Professional Perspective

Health Care Privacy Concerns Post-Dobbs

Adam H. Greene, Davis Wright Tremaine

Bloomberg Law

Health Care Privacy Concerns Post-Dobbs

Contributed by Adam H. Greene, Davis Wright Tremaine

On June 24, 2022, the US Supreme Court released its opinion *Dobbs v. Jackson Women's Health Organization*, 142 S.C. 2228 (2022), reversing *Roe v. Wade* and holding that the US Constitution does not confer a right to abortion. While the decision was not a surprise after the leak of a draft months prior, it nevertheless sent shockwaves across the country.

In a number of states, abortion is now illegal or will be soon. Additionally, many states are considering laws that would prohibit residents from obtaining abortions in other states or could punish those who facilitate such procedures. The result has been a renewed focus on health information privacy, especially concerns that reproductive health information could form the basis of civil or criminal actions.

Tech Companies Respond

A number of technology companies have taken immediate action in the wake of *Dobbs* to protect the privacy of reproductive health information. On June 30, 2022, Flo Health announced the launch of an "Anonymous Mode" for its Flo app, a women's health app that boasts over 230 million users. On July 1, 2022, Google announced that it is implementing measures to automatically delete location history data indicating that an individual visited an abortion clinic, fertility center, or certain other particularly sensitive locations.

HIPAA Guidance

The US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), which administers and is the primary enforcer of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), also was quick to issue guidance addressing the *Dobbs* decision. On June 28, 2022, HHS Secretary Xavier Becerra directed agencies to take immediate action in response to the decision, including for OCR "to ensure patient privacy and nondiscrimination for patients seeking reproductive health care, as well as for providers who offer reproductive health care." In response, OCR issued two guidance documents on June 29, 2022, one focusing on entities covered by HIPAA and the other on safeguarding consumer information on personal devices that falls outside of HIPAA.

In the first guidance document, OCR details how the HIPAA Privacy Rule, which governs the use and disclosure of most individually identifiable health information held or transmitted by a covered entity or its business associate, applies to the privacy of information relating to abortions and other sexual and reproductive health care. The guidance states that:

- The Privacy Rule permits, but does not require, covered entities–such as health care providers–to disclose protected health information (PHI) when required by law, and the disclosure must be limited to the relevant requirements of the law. OCR clarifies that a law that permits but does not expressly require reporting of PHI would not qualify for this Privacy Rule permission.

- The Privacy Rule does not require a covered entity to disclose PHI to law enforcement and does not permit a covered entity or its workforce member to report an individual's abortion or other reproductive health care to law enforcement in the absence of a mandate enforceable in a court of law.

- The Privacy Rule's permission to disclose PHI to avert a serious threat to health or safety requires that the disclosure be consistent with applicable standards of ethical conduct, and it would be inconsistent with professional standards of ethical conduct of the American Medical Association and American College of Obstetricians and Gynecologists to disclose PHI to law enforcement or others regarding an individual's interest, intent, or prior experience with reproductive health care.

The Privacy Rule permits a covered entity to disclose protected health information in response to a law enforcement official's "administrative request" that includes the following elements:

- The information 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
- De-identified information could not reasonably be used

Prior OCR guidance regarding this permission stated that such an administrative request "may be made without judicial involvement" as long as there was a written statement with the above elements.

OCR has revised this law enforcement guidance, however, to remove the reference to a lack of judicial involvement, and the new guidance related to *Dobbs* indicates 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."

Accordingly, OCR appears to have changed its interpretation of what constitutes an "administrative request" under the Privacy Rule's permission for disclosures to law enforcement. In light of this new guidance, it seemingly would be high risk under HIPAA for a covered entity to disclose reproductive health information to law enforcement based on a written statement unless the administrative request is enforceable in a court of law.

Overall, the theme of the OCR guidance regarding covered entities is that there are limited circumstances in which a covered entity may disclose PHI regarding an abortion or reproductive health services to law enforcement or others who might use the information to prosecute the patient or others, and that any such disclosure is never required by HIPAA itself.

