NOW & NEXT

Healthcare & Data Privacy Alert

JULY 12, 2022

Data privacy in the post-*Roe* era

By Valerie Breslin Montague, Jenny Holmes, Meredith LaMaster, and Sarah Swank

Roe's reversal disrupts settled expectations regarding the privacy of women's health information—and the role of healthcare practitioners, app developers, and cell phone providers in protecting it.

What's the Impact?

- In the post-*Roe* era, individual states will be responsible for legislating abortion
- With many states looking to enact complete abortion bans with criminal penalties, physicians, app developers, and other service providers could be subpoenaed to provide personal and health data to aid law enforcement in prosecuting those who seek out abortions

On June 24, 2022, SCOTUS overturned *Roe* through its landmark decision in *Dobbs v. Jackson Women's Health Organization* (*Dobbs*). As a result, states are now responsible for deciding the future of access to abortion and other critical reproductive health services for the first time in nearly 50 years. While some states have previously enacted "trigger laws" to ban abortion entirely with the expectation that *Roe* may be overturned, others have codified the right to choose through their state legislatures, leaving many women's health choices in flux. Numerous women's reproductive rights groups have filed lawsuits and temporary restraining orders in state

courts across the country to prevent these trigger laws from going into effect. While the judicial landscape currently remains murky, healthcare practitioners, app developers, and cell phone providers are left in a precarious position in states where, moving forward, individuals seeking out abortions, the doctors that perform them, and individuals that assist them in the process are at risk of being prosecuted by law enforcement.

Background

On January 22, 1973, SCOTUS issued a 7-2 decision in the case of Jane Roe versus Henry Wade, ruling that the Due Process Clause of the Fourteenth Amendment provides individuals with a fundamental right to privacy. The ruling was not without controversy, with pro-life groups advocating for the overturn of *Roe* since its inception. On June 24, 2022, SCOTUS handed down a 6-3 decision in *Dobbs*. In the majority opinion authored by Justice Samuel Alito, SCOTUS reasoned that the right to abortion was not considered when the Due Process Clause was ratified in 1868 and, therefore, not rooted in the country's history or tradition.

With the new *Dobbs* decision comes a number of data privacy questions, particularly what, if any, data healthcare practitioners, app developers, and cell phone providers are required to disclose to law enforcement. These questions could arise in states where women and doctors may now be prosecuted for seeking out and providing abortions. Additionally, for those persons that travel to states where abortion is still legal, individuals who assist them in obtaining the abortion can potentially be charged with aiding and abetting residents of a state in the state in which the individual ending their pregnancy resides. Uncertainty faces individuals in light of this decision because previously legal reproductive services are replaced in some states with warnings for women to delete ovulation and menstrual cycle apps on their phones, to leave phones at home when visiting doctors, and to practice caution with online searches.

Healthcare Practitioners

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Privacy Rule)

Under the protections of the HIPAA Privacy Rule, individuals who solicit information on abortion and other sexual healthcare can largely be assured that their protected health information (PHI) will remain private.[12] Administered and enforced by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the Privacy Rule establishes requirements for covered entities, including most healthcare providers, healthcare clearinghouses, and health plans (Covered Entities)[3], regarding the use, disclosure, and protection of PHI. PHI includes demographic information that can used to identify an individual, such as their name, address, age, Social Security number, health history, diagnoses and conditions, email address, and past,

[1] 45 C.F.R. Part 160 and Subparts A and D of Part 164.

[2] 45 C.F.R. § 160.103.

[3] *Id.*

present, or future physical or mental health or condition.[4] The Privacy Rule also extends to a Covered Entity's vendors who receive or access the Covered Entity's PHI on their behalf (Business Associates), in that a Business Associate may only use or disclose PHI as allowed under HIPAA and their agreement with a Covered Entity or as allowed under the law.[5] Without an authorization signed by the individual, Covered Entities may only use or disclose PHI as expressly allowed by the Privacy Rule. Designed to shield privacy rights and promote access to healthcare services, only certain disclosures may be made to law enforcement officials without a person's permission when the disclosure is not for purposes of healthcare. On June 29, 2022, OCR promulgated guidance regarding disclosures of PHI related to abortion and reproductive healthcare.

