Employee Relations
LAW JOURNAL

Privacy of Health Information After *Dobbs*: OCR Guidance on Disclosures of PHI and The Privacy of Personal Information on Devices

By Gina L. Bertolini, Jacqueline B. Hoffman and Martin A. Folliard

To ensure patient privacy and nondiscrimination for patients seeking reproductive health care, as well as for providers who offer reproductive health care after the U.S. Supreme Court's ruling in Dobbs v. Jackson Women's Health Organization*, the U.S. Department of Health and Human Services' Office for Civil Rights issued new guidance addressing privacy rights related to reproductive health care under the Health Insurance Portability and Accountability Act. This article outlines the guidance.*

In the wake of the U.S. Supreme Court's ruling in *Dobbs v. Jackson Women's Health Organization*, the U.S. Department of Health and Human Services ("HHS") Secretary Xavier Becerra directed the Office for Civil Rights ("OCR") within HHS to ensure patient privacy and nondiscrimination for patients seeking reproductive health care, as well as for providers who offer reproductive health care.[1] In response, OCR issued new guidance addressing privacy rights related to reproductive health care under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[2]

Gina L. Bertolini is a partner at K&L Gates LLP concentrating her practice exclusively on health law; primarily representing academic medical centers, hospitals and health systems. Jacqueline B. Hoffman is a partner at the firm and a member of the health care and FDA practice group. Martin A. Folliard is an associate at the firm practicing in the health care and FDA practice group. The authors may be reached at gina.bertolini@klgates.com, jackie.hoffman@klgates.com and marty.folliard@klgates.com, respectively.

OCR's guidance consists of two posts under a new Special Topic: HIPAA and Reproductive Health. The first guidance reiterates that federal law protects Protected Health Information ("PHI") (as defined by HIPAA's regulations) from unauthorized disclosures, including PHI related to abortion and other sexual and reproductive health care, and outlines the "narrowly tailored" circumstances in which disclosures to law enforcement officials are permitted.[3] The second post, while posted under guidance for professionals, is written directly for patients and consumers and addresses concerns that health information applications (apps) on smartphones may threaten an individual's right to privacy by clarifying how medical information on personal cell phones and tablets is or is not protected by federal law, and provides tips for protecting privacy when using these programs.[4]

This article outlines and further explains OCR's guidance on both topics.

HIPAA PRIVACY RULE AND DISCLOSURES OF INFORMATION RELATING TO REPRODUCTIVE HEALTH CARE

*When Are Law Enforcement Disclosures Permitted in a Post-*Dobbs *World?*

In its guidance related to HIPAA's Privacy Rule and disclosures to law enforcement, OCR primarily focuses on two exceptions under HIPAA: (1) disclosures that are "required by law," and (2) disclosures "for law enforcement purposes."

Under the first category, OCR emphasizes that disclosures not subject to patient authorization but meeting HIPAA's "required by law" exceptions are limited to legal mandates at the federal or state level that specifically require the disclosure of PHI.[5] In other words, it is not enough for a law to prohibit the underlying activities or actions that would be the subject of the disclosure to permit the disclosure of PHI under HIPAA; rather, there must also be a legal mandate for disclosure of such information or disclosure must be pursuant to legal process, such as a court order, provided all other conditions outlined in HIPAA's Privacy Rule are met. Even where disclosures are legally mandated by another law or a court order, thus meeting HIPAA's "required by law" exception, such disclosures are permissible only if they are limited to the relevant requirements of such legal mandate.

