Protecting the Privacy of Reproductive Health Information After the Fall of Roe v Wade

Kayte Spector-Bagdady, JD, MBE; Michelle M. Mello, JD, PhD, MPhil

The Supreme Court's decision in Dobbs v Jackson's Women's Health Organization, eliminating federal protection for abortion rights recognized since 1973 in Roe v Wade, will trigger the adoption and enforcement of numerous state laws banning or restricting abortion. The most pressing concerns for physicians and health care facilities are how to minimize these laws' adverse effects on patients and provide quality reproductive health care within legal limits. Yet, another vital issue also merits attention: How can clinicians and facilities protect their patients—and themselves—from having reproductive health information used to incriminate them?

New abortion restrictions may clash with privacy protections for health information in 3 ways. And despite popular misconceptions about the breadth of the Privacy Rule of the Health Information Portability and Accountability Act (HIPAA) and other information privacy laws, current federal law provides little protection against these scenarios.

First, using a patient's medical records to support legal action against those seeking, obtaining, or abetting an abortion may be possible. HIPAA protects individually identifiable health information in electronic records controlled by a "covered entity" (a clinician or facility, health plan, or health care clearinghouse) against disclosure without the patient's authorization, but it contains notable exceptions. These include reporting child abuse or neglect to an "appropriate government authority"; responding to a court order, subpoena, or discovery request for information relating to a lawsuit; and giving information to law enforcement officials "as required by law." Thus, HIPAA does not bar compliance with child abuse or neglect reporting requirements, nor will it shield entities that defy investigative demands for information for law enforcement or other legal purposes.

Nor do other legal rules predictably provide protection. Securing a search warrant in conformance with the Fourth Amendment requires only "probable cause" to believe the search will uncover evidence of a crime. Subpoenas can be quashed if they are unreasonable or overbroad, but these are notoriously loose requirements. Thus, law enforcement officials may be able to use a subpoena to obtain patients' medical records related to abortions. State statutes generally designate confidential communications or other information arising within a patient-physician relationship as privileged and therefore inadmissible in legal proceedings. However, this privilege is not absolute, its scope varies greatly across states, and in many cases medical record information has been successfully used to substantiate a criminal charge, such as child abuse. Thus, there is substantial uncertainty about how courts will address assertions of physician-patient privilege relating to reproductive health care records. Indeed, when former Attorney General John Ashcroft sought hospital records of late-stage abortions when defending the Partial-Birth Abortion Ban Act of 2003, reviewing courts all reached different decisions.

A second privacy concern is the potential use of health care facility records to incriminate an institution or its clinicians for providing abortion services. Relevant records could include electronic health records, employee emails or paging information, and mandatory reports to state agencies. Furthermore, HIPAA permits disclosure of protected health information to a health care regulatory agency in connection with civil, administrative, or criminal investigations or disciplinary actions relating to a practitioner's or facility's health care provision—for instance, a state board of medical licensing investigating whether a physician provided illegal abortions.
Many clinicians may not realize that if they are using an institutional email address or server, their institution likely has direct access to information and communications stored there, which can be used to search for violations. State Freedom of Information Act (FOIA) laws also allow citizens to request “public records” related to an official function from employees of government hospitals and clinics. Although exceptions exist for information that would invade an individual’s privacy (eg, individual patient medical information), FOIA requests could sweep in email discussions regarding the provision of abortion care generally. As to mandatory reporting, most states require facilities to send detailed data on the volume and nature of abortion services provided, and some require the reason for providing abortions. Although patients’ names are removed, many potentially identifying characteristics remain. This information, too, is useful for law enforcement and may be subject to FOIA requests. In addition, state mandatory reporting laws for child abuse might be interpreted to cover abortions—particularly if life is defined as beginning at fertilization.

A third concerning scenario is that information generated from a person’s online activity could be used to show that they sought an abortion or helped someone do so. Much reproductive health information is collected and shared through websites and apps that are not HIPAA-regulated or protected by physician-patient privilege, such as period tracking apps (used by millions of US women) that collect information on timing of menstruation and sexual activity and on reproductive health information construed from shopping data. There are many instances of internet service providers sharing user data with law enforcement and prosecutors obtaining and using cell phone data in criminal prosecutions. Commercially collected data are also frequently sold to or shared with third parties. Even putatively deidentified data often contain sufficient information to reidentify individuals or facilities when triangulated with other data. Thus, pregnant persons may unwittingly create incriminating documentation that has scant legal protection and is useful for enforcing abortion restrictions. A 2021 Texas law awards citizens who file successful lawsuits against someone who performs or abets an abortion a $10,000 bounty, putting a direct value on pregnancy information. Some lawsuits have already been filed.

How can clinicians and health care facilities protect their patients and themselves? First, when counseling patients of childbearing age about reproductive health issues, clinicians should explain the risks of generating pregnancy-related information online. For tips on minimizing their digital footprint, patients can be referred to expert organizations. Clinicians also should not presume that more clinical documentation is always better for managing medicolegal risk. Recording less information may be more protective and prevent information from being used in unwanted ways—for example, not speculating about whether a miscarriage was spontaneous when a patient presents in the emergency department with vaginal bleeding. When documenting reproductive health encounters, clinicians should ask themselves: “What information needs to be in the medical record to assure safe, good-quality care, buttress our claim for reimbursement, or comply with clear legal directives?”

Using email and texting with awareness that messages may be seen by others is also important. Clinicians should avoid word choices that could be construed as evidence of illegal activity. Generally, legally complex conversations are best conducted in person or by phone. And if abortion-related patient information is sought by state law enforcement officials, a facility’s legal counsel should be consulted about asserting physician-patient privilege and determining whether the disclosure is mandated, or just permitted, by law. This professional privilege must be actively asserted to protect evidence from being admitted, and physicians and their counsel are better positioned to advocate for it than patients.

Ultimately, broader information privacy laws are needed to fully protect patients and clinicians and facilities providing abortion services. California recently expanded protections for commercially collected personal information and has been enforcing protections related to reproductive health data. Comprehensive federal digital privacy legislation is reportedly inching closer to bipartisan agreement in the Congress. As states splinter on abortion rights after the Dobbs Supreme Court
decision, the stakes for providing robust federal protection for reproductive health information have never been higher.

REFERENCES
3. Physician-patient privilege as extending to patient’s medical or hospital records, 10 ALR 4th 552 (2022).