Biden Administration Seeks to Clarify Patient Privacy Protections Post-Dobbs, Though Questions Remain

Article By

Alaap B. Shah
Allen R. Killworth
Marylana Saadeh Helou
Devon Minnick

Epstein Becker & Green, P.C.
Health Law Advisor

Related Practices & Jurisdictions

- Administrative & Regulatory
- Health Law & Managed Care
- Communications, Media & Internet
- Civil Rights
- All Federal

Thursday, August 11, 2022

On July 8, two weeks following the Supreme Court’s ruling in Dobbs v. Jackson that invalidated the constitutional right to abortion, President Biden signed Executive Order 14076 (E.O.). The E.O. directed federal agencies to take various actions to
protect access to reproductive health care services,[1] including directing the Secretary of the U.S. Department of Health and Human Services (HHS) to “consider actions” to strengthen the protection of sensitive healthcare information, including data on reproductive healthcare services like abortion, by issuing new guidance under the Health Insurance and Accountability Act of 1996 (HIPAA).[2]

The directive bolstered efforts already underway by the Biden Administration. A week before the E.O. was signed, HHS Secretary Xavier Becerra directed the HHS Office for Civil Rights (OCR) to take steps to ensure privacy protections for patients who receive, and providers who furnish, reproductive health care services, including abortions.[3] The following day, OCR issued two guidance documents to carry out this order, which are described below.

Although the guidance issued by OCR clarifies the privacy protections as they exist under current law post-Dobbs, it does not offer patients or providers new or strengthened privacy rights. Indeed, the guidance illustrates the limitations of HIPAA regarding protection of health information of individuals related to abortion services.

A. HHS Actions to Safeguard PHI Post-Dobbs

Following Secretary Becerra’s press announcement, OCR issued two new guidance documents outlining (1) when the HIPAA Privacy Rule may prevent the unconsented disclosure of reproductive health-related information; and (2) best practices for consumers to protect sensitive health information collected by personal cell phones, tablets, and apps.

(1) HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care

In the “Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe,”[4] OCR addresses three existing exceptions in the HIPAA Privacy Rule to the disclosure of PHI without an individual’s authorization and provides examples of how those exceptions may be applied post-Dobbs.

The three exceptions discussed in the OCR guidance are the exceptions for disclosures required by law,[5] for purposes of law enforcement,[6] or to avert a serious threat to health or safety.[7]

While the OCR guidance reiterates that the Privacy Rule permits, “but does not require” disclosure of PHI in each of these exceptions,[8] this offers limited protection that relies on the choice of providers whether to disclose or not disclose the information. Although these exceptions are highlighted as “protections,” they expressly permit the disclosure of protected health information. Further, while true that the HIPAA Privacy Rule itself may not compel disclosure (but merely permits disclosure), the guidance fails to mention that in many situations in which these exceptions apply, the provider will have other legal authority (such as state law) mandating the disclosure and thus, a refusal to disclose the PHI may be unlawful based on a law other than HIPAA.
Two of the exceptions discussed in the guidance – the required by law exception and the law enforcement exception – both only apply in the first place when valid legal authority is requiring disclosure. In these situations, the fact that HIPAA does not compel disclosure is of no relevance. Certainly, when there is not valid legal authority requiring disclosure of PHI, then HIPAA prohibits disclosure, as noted as in the OCR guidance. However, in states with restrictive abortion laws, the state legal authorities are likely to be designed to require disclosure – which HIPAA does not prevent.