To illustrate disclosures that may or may not be "required by law," OCR provides the example of an individual who seeks treatment at a hospital emergency department due to complications related to a miscarriage during the tenth week of pregnancy. In that instance, a hospital workforce member suspects the individual of having taken medication to end their pregnancy. Assuming state law prohibits abortion after six

weeks of pregnancy, but does not *expressly require* the hospital to report individuals to law enforcement, the Privacy Rule would not permit a disclosure to law enforcement under the "required by law" exception. OCR explains that, where state law "does not *expressly require* such reporting," a disclosure in such circumstances would be impermissible and would constitute a breach of unsecured PHI, requiring a breach notification to both HHS and the individual who was the subject of the disclosure.[6]

Additionally, OCR's guidance emphasizes that a disclosure is "for law enforcement purposes" where the disclosure is pursuant to legal process such as a warrant, subpoena or summons and "as otherwise required by law," provided all conditions outlined in the Privacy Rule for such disclosures are met. For instance, where a hospital or other health care provider's workforce member, absent a statutory requirement, initiated a report of an individual's abortion or other reproductive health care to law enforcement or made a disclosure at the request of law enforcement, such disclosure would not be permissible "for law enforcement purposes."

OCR points out the lack of a law enforcement purpose where (a) state laws have not generally required health care providers to report "an individual who self-managed the loss of a pregnancy" to law enforcement (e.g., an individual experiencing a miscarriage); (b) state fetal homicide laws have not specifically penalized pregnant individuals; and (c) appellate courts have historically rejected efforts to use existing criminal and civil laws intended to protect children as the basis for arresting or detaining pregnant individuals. In other words, there might not be a sufficient "law enforcement purpose" for a disclosure where a law does not impose civil or criminal liability on a pregnant individual.

Another example includes a law enforcement official requesting records of abortions performed at a reproductive health care clinic. If the request is not accompanied by a court order or other mandate enforceable in a court of law, the Privacy Rule would prohibit the clinic from disclosing PHI in response to the request. In contrast, where the law enforcement official presents a court order requiring the clinic to produce PHI about an identified individual who has obtained an abortion, the Privacy Rule "would permit *but not require* the clinic to disclose the requested PHI," and it may disclose only the PHI expressly authorized by the court order.[7] OCR's distinction between "required" and "permissive" disclosures generally refers to a particular disclosure that is not mandated by the Privacy Rule itself, thus not "required," but assuming the disclosure meets an exception, is permissible and would not constitute a breach under HIPAA's Privacy Rule. Of course, in many instances, a health care provider may be compelled to act pursuant to other legal mandates, such as a court order or other lawful process under state or federal law, and to the extent any objections to disclosure would be appropriate, they must be managed consistent with applicable law.

Lastly, OCR addresses disclosures to avert a serious threat to health or safety, and states that, based on professional societies, including the American Medical Association and American College of Obstetricians and Gynecologists, it is inconsistent with professional standards of ethical conduct to disclose PHI to law enforcement or others "regarding an individual's interest, intent, or prior experience with reproductive health care."[8] Examples include a statement by a pregnant individual in a state that bans abortions demonstrating her intent to travel out of state for an abortion, and a desire by the health care provider to report the statement to law enforcement to attempt to prevent the abortion from taking place.

OCR states that "[a] statement indicating an individual's intent to get a legal abortion, or any other care tied to pregnancy loss, ectopic pregnancy, or other complications related to or involving a pregnancy" would not qualify as a "serious and imminent threat to the health or safety of a person or the public."[9] OCR also states that it would be inconsistent with long held professional ethical standards to compromise the integrity of the patient–physician relationship in this way.[10] According to OCR, such disclosures may both increase the risk of harm to the individual and could be considered by OCR to be a HIPAA breach.

OCR ends its guidance by reminding health care providers to seek legal assistance navigating their responsibilities under state and federal laws regarding abortion and reproductive care, and informs patients how to file a complaint regarding a violation of their health privacy rights.

TAKEAWAYS

With this guidance, OCR makes clear its intent to protect the privacy of individuals seeking reproductive health care, including abortions. OCR suggests that laws prohibiting certain behavior do not, in and of themselves, permit disclosures of PHI about *an individual* and such prohibited activity. Instead, the law must specifically mandate such disclosure, or disclosure must be pursuant to a legally cognizable process, and all other conditions outlined in HIPAA's Privacy Rule must be met. Only then, according to the guidance, is a disclosure permitted without resulting in a HIPAA breach. Depending on the state, however, laws that support criminal or civil action against (i) an individual seeking an abortion, (ii) an individual performing an abortion, or (iii) an individual providing the means for an abortion (e.g., in some states, prescribing medication abortion), may be used as the basis for a disclosure of PHI "for law enforcement purposes," and in states where such laws are in effect, disclosures may be permissible. Accordingly, in the face of new state laws that proscribe certain actions of third parties, HIPAA may not provide the level of protection against disclosure of PHI that may be inferred based on OCR's guidance.

