accountability Act ("HIPAA") as well as other potential strategies that healthcare providers and application developers may use to protect the data of their patients and other users.

The U.S. Supreme Court's recent decision to overturn *Roe v. Wade* in *Dobbs v. Jackson Women's Health Organization* has raised many questions about potential efforts by law enforcement agencies to obtain data from healthcare and other service providers to detect the performance of a possibly unlawful abortion. For example, data collected by period-tracking apps, patients' self-reported symptoms, or diagnostic-testing results might be used to establish the timeframe in which an individual became pregnant, and then demonstrate that a pregnancy was terminated, as part of investigative or enforcement efforts against individuals or organizations allegedly involved in such termination.[1]

Scott A. Weinstein, a partner in McDermott Will & Emery, provides legal counsel on healthcare regulatory compliance, contracting and transactional due diligence. Jayda Greco is an associate at the firm whose practice is at the intersection of healthcare regulatory, privacy and compliance, product counseling and marketing law. David Quinn Gacioch, a partner in the firm, focuses his practice on healthcare litigation and enforcement defense. Daniel F. Gottlieb, a partner in the firm, counsels healthcare industry clients including healthcare providers, health plans, health information technology vendors, life sciences companies and data aggregators. Carolyn V. Metnick, a partner in the firm, represents healthcare industry clients including hospitals and health systems, physician organizations and digital health companies. The authors may be contacted at sweinstein@mwe.com, jgreco@mwe.com, dgacioch@mwe.com, dgottlieb@mwe.com and cmetnick@mwe.com, respectively.

On June 29, 2022, the office within the U.S. Department of Health and Human Services ("HHS") that is responsible for enforcing the Health Insurance Portability and Accountability Act ("HIPAA"), the Office for Civil Rights ("OCR"), issued guidance[2] addressing how HIPAA limits disclosures by covered entities and business associates to law enforcement agencies in the absence of a court order or other legal mandate. The guidance provides helpful insight on how OCR may use HIPAA enforcement to discourage unauthorized disclosures of protected health information ("PHI") to law enforcement officials in the wake of new state laws outlawing abortion. The guidance also implicitly confirms, however, that HIPAA does not provide a complete shield against law enforcement and litigation-driven requests for abortion-related information.

President Biden issued an executive order[3] on July 8, 2022, that in part aims to address privacy concerns related to reproductive healthcare and the limitations to HIPAA's current protections. President Biden's executive order calls on the Federal Trade Commission ("FTC") to consider steps to protect consumers' privacy when they seek information about the provision of reproductive healthcare services, and on the Secretary of HHS to consider additional actions, including under HIPAA, to protect sensitive information related to reproductive healthcare.

In this article, we examine the HIPAA protections discussed in the OCR guidance as well as other potential strategies that healthcare providers and application developers may use to protect the data of their patients and other users.

DISCLOSURES TO LAW ENFORCEMENT UNDER HIPAA

HIPAA permits covered entities and business associates to disclose PHI to law enforcement if certain conditions are met. Specifically, HIPAA permits disclosures in response to requests from law enforcement that are accompanied by a court order, a subpoena or summons issued by a judicial officer or grand jury, or an administrative agency request made under a similar process authorized under law. OCR emphasizes in its guidance that these are permitted rather than required disclosures under HIPAA. This means that although a covered entity's or business associate's failure to comply with a law enforcement request could, depending on the specific circumstances, constitute a violation of state law, it would not constitute a violation of HIPAA.

In the guidance, OCR reinforces that disclosures by covered entity or business associate workforce members to law enforcement regarding an abortion or an individual's reproductive healthcare absent a court order or other mandate enforceable in a court of law are violations of HIPAA. The guidance elaborates that its position on such disclosures "is true whether the workforce member initiated the disclosure to law enforcement or others *or the workforce member disclosed PHI at the request of law enforcement*."[4] OCR appears to be stressing that covered entities and business

associates could be cited with a HIPAA violation if they were to disclose PHI to law enforcement absent a qualifying subpoena, warrant or other legal mandate, even if a law enforcement agent had initiated the request.

OCR additionally notes that in the absence of mandatory reporting obligations under state law, covered entities and business associates would be prohibited by HIPAA from proactively reporting abortions or other reproductive healthcare to state law enforcement authorities.

