HIPAA, Privacy, and Reproductive Rights in a Post-Roe Era

The Supreme Court ruling in Dobbs v Jackson Women's Health Organization represents the case that ends the Roe v Wade era of abortion being considered a protected constitutional right. Physicians and other health care professionals are rightly concerned because of the liability they could face for providing abortion services. For example, in a post-Roe Texas, the liability could amount to life in prison and fines as high as $100,000 under criminal law and up to $10,000 and attorneys' fees in private suits. Some clinicians are also concerned because often the care involved for patients with miscarriages could potentially be mistaken for the provision of abortion services. Online forums are filled with posts articulating concern for patients experiencing miscarriage being falsely accused of seeking an illegal abortion. Some clinicians may perceive that the Health Insurance Portability and Accountability Act (HIPAA) could be used as a shield to protect patients and themselves from criminal justice and third-party investigations.

HIPAA does protect certain types of health care data but does not sufficiently protect either clinicians or patients from post-Roe liability. This Viewpoint describes the limits of the protections offered to clinicians and health care centers, patients seeking abortion services, and patients who experience miscarriages and discusses what physicians and other health care professionals and what patients should be mindful of in a post-Roe era.

HIPAA Does Not Completely Shield Clinicians or Health Care Organizations

HIPAA's Privacy Rule requires written patient authorization for clinicians, health care centers, health insurance companies, government health programs, and others to disclose identifiable health information. At its face, this would seem to cover abortion services and other reproductive services such as care for patients with miscarriage. However, several exceptions in HIPAA's privacy rule undermine the use of HIPAA as a shield against investigations into legally prohibited abortion services.

According to provisions in the HIPAA Privacy Rule, HIPAA will not protect patients' privacy in the face of virtually any legal proceeding (civil or criminal), especially if warrants, discovery requests, subpoenas, and law enforcement are involved. 45 CFR 164.512(e)(i) authorizes disclosure of protected health information (PHI) in the course of judicial or administrative proceedings if there is a court order. Similarly, 45 CFR 164.512(e)(ii) authorizes disclosure in response to a subpoena or discovery request provided the interested party has either notified the relevant individuals to give them an opportunity to object or has put in place a qualified protective order. 45 CFR 164.512(f) authorizes disclosure as required by law or pursuant to a court-ordered warrant or subpoena or administrative request, provided that the information sought is relevant to a legitimate law enforcement inquiry and deidentified information could not be used. 45 CFR 164.512(f)(5) also allows a clinician or health care entity to disclose PHI to law enforcement if they believe, in good faith, that a crime has occurred on the premises of the entity. 45 CFR 164.512(d) authorizes disclosure of PHI to a health oversight agency while 45 CFR 164.512(b) authorizes disclosure for public health activities.

Together, all these exceptions render HIPAA's privacy protections extremely limited with regard to abortion services in a state such as Texas. With the Dobbs decision ending Roe's constitutional protections for abortions, Texas law enforcement officials would likely easily obtain warrants for relevant medical files in the course of investigating physicians providing reproductive care. Parties seeking to enforce the provision of Texas' Senate Bill 8, the private right of action against physicians, other clinicians, and health care centers suspected of "aiding and abetting" patients seeking abortions, would likewise be able to avail themselves of the exceptions articulated in 45 CFR 164.512(e). A health system could even disclose PHI if it suspected one of its physicians of illegally providing abortions on its premises. It is possible that a state such as Texas could pass a law requiring disclosure of any potential abortions or suspicious miscarriages to a relevant health oversight or public health agency.

One aspect is that these obligations are not proactive, but rather reactive. That is, clinicians and health care centers do not have the obligation to voluntarily disclose PHI. In fact, in the absence of a warrant or similar document compelling disclosure, it is better to not disclose to avoid potential HIPAA liability. But physicians, other clinicians, and health care centers should stay aware of any new laws compelling proactive disclosure of patient PHI when there is a suspected abortion because those regulations may be coming.
HIPAA Protects Individuals Seeking Abortion Services or Care for Miscarriage Even Less

HIPAA is a narrow statute in that it is concerned only with PHI found in electronic health records maintained by covered entities, such as clinicians and health care centers. Individuals seeking abortion services or experiencing a miscarriage and have concerns that law enforcement will mistake their miscarriage for an abortion should be aware that HIPAA’s limited protections apply in the only context of medical records generated by interactions with traditional clinicians, health care centers, and hospitals. In addition, even these medical records will have the limited protections (as discussed above) and are vulnerable to the exceptions regarding law enforcement and judicial proceedings.

However, a substantial amount of information related to fertility, reproductive choices, and abortion does not fall under HIPAA. Some women who experienced miscarriage have been prosecuted for second-degree murder and feticide on the basis of nonmedical data, such as online searches for misoprostol and text messages to friends. Fertility tracking apps record a significant amount of data and could be used for surveillance of women of reproductive age. Similarly, location trackers have data about which users have visited abortion clinics, payment apps have information on donors to abortion funds, and search engines have information related to abortion-related searches. Because HIPAA does not attach to these services, some companies may choose to proactively sell these data to interested third parties or share information related to abortion services with law enforcement. Online data-location Safe Graph, for example, reportedly sold location data for more than 600 Planned Parenthood clinics until online advocacy and criticism forced it to stop.

It is possible that some state data privacy statutes and regulations, such as the California Consumer Privacy Act, could provide some very limited protection to individuals within those states. But the conflict between a state law compelling disclosure of abortion-related data and another state law prohibiting the disclosure of such data is a novel one. Virtually all of these state statutes include exceptions for subpoenas and warrants, similar to HIPAA. Individuals instead should be very cautious about generating any digital trail by taking such precautions as leaving their phones at home when visiting a clinician or center for abortion services to avoid generating geolocation data and using privacy-preserving browsers and search engines such as Firefox and DuckDuckGo. They also could work with digital privacy advocates such as the Electronic Frontier Foundation, Digital Defense Fund, and the American Civil Liberties Union (ACLU) to demand more explicit digital privacy protections, including encryption, promises not to sell sensitive data, and commitment to resist disclosure of user data to law enforcement whenever possible.

Considering that the Senate Commerce Committee has unsuccessfully tried for years to develop a federal comprehensive privacy bill, digital privacy advocates may want to focus their efforts on administrative agencies such as the Federal Trade Commission and on consumer actions to pressure large technology companies into improving their privacy practices.

What Is Next?

Information about reproductive choices and services is among some of the most sensitive health data possible. The US is entering a legal era in which this information will likely be sought by some state law enforcement agencies and some interested third parties to prosecute individuals who seek abortion services, patients who have miscarriages that may appear to be abortions, and clinicians who provide care for and support both groups of patients. Physicians, other health care professionals, and health care centers, along with individuals seeking abortion services, should understand the limited protections provided by HIPAA and the negligible protections related to health tech data. At minimum, patients should be educated on the very real risk that digital data mining could be used to support abortion-related prosecutions and civil actions. Advocates should demand that health technology companies increase their data privacy protection commitments when the data are relevant to reproductive choices.