The second OCR guidance document focuses on the privacy of health information on personal devices that falls outside of HIPAA. The guidance warns individuals that their sensitive reproductive health information generally is not protected by HIPAA when on a personal device. OCR provides some suggestions for safeguarding such information, such as:

- Avoid downloading unnecessary or random apps, especially free ones, that could put personal data on the app and health information on the device at risk.
- Avoid allowing apps to access location data other than when such data is absolutely necessary for the app to function, such as navigation and traffic apps that require location data to function.
- Use communication apps, mobile web browsers, and search engines that are recognized as supporting increased privacy and security, such as through encryption, limiting tracking tools, and that do not collect and store personal information

The OCR guidance provides specific instructions for Apple iOS and Google Android users regarding how to adjust certain settings to better protect privacy and security of data and provides additional resources from other government agencies—such as the FTC—and private entities.

Calls to Amend Privacy Rule

Even with this guidance, though, concerns regarding HIPAA and reproductive health information remain. For example, while the June 29 guidance indicates that a disclosure to law enforcement is only permitted if accompanied by a "mandate enforceable in a court of law," the regulatory text does not explicitly provide that a law enforcement official's "administrative request" must involve a court.

The new guidance also does not address the Privacy Rule's permission for a covered entity to disclose certain identifying PHI about an individual in response to a law enforcement request to locate a suspect, fugitive, or material witness. The concern is that law enforcement officials in states that ban abortion could broadly request information about individuals who obtain services out of state, and a covered entity's workforce member could respond by notifying law enforcement of reproductive health services against the wishes of the patient.

Additionally, while OCR was quick to publish guidance in the wake of *Dobbs*, two senators have written to HHS seeking significantly more action with respect to HIPAA. Senators Michael Bennet (D-Colo.) and Catherine Cortez Masto (D-Nev.) praised OCR for its guidance but urged HHS to go further, updating the Privacy Rule to clarify:

- Who is a covered entity and to limit when that entity can share information or other reproductive health services
- That this information cannot be shared with law enforcement agencies who target individuals who have an abortion
- That pregnancy care centers, also known as crisis pregnancy centers, are required to follow the Privacy Rule

Impact of Information Blocking Rule

While the Privacy Rule never requires a covered entity to disclose reproductive health information, its permission to disclose this information, including to law enforcement, now needs to be considered in light of the 21st Century Cures Information Blocking Rule, 45 C.F.R. part 171. If a law enforcement official requests electronic health information that includes reproductive health information, any denial or delay in providing this information may implicate the Information Blocking Rule.

There is an exception for preventing harm, but when the requestor is a third party, such as a law enforcement official, then the harm exception generally requires a reasonable belief that providing the access would endanger the life or physical safety of the individual or another person. The risks posed by providing access to law enforcement are unlikely to rise to this level– the risk of physical harm. The lower standard of "substantial harm" to the patient currently is not applicable for law enforcement requests and other third party requests.

Another potentially applicable exception is the privacy exception. Where a disclosure to law enforcement is permissible under applicable privacy laws, the privacy exception generally will not apply. But the privacy exception does exempt a denial of access if the patient requests that the health care provider not provide such access, the health care provider documents the request within a reasonable time period, the health care provider's practice is implemented in a consistent and non-discriminatory manner, and if the restriction can only be terminated if certain criteria are met.

Additionally, if HIPAA permits a disclosure to law enforcement but a state law prohibits such disclosure or includes additional conditions, then compliance with the state law would not be information blocking. If a health care provider operates in multiple states, then it would not be information blocking for the provider to maintain a national set of policies that complies with the most restrictive state laws.

Finally, under the statute and regulation, a health care provider only violates the Information Blocking Rule if it knows its practice to be unreasonable. Here, a health care provider can deny access to law enforcement and take the position that it believed its denial was reasonable.