For instance, if a health care provider receives a valid subpoena from a Texas court that is ordering the disclosure of PHI as part of a case against an individual suspected of aiding and abetting an abortion, in violation of Texas’ S.B. 8, then that provider could be held in contempt of court for failing to comply with the subpoena, despite the fact that HIPAA does not compel disclosure.[9] For more examples on when a covered entity may be required to disclose PHI, please see EBG’s prior blog: The Pendulum Swings Both Ways: State Responses to Protect Reproductive Health Data, Post-Roe.[10]

Notably, the OCR guidance does provide a new interpretation of the application of the exception for disclosures to avert a serious threat to health or safety. Under this exception, covered entities may disclose 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. OCR states that it would be inconsistent with professional standards of ethical conduct to make such a disclosure of PHI to law enforcement or others regarding an individual’s interest, intent, or prior experience with reproductive health care. Thus, in the guidance, OCR takes the position that if a patient in a state where abortion is prohibited informs a health care provider of the patient’s intent to seek an abortion that would be legal in another state, this would not fall into the exception for disclosures to avert a serious threat to health or safety. Covered entities should be aware of OCR’s position and understand that presumably OCR would view any such disclosure as a HIPAA violation.

(2) Protecting the Privacy and Security of Individuals’ Health Information When Using Personal Cell Phones or Tablets

OCR also issued guidance on how individuals can best protect their PHI on their own personal devices. HIPAA does not generally protect the privacy or security of health information when it is accessed through or stored on personal cell phones or tablets. Rather, HIPAA only applies when PHI is created, received, maintained, or transmitted by covered entities and business associates. As a result, it is not unlawful under HIPAA for information collected by devices or apps – including data pertaining to reproductive healthcare – to be disclosed without consumer’s knowledge.[11]

In an effort to clarify HIPAA’s limitation to protect such information, OCR issued guidance to protect consumer sensitive information stored in personal devices and apps.[12] This includes step-by-step guidance on how to control data collection on
their location, and how to securely dispose old devices.[13]

Further, some states have taken steps to fill the legal gaps to varying degrees of success. For example, California’s Confidentiality of Medical Information Act (“CMIA”) extends to “any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information.”[14] As applied, a direct-to-consumer period tracker app provided by a technology company, for example, would fall under the CMIA’s data privacy protections, but not under HIPAA. Regardless, gaps remain as the CMIA does not protect against a Texas prosecutor subpoenaing information from the direct-to-consumer app. Conversely, Connecticut’s new reproductive health privacy law,[15] does prevent a Connecticut covered entity from disclosing reproductive health information based on a subpoena, but Connecticut’s law does not apply to non-covered entities, such as a period tracker app. Therefore, even the U.S.’s most protective state privacy laws do not fill in all of the privacy gaps.

Alongside OCR’s guidance, the Federal Trade Commission (FTC) published a blog post warning companies with access to confidential consumer information to consider FTC’s enforcement powers under Section 5 of the FTC Act, as well as the Safeguards Rule, the Health Breach Notification Rule, and the Children’s Online Privacy Protection Rule.[16] Consistent with OCR’s guidance, the FTC’s blog post reiterates the Biden Administration’s goal of protecting reproductive health data post-Dobbs, but does not go so far as to create new privacy protections relative to current law.

B. Despite the Biden Administration’s Guidance, Questions Remain Regarding the Future of Reproductive Health Privacy Protections Post-Dobbs

Through E.O. 14076, Secretary Becerra’s press conference, OCR’s guidance, and the FTC’s blog, the Biden Administration is signaling that it intends to use the full force of its authorities – including those vested by HIPAA – to protect patient privacy in the wake of Roe.

However, it remains unclear how this messaging will translate to affirmative executive actions, and how successful such executive actions would be. How far is the executive branch willing to push reproductive rights? Would more aggressive executive actions be upheld by a Supreme Court that just struck down decades of precedent permitting access to abortion? Will the Biden Administration’s executive actions persist if the administration changes in the next Presidential election?

Attorneys at Epstein Becker & Green are well-positioned to assist covered entities, business associates, and other companies holding sensitive reproductive health data understand how to navigate HIPAA’s exemptions and interactions with emerging guidance, regulations, and statutes at both the state and Federal levels.

Ada Peters, a 2022 Summer Associate (not admitted to the practice of law) in the firm’s Washington, DC office and Jack Ferdman, a 2022 Summer Associate (not admitted to the practice of law) in the firm’s Boston office, contributed to the preparation of this

[2] Id.


[7] 45 CFR 164.512(j)

[8] Id.


[13] Id.


