HHS Issues Post-Dobbs Guidance to Protect Patient Privacy

Friday, July 8, 2022

On June 29, 2022, the U.S. Department of Health and Human Services (“HHS”) issued two guidance documents to “help protect patients seeking reproductive health care, as well as their providers” following the Supreme Court’s decision in Dobbs vs. Jackson Women's Health Organization. These guidance documents address the legal protections for individuals’ protected health information (“PHI”) relating to abortion and other reproductive health care, as well as how individuals can protect their medical information on personal devices, menstruation tracking apps, and other health-related apps.

The first guidance document addresses how and when the HIPAA Privacy Rule permits disclosure of an individual’s PHI, including information related to an individual’s abortion and other forms of sexual and reproductive health care. The guidance explains that HIPAA-covered entities and business associates can only use or disclose PHI as expressly permitted or required by the Privacy Rule. In particular,
the Privacy Rule permits but does not require, a covered entity or business associate to disclose an individual’s PHI (1) when required by law; (2) for law enforcement purposes under certain conditions; or (3) to avert a serious threat to the health or safety of a person or the public. The guidance clarifies how each of these permitted disclosures applies to PHI related to an individual’s reproductive health or abortion.

- **Disclosures Required by Law**: The Privacy Rule permits but does not require, the disclosure of PHI as required by law only under “a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.” Such disclosure cannot exceed what is required by law. For example, HHS explains that if a “state or other law prohibits abortion after six weeks of pregnancy but does not require the hospital to report individuals to law enforcement,” the Privacy Rule would not permit disclosure to law enforcement under the “required by law” permission.

- **Disclosures for Law Enforcement Purposes**: The Privacy Rule permits, but does not require, the disclosure of PHI for law enforcement purposes “pursuant to process and as otherwise required by law,” such as in response to a “a law enforcement request made through such legal processes as a court order or court-ordered warrant, or a subpoena or summons.” Such a disclosure is limited to only the PHI requested by law enforcement. The Privacy Rule does not otherwise permit a covered entity or business associate to choose to report an abortion to law enforcement absent a court-enforceable mandate. For example, HHS explains that absent a court-enforceable mandate, a law enforcement official cannot request abortion records from a reproductive health care clinic. Further, even if law enforcement presents the clinic with a court order, the Privacy Rule does not require, but merely permits, the clinic to disclose the requested PHI.

- **Disclosures to Avert a Serious Threat to Health or Safety**: The Privacy Rule permits, but does not require, the disclosure of PHI, “consistent with applicable law and standards of ethical conduct, . . . if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the disclosure is to a person or persons who are reasonably able to prevent or lessen the threat.” HHS explains that an individual’s statement regarding their intent to receive legal abortion care does not qualify as a “serious and imminent threat to the health or safety of a person or the public,” and thus cannot be disclosed to law enforcement under this type of permitted disclosure.

The second guidance document addresses the concerns raised by patients surrounding ovulation trackers and other smartphone applications that may present a privacy risk to those seeking abortion or other reproductive health care. HHS explains that although the HIPAA Privacy, Security and Breach Notification Rules generally do not protect the privacy or security of individuals’ health information on personal cell phones or tablets (which does not constitute PHI under HIPAA), individuals can still take steps to protect their health information stored on such devices. These steps include but are not limited to:

- avoid downloading unnecessary apps, particularly “free” ones, and limit apps’ access to location information;
• use communication apps, web browsers, and search engines that are more private and secure, such as those that use strong encryption when transmitting data, limit or block tracking tools and do not collect or store personal information; and

• leave one’s device at home if one is concerned about the privacy of one’s activities that may communicate information about one’s reproductive health care.