Disclosures required by law

The Privacy Rule allows, but does not require, that Covered Entities disclose an individual's PHI, without the individual's authorization, when the disclosure is mandated under another law and the disclosure complies with the requirements of that law.[6] Permissible PHI disclosures under other laws are restricted to those persons required under that specific law when required to make a court-enforceable disclosure.[7] The only information that may be disclosed is what is required by that other law. Any requested disclosures that fall outside the "required by law"[8] definition outlined in the HIPAA regulations, or that go beyond the scope required under the law, are not considered permissible disclosures.

In its guidance, OCR presents a scenario where an individual must obtain emergency care at a hospital due to miscarriage complications during their tenth week of pregnancy and a hospital employee suspects that the individual took medication to induce the miscarriage. If state law bans abortions after six weeks but does not outwardly require hospital employees to report the incident to law enforcement, OCR states that such disclosure is not permissible under the Privacy Rule's "required by law" exception. If hospital personnel nonetheless make a report to law enforcement, it would be a breach of unsecured PHI on the part of the hospital that would require notification to OCR and to the patient.

Disclosures to law enforcement

Similarly, the Privacy Rule allows for, but does not require, PHI disclosures to law enforcement "pursuant to process and as otherwise required by law."[9] A Covered Entity is able to respond to requests obtained through court orders and court-ordered warrants, as well as court-ordered subpoenas and summons; provided, however, that the entity may only disclose the requested PHI so long as all Privacy Rule required conditions have been satisfied.

---

[4] *Id.*

[5] 45 C.F.R. § 164.502 (a)(3).

[6] 45 C.F.R. § 164.512(a)(1).

[7] 45 C.F.R. § 164.103.

[8] *Id.*

[9] 45 C.F.R. § 164.512(f)(1).

Unless there is a mandate enforceable in court that compels the disclosure, a Covered Entity's employee, workforce member, or Business Associate may not report individual abortions or other reproductive health decisions to law enforcement. This applies to instances where the employee of the Covered Entity initiated the disclosure to law enforcement and those where the disclosure is made at the request of law enforcement. As noted in OCR's guidance, these are considered impermissible disclosures because state laws largely do not require that physicians or other employees report individuals to law enforcement when the individual induces an abortion. The guidance further explains that most state fetal homicide laws are not designed to penalize pregnant persons and appellate courts have largely refused to use existing laws enacted for other purposes as mechanisms to punish pregnant individuals.

OCR provides another example of the application of the privacy rule when law enforcement personnel visit a reproductive health clinic and request records of abortions performed at the clinic. Without a court order or some other sort of legal mandate, it would be impermissible under HIPAA for the clinic to honor law enforcement's request and disclose patient PHI. Such disclosure would be considered a breach of unsecured PHI and would require notification to OCR and any affected patients. If law enforcement does have a court order requiring the clinic to provide information about individuals who have received abortions, the Privacy Rule would permit but not require the clinic to disclose the PHI. The disclosure must be limited in scope to the PHI requested by the court order. As further discussed below, although HIPAA does not require a PHI disclosure in this circumstance, the Covered Entity could face legal liability if it fails to comply with a court order or other legal mandate.

Disclosures to avert serious health or safety threats

When serious threats to an individual or the general public's health or safety emerge and require de-escalation, the Privacy Rule allows, but again, does not require, Covered Entities to make lawful, ethical disclosures of PHI to those who can aid in the de-escalation process.[10] OCR notes in its guidance, however, it is largely seen as unethical by the major professional societies to make disclosures to law enforcement regarding a person's reproductive health interests and intentions.[11]

In the guidance, OCR discusses a scenario of an individual residing in a state with a total abortion ban. In this scenario the individual alerts their medical provider of their intent to terminate their pregnancy in a state where abortion is legal. OCR states that it would be impermissible under HIPAA for this purpose for the provider to disclose the patient's PHI to alert law enforcement of the individual's interest in seeking an abortion. Among other reasons, OCR notes that a legal abortion does not represent a serious threat to the individual's or general public's health and safety. Indeed, the disclosure could be seen as unprofessional because of its impact on the patient-physician relationship and the potential for harm to the affected individual. As such, this

---

[10] 45 C.F.R. § 164.512(j).

[11] See American College of Obstetricians and Gynecologists, *Decriminalization of Self-Induced Abortion* (Dec. 2017); see also American Medical Association, *Unconstitutional attack on reproductive health must not stand* (Oct. 13, 2021).

type of disclosure is seen as a breach of unsecured PHI requiring notification to OCR and the affected patient.