OUT-OF-STATE SUBPOENAS

When a state law enforcement agency seeks information from a person or entity located in another state, the law enforcement agency will typically look to the state of the target person or entity to reissue a court-approved subpoena in accordance with the laws of the target state. All 50 states and the District of Columbia have passed the Uniform Interstate Depositions and Discovery Act ("UIDDA"), which establishes the necessary processes for reissuing subpoenas in this manner. In anticipation of the *Dobbs* decision, New York[5] and other states have enacted safe-harbor laws prohibiting courts in the state from issuing subpoenas in response to out-of-state law enforcement agency requests for assistance with abortion-related investigations where the alleged abortion-related conduct at issue would be legal if it occurred in New York. This is aimed at preventing prosecutors in states with abortion bans from seeking to issue and enforce out-of-state subpoenas related to abortions that are legal under the laws of the state being asked to assist in such efforts. We anticipate that other states will follow the lead of New York, Connecticut, California and others in passing similar laws that protect their residents from out-of-state subpoena requests.

Health systems, health plans, hospitals, telehealth providers and digital health application developers will need to carefully examine whether they are in a position to avail themselves of these protective state laws, or if they could be forced to respond to subpoena requests for the information concerning reproductive health care. They should consider the following questions:

- Does the company have any property or other physical presence in a state that has outlawed or will outlaw abortion, such that shield laws passed in other states arguably may not protect it?

- Are employees of the entity located in or licensed to provide care to patients in a state that has outlawed or will outlaw abortion?

- Does the company maintain any data storage facilities, servers or other patient records located in the state?

We expect that law enforcement officials within states that have banned abortion will seek to use any such connection or presence as leverage to issue and obtain compliance with subpoena requests relating to abortion services and associated reproductive health information. States with abortion bans may also look for opportunities to serve persons or entities that reside outside the state, such as when an officer of the company travels to a state with an abortion ban. Companies that wish to avoid responding to such subpoenas will therefore need to consult with their legal counsel to consider if there are any defenses they can raise against effective service or production of their customers' reproductive health information. For example, companies may consider reviewing the state's physician-patient privilege statute or regulation, as such laws could provide a good faith and potentially effective basis on which to resist production depending on the strength of the privilege protection in the state.

DATA MINIMIZATION

In response to the perceived threat of subpoena requests, companies that provide healthcare and healthcare-related services to women may also reexamine how they document reproductive health services. Some providers may avoid creating records that indicate a patient was considering an abortion, to the extent not required by law or contract to do so. Application developers may refine the information they collect and store through their applications, as well as their data retention policies, to limit the amount of information they retain that could reveal that a user sought or received reproductive health services, if they were to receive an enforceable subpoena or other law enforcement request. Healthcare providers and application developers should work closely with their legal counsel to examine proposed data minimization practices to ensure the effectiveness of such practices and confirm that they comply with federal or state medical record and document retention laws and sufficiently and accurately document services rendered for billing purposes.

Data minimization responses reflect that, in the age of smartphones and wearable devices, a growing amount of information collected every day could, if obtained by law enforcement officials, potentially reveal that a user obtained an abortion. Recognizing that consumers are concerned with this prospect, OCR issued a second guidance[6] document that outlines strategies and best practices for consumers to protect health data collected via smartphones and wearable devices. For example, OCR suggests that consumers can minimize their "digital footprint" by turning off location services and avoiding giving apps permission to access location data (unless necessary to operate the app). Additionally, the guidance suggests that consumers use communication apps, mobile web browsers and search engines that support increased privacy and employ security measures such as encryption.

Although consumer education and information collection transparency could help users make informed decisions about data-sharing settings on their devices, patients and application users will continue to look to providers and application developers to answer questions and concerns about data protection for reproductive health information. Healthcare providers and application developers should therefore consider updating their online privacy policies or posting information about their reproductive health information privacy practices to address potential patient and user information collection concerns, being careful not to overstate the protections that HIPAA and other state privacy laws provide against disclosure of health information to law enforcement.

NOTES

1. Most, but not all, states' post-*Dobbs* abortion prohibition laws exempt the patient who underwent the abortion from liability.

2. *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html*.

3. *https://www.whitehouse.gov/briefing-room/presidential-actions/2022/07/08/executive-order-on-protecting-access-to-reproductive-healthcare-services/*.

4. Emphasis added.

5. *https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislative-package-protect-abortion-and-reproductive*.

6. *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html*.