NELSON HARDIMAN
HEALTHCARE LAWYERS

Client Alert: A Priority Telehealth Update – Data Security, Privacy, and Physician-Patient Confidentiality Post-Dobbs

A Priority Telehealth Update: Data Security, Privacy, and Physician-Patient Confidentiality Post-*Dobbs*

The Supreme Court's June decision in *Dobbs v. Jackson Women's Health*, overturning *Roe v. Wade*, gave states the authority to criminalize abortion. So far, eleven states have adopted laws prohibiting abortion immediately after conception, and two others have bans effective after six weeks of pregnancy. These statutes have triggered multiple dilemmas related to medical privacy. Patients who live in abortion-prohibitive states are now worried if what they share with their physician will be kept in confidence if it concerns personal reproductive decisions. Clinicians are struggling with what changes they need to make to protect patient privacy and conflicts between accepted standards that guide physician-patient recordkeeping and a new concern for greater assurances of privacy. Entities processing and storing patient medical data (i.e. providers, insurers, third-party data brokers) are scrambling to implement clear guidelines to navigate situations where state law enforcement requests may conflict with privacy requirements mandated by state and federal law.

"Can I Trust My OB/GYN?"

One of the arguments made by physician organizations in *Dobbs* was that overturning *Roe* would have a chilling effect on the physician-patient relationship. In *Roe*, the Court recognized that a right of privacy, originating from the Fourteenth Amendment's concept of personal liberty, was "broad enough to encompass a woman's decision whether or not to terminate her pregnancy." This is no longer the case. *Dobbs*' reversal of *Roe* significantly narrowed the scope of privacy as a constitutionally protected right, allowing state governments to restrict the personal decisions and medical options available related to terminating a pregnancy. This created an immediate conundrum for patients, living in restrictive states, who would like to discuss their circumstances and explore options with their personal physician. It has become harder for clinicians and patients to have candid conversations and for providers to offer advice, even when an abortion is thought medically necessary, in fear that anything said may trigger a risk of potential liability. Patients may feel the need to withhold vital personal medical information, lest a healthcare professional become a willing or even unwilling source of information about violating abortion laws. How can a patient make "informed" healthcare decisions if the patient is reluctant to disclose relevant medical history or a doctor refrains from discussing both in-state and broader out-of-state health choices?

Can Law Enforcement Demand Personal Medical Information?

For the healthcare community, state abortion bans raise difficult questions concerning how law enforcement officials may seek abortion-related personal health records from providers, health-plans, mobile devices, or third-party sources when investigating abortion-related violations of state law. Medical practice today is governed by multiple layers of privacy statutes, regulations, and protections including HIPAA, state medical privacy laws, and state consumer privacy laws. Depending on the circumstances, providers may be prohibited, permitted, or lawfully required to share a patient's personal medical information (PMI) with state investigators. Many providers are likely to test these laws by conscientiously objecting to providing information.

Following *Dobbs*, the Office of Civil Rights (OCR) released **HIPAA Privacy Rule Guidance** regarding when abortion disclosures are required by law. OCR discusses a scenario where a "pregnant individual in a state that bans abortion informs their health care provider that they intend to seek an abortion in another state where abortion is legal." According to the OCR, the Privacy Rule would not permit a provider to report the statement to law enforcement in "an attempt to prevent an abortion from taking place." Some of OCR's scenario guidance will likely be tested in court. For example, the guidance notes that a court order from law enforcement in a hostile state to a reproductive health care clinic, the HIPAA Privacy Rule may permit but will not require the clinic to disclose the requested PHI." Providers may be caught in a Catch-22 if state law requires disclosure while federal regulatory guidance deems compliance voluntary or outright prohibited.

Can Digital Medical Data Be Protected?

Text messages, emails, and private messaging over social media can be used as evidence of an unlawful abortion if collected by law enforcement. Recently, police in Nebraska used online communication as part of their investigation into an alleged abortion. To avoid receiving warrants concerning unlawful abortions, Apple decided to shift data collection to "local storage only" for its fertility tracking tools on its newly released Apple Watch Series 8. For providers, the entire medical field is moving toward greater levels of cloud-based integration.

Unfortunately, software programs like DoseSpot, which allows physicians to see prescribing history for a common patient, as well as e-prescription platforms like SureScript, are distinctively vulnerable to law enforcement searching for evidence of a medication abortion. The same may be said for the host of technology companies, such as Epic, Meditech, or Optum, that provide electronic health record (EHR) solutions. Ironically, from the standpoint of good medical outcomes, patients are usually better off when their clinicians can access one another's treatment records for a shared patient. Against this trend, women's healthcare providers that want to better protect patient privacy may decide to step away from cloud-based platforms, reverting to firewalled local data storage systems or even paper records.

Medical Ethics and State Law

As state abortion bans take effect, it remains an open question how accompanying law enforcement actions will impact the medical profession's nationally shared privacy standards that have long-been the backbone of provider-patient interactions. According to the AMA's Code of Ethics, physicians are obliged to safeguard what a patient shares in confidence lest the patient withhold critical health information. Where states make it unlawful to assist or aid in the obtainment of an abortion, clinicians face a dilemma whenever their duty to furnish or recommend a type of abortion-related care that is in the patient's "best medical interest" is specifically barred by state law. Clinicians and providers may need to consider novel strategies to best protect physician-patient confidentiality and general patient privacy while still operating "within the constraints of the law."

For the latest on post-*Dobbs* privacy issues, join Nelson Hardiman for Part IV of our Telemedicine Abortion Webinar Series, focusing this month on Data Security, Privacy, and Physician-Patient Confidentiality post *Dobbs*. Register Here

Authored By:

Harry Nelson, Managing Partner, Nelson Hardiman
Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP, Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at every point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact us.