In practice, the current risk under the Information Blocking Rule with respect to withholding reproductive information from law enforcement may be minimal. First, while the Information Blocking Rule is in effect, HHS has not yet promulgated regulations setting forth enforcement mechanisms with respect to health care providers. Accordingly, the risk of enforcement is very low. Additionally, even if enforcement mechanisms were in place, the current administration is unlikely to bring an enforcement action against a health care provider for refusing to provide reproductive health information to law enforcement. Furthermore, HHS currently is unlikely to claim that a health care provider knew such a practice to be unreasonable.

The biggest risk is with a change in executive administration. A future administration could take a very different posture with respect to reproductive health information and law enforcement and could potentially claim that any denial of access to law enforcement where legally permissible constitutes information blocking.

Protecting the Privacy of Reproductive Health Information

In light of *Dobbs*, it clearly is time to rethink how to address the privacy of reproductive health information. One potential analogy is substance use disorder (SUD) information. While SUD information is protected by the HIPAA Privacy Rule, it is also subject to the significantly more stringent regulations in 42 C.F.R. part 2 (the Part 2 Rule). Health care providers find it exceedingly difficult to sufficiently lock down SUD information in accordance with the Part 2 Rule, and there have been calls to revise the Part 2 Rule, with one article from a leading health care journal calling it "outdated." In an online comment responding to this article, the now former director of the Substance and Mental Health Services Administration clarified why SUD information merits different treatment then other types of sensitive health information:

It is illegal to use heroin; it is not illegal to have diabetes. It is illegal to use marijuana; it is not illegal to be depressed. It is illegal to use street methamphetamine; it is not illegal to have hypertension. It is illegal to use PCP; it is not illegal to be obese. … It may be inconvenient for the health care delivery system to ask a patient for permission to codify information that could incriminate them in a legal forum, but it is disingenuous for health care providers to ignore the risk of disclosure of such information to the medical record.

Unfortunately, the health care system may need to start thinking about reproductive health information in the same manner and create new rules to ensure that such information is not used to prosecute a patient, or someone involved in the patient's care.

To start, health care providers could take a few steps:

- Health care providers may wish to review and revise their policies on disclosures of PHI to law enforcement. For example, if a policy permits disclosure of PHI to law enforcement based on a non-judicial "administrative request" accompanied by a written statement with the three statements specified in 45 C.F.R. § 164.512(f)(1)(ii)(C), then the health care provider may want to revise the policy to better align with OCR's new guidance, prohibiting disclosure absent a court mandate. If the policy permits disclosure of limited PHI in response to a law enforcement request to identify a suspect, fugitive, or material witness, then the health care provider may revise the policy to prohibit such disclosures without the privacy officer's approval or when the law enforcement request pertains to reproductive health services.

- The Privacy Rule requires a covered entity to sanction a workforce member who fails to comply with the Privacy Rule or the covered entity's privacy policies and procedures. If a health care provider implements more stringent policies than HIPAA with respect to disclosing reproductive health information to law enforcement, then the provider may notify workforce members of the sanctions that will be imposed for violating these policies.

- Providers could consider asking patients who receive certain reproductive health services whether they would like to request a restriction on disclosure to law enforcement. If a patient chooses to request such a restriction and the health care provider agrees to it, then denial of a law enforcement request for the information may satisfy the privacy exception to the Information Blocking Rule. Of course, a health care provider should only follow this path if it can implement the restriction.

Additionally, HHS could consider regulatory changes:

- Instead of locking down reproductive health information in the same manner as SUD information—which may impair care and is difficult to implement—HHS could consider creating targeted changes to the Privacy Rule that prohibit the disclosure of reproductive health information to law enforcement or state courts unless the patient provides written consent. The HIPAA statute seemingly provides HHS with discretion to preempt state laws, including state court orders, to the extent that they are contrary to the Privacy Rule and offer less privacy protection.

- HHS could revise the Information Blocking Rule to include an exception for disclosing certain categories of especially sensitive health information, such as 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.

With these steps, health care providers and HHS could help individuals obtain safe reproductive health services in states where it is legal without the information being used for prosecutions in states where it is not.