Proskauer

Privacy Post-Dobbs

Health Care Law Brief on **July 8, 2022**

Fifty years of legal precedent established by *Roe v. Wade,* 410 U.S. 113 (1973), and *Planned Parenthood of Southern Pa. v. Casey,* 505 U.S. 833 (1992), were overturned in *Dobbs v. Jackson Women's Health Organization*, holding that the Constitution does not confer a right to abortion and leaving abortion laws to individual states to decide. This new landscape has introduced a wave of legal questions, and among these are questions regarding the protection of personal information related to abortion and contraceptive services. In efforts to address some of these privacy questions, the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") published new guidance with respect to the Health Information Portability and Accountability Act (HIPAA) Privacy Rule ("Privacy Rule"). The new HIPAA guidance generally reminds providers about their obligations under the Privacy Rule to safeguard patients' protected health information ("PHI"), even under many circumstances where the information has been requested by government officials or in the context of litigation. In addition, recognizing the extent to which patient information is held on patients' personal smartphones and not protected under HIPAA (e.g., data entered into personal health apps, search history related to abortion and other reproductive care, and geolocation data), yet may be relevant under new criminal and civil state abortion laws, HHS issued supplemental guidance to consumers on how to protect and secure personal information on phones and tablets that is not otherwise protected by HIPAA.

Under the Privacy Rule, disclosure of PHI without patient authorization is permitted only in "narrow circumstances", and disclosure of PHI to law enforcement is limited based on the facts and the nature of the requests (e.g., court-ordered warrant, subpoena, or to prevent or lessen a "serious and imminent threat to health or safety.")[1] The Privacy Rule expressly defers to a provider's professional judgement in determining what constitutes a "serious and imminent threat";[2] however, per the guidance, OCR has clarified that it is "inconsistent with professional standards of ethical conduct to make such a disclosure of PHI to law enforcement or others regarding an individual's interest, intent, or prior experience with reproductive health care."[3] Moreover, the "narrow circumstances" for disclosure include, but are not limited to, efforts to:

- Comply with a court order, court-ordered warrant, subpoena, summons issued by a judicial officer, or a grand jury subpoena (45 CFR 164.512(f)(1)(ii)(A)-(B);
- Respond to an administrative request[4] ((45 CFR 164.512(f)(1)(ii)(C));
- Report PHI that a covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises (45 CFR 164.512(f)(5));
- Respond to a request for PHI about a victim of a crime, and the victim agrees (45 CFR 164.512(f)(3)); and
- Report PHI to law enforcement when required by law to do so (45 CFR 164.512(f)(1)(i)).

Thus, absent a court order, the Privacy Rule's exceptions to disclose PHI for law enforcement purposes do **not** permit disclosure to law enforcement where a hospital or health care provider wishes to report an individual's abortion or other reproductive health care. Thus, a hospital employee who suspects a patient of having an abortion in a state where it is illegal cannot report the planned abortion to law enforcement unless a state law specifically requires such reporting. HHS clarifies that a statement indicating an individual's intent to get a legal abortion, or any other care tied to pregnancy loss, ectopic pregnancy, or other complications related to or involving a pregnancy does **not** qualify as a "serious and imminent threat to the health and safety" of a person or the public.[5] Disclosing such information to law enforcement under such circumstances would be impermissible and would constitute a breach of unsecured PHI, requiring notification to HHS and the individual affected.[6]

And, while the Privacy Rule generally **does not** protect the privacy or security of an individual's health information when it is accessed through or stored on a personal cell phone or tablet, guidance released last week by HHS outlined how individuals can protect themselves. The Privacy Rule only applies when PHI is created, received, maintained, or transmitted by covered entities and business associates (e.g., health care providers and health insurers), and does not extend to protecting the privacy of an individual's Internet search history, any information that one voluntarily shares online, or an individual's geographic location information. Consequently, the guidance sheds light on the ways one can protect their digital footprint and decrease how devices collect and share health and personal information.

Moreover, in response to the *Dobbs* decision and increasing concerns that personal data will be used to incriminate people seeking abortions, Sen. Elizabeth Warren, supported by a slate of five Democratic senators, proposed the passing of the Health and Location Protection Act to bar "data brokers from selling or transferring location data and health data." If approved, the bill would permit the Federal Trade Commission and states' attorneys general to sue brokers found to be in violation of the law. Notably, the legislation would include exceptions for compliance with HIPAA.

The legislative and regulatory landscape addressing abortion and reproductive health services is certain to change in the near future as states respond to the *Dobbs* decision. As granted by *Dobbs*, states will now have the authority to enforce their own abortion rules, which creates an opportunity for widely varying state statutes, penalties, exceptions, circumstances, and a variety of other consequences across the country. Health care providers that provide a full spectrum of women's health care services, including abortion, will need to review their policies and procedures to ensure compliance with state laws and to understand how the *Dobbs* decision affects the care they can provide to patients. Providers should be familiar with the new guidance to verify the circumstances under which HIPAA permits the disclosure of PHI without patient authorization.

Proskauer is available to assist with addressing the short- and long-term implications of the *Dobbs* decision in the wake of forthcoming regulatory changes.

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

[2] https://www.hhs.gov/hipaa/for-professionals/faq/3002/what-constitutes-serious-imminent-threat-that-would-permit-health-care-provider-disclose-phi-to-prevent-harm-patient-public-without-patients-authorization-permission/index.html

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

[4] Provided that: 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; **and** de-identified information could not reasonably be used.

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

[6] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

View Original