Permitted versus required or must protect

Although the HIPAA Privacy Rule does not *require* disclosures that are (i) required by law, (ii) to law enforcement, or (iii) to avert serious health or safety threats, and although the recent OCR guidance repeatedly references that Covered Entities are *permitted*, but not *required*, to make such disclosures, it is important to note that Covered Entities may be at risk for court sanctions or other legal liabilities if they are legally required or compelled to produce information and fail to do so. The Privacy Rule is not a shield or defense that a Covered Entity can use to decline to disclose protected health information if the requesting party complies with the parameters of a HIPAA exception.

On the other hand, states can provide additional protections related to the confidentiality of women's reproductive health information. Under its preemption provisions, HIPAA defers to state laws that provide greater confidentiality to individuals. For example, in New York, Article 27-F provides for greater privacy protections than HIPAA for the confidentiality and privacy of individuals being tested, exposed to or treated for HIV. Under the New York State law, any individual or facility covered by the law *must* keep that information confidential even if HIPAA were to permit its disclosure.

Covered Entities should carefully review the legal authority presented with requests for PHI and ensure that they have a clear understanding of their legal obligations to disclose or protect health information regarding an individual prior to responding to a request.

App developers and cell phone providers

Another area of concern in light of the *Dobbs* decision is data stored on an individual's cell phone or tablet. Unless PHI is created or transmitted through a Covered Entity or their Business Associate, it is generally not protected under HIPAA. In fact, browser search histories, posts in public online forums, and location tracking information are not covered by HIPAA. Similarly, if an app is utilized to store health information or track a menstrual cycle for personal use, it is not protected unless provided by a Covered Entity or its Business Associate. On June 29, 2022, OCR issued guidance offering tips on how an individual can protect themselves when using health apps or accessing or storing their PHI or personal information on their cell phone or tablet.

In fact, many mobile applications utilize personal information for commercial and other purposes beyond the reason individuals provided such information. There is no overarching federal law that prevents such uses. Rather, individual states such as, California, Virginia, Colorado, Connecticut, and Utah have developed comprehensive consumer privacy laws to protect their residents. Yet, for most, companies can use and disclose personal information consistent with their public privacy policies.

Many companies can freely disclose personal information received from an app to law enforcement with or without a subpoena. Companies could also choose to sell this data to the

government. In the days since *Dobbs* was decided, many called upon women to delete their cycle tracking apps out of fear that prosecutors could use this information to build a case against a woman who received an abortion.

Many of these apps made public statements, pointing to their published privacy policies, promising that they would not sell or disclose user information without a valid subpoena. However, many apps are going a step further and seeking ways to anonymize user data so that even in the case of a subpoena, the information would not identify any specific individual. Further, cell phone providers collect geolocation data that could be used to place an individual at an abortion clinic. Other providers may have access to an online search history that could also be used as circumstantial evidence in building a case against a woman. These companies must decide their course of action in the event of a law enforcement request for this information and should develop clear policies outlining their practices. It is advisable that any public-facing privacy policies or other statements are up-to-date and aligned with current practices, informing the user of any disclosures of personal information.

Although app developers and cell phone and other service providers may fall outside of HIPAA regulation, Section 5 of the Federal Trade Commission (FTC) Act prohibits unfair and deceptive trade practices. Privacy has long been a consumer protection priority for the FTC. On July 11, 2022, the acting associate director of the FTC's Privacy and Identity Protection Division stated in a blog post that the FTC will "vigorously" enforce the law if it finds illegal conduct that exploits an individual's location or health data. The acting associate director adds, "The misuse of mobile location and health information – including reproductive health data – exposes consumers to significant harm."

Takeaways

While the post-*Roe* landscape continues to evolve, it is important to consider the impact of the *Dobbs* opinion on the legal requirements related to the legal privacy requirement of personal information. Companies keep up to date on federal and state laws and guidance related to the application of their current policies, including their privacy policies and data management policies. These policies should align with real-life practices and a changing legal landscape. Personnel, particularly those at healthcare provider organizations, should be trained on what is and is not a permissible disclosure of PHI and personal information, particularly because the HHS Secretary has indicated that enforcement of privacy violations related to reproductive health is a priority for HHS. As we wait and see the extent to which law enforcement will seek PHI and personal information to enforce these bans, entities should take proactive steps to protect user information.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Meredith D. LaMaster
312.977.9257
mlamaster@nixonpeabody.com

Sarah Swank
202.585.8500
sswank@nixonpeabody.com