Within this context, health care entities should remind its health care providers and workforce members not to confuse or conflate state abortion prohibitions with mandatory reporting laws, and to be aware that

any mandatory reporting should be reviewed by legal counsel to avoid an unauthorized disclosure of PHI and a HIPAA violation. Hospitals and health systems may want to engage in dialogue with front-line health care providers who are mandatory reporters in other contexts, for example child abuse and mandatory reporting of certain wounds, to assure that they understand the distinctions between these reporting requirements and state law prohibitions or limitations on abortions and other reproductive health care. Otherwise, there is a risk of violating federal or state law confidentiality requirements.

PROTECTING THE PRIVACY AND SECURITY OF YOUR HEALTH INFORMATION WHEN USING YOUR CELL PHONE OR TABLET

Health Information and Personal Devices

Written directly for patients and consumers, OCR's guidance on the use of apps on personal devices stresses that HIPAA's Privacy and Security Rules generally do not protect the privacy and security of health information when it is accessed through or stored on individual cell phones or tablets.[11] OCR indicates that questions have arisen on this issue, in particular in relation to apps that provide services related to reproductive health, such as tracking menstruation cycles (also known as "period trackers"). OCR emphasizes that, unless the app is directly provided by a Covered Entity or its Business Associate (as defined under HIPAA), information voluntarily shared with the app, including geographic location information and internet search history, are not considered PHI and are not protected by HIPAA.[12] This is true even if the source of such information is a Covered Entity. Such information, OCR makes clear, already may be viewed or collected by other entities, used for targeted marketing by the app or device vendor, or sold to other third parties, including data brokers who may use such personal information for marketing or other purposes.

OCR's guidance includes several tips for decreasing third party use of personal information without the individual's knowledge, including avoiding downloading apps, especially apps that are free; not allowing apps to access the individual's device's location data (other than those that require location information for the service); and turning off location services on personal cell phones and tablets.[13] The guidance also includes instructions for Apple and Android users to proactively take steps to minimize disclosure of personal information, including turning off location services, denying permission to track activity across apps and web sites, and deleting the personal advertising ID. The guidance reminds consumers that many apps track location and activity information, including ride sharing apps, social media, and check-in apps, and encourages consumers to review app support and search functions to learn how to delete location and activity history.

Even with those protective measures, the guidance indicates that the device itself and the cellular service provider generally are not considered HIPAA Covered Entities or Business Associates and may store communications sent and received on the personal device, including text messaging and email information, details regarding calls made and received, and when communications were made.[14] For these and other reasons, OCR encourages consumers to review Federal Trade Commission resources on protecting privacy when using apps, as well as Consumer Reports' reviews of data practices, and to take steps to protect the privacy of health and other personal information before disposing of old devices.

Lastly, OCR reminds consumers that the best way to protect health and personal information from being collected and shared without their knowledge is to limit what personal information is sent and stored on or through devices, unless the consumer is confident that communications are sent and received through a protected means of communication such as a health care provider portal.[15] The guidance provides several resources related to protecting the privacy of personal information, including from FTC, Office of the National Coordinator for Health IT ("ONC"), the Federal Communications Commission ("FCC"), and private sources such as The New York Times and The Washington Post.

TAKEAWAYS

In summary, OCR's guidance reminds consumers that apps accessed through personal devices, such as cell phones, that are not provided directly by a Covered Entity or its Business Associate (such as a health system app that allows access to records, appointment scheduling, communications with providers, etc.) are not protected by HIPAA. This includes the many apps that offer services related to health care, such as period trackers, but are not provided by Covered Entities. However, even Covered Entities (and their Business Associates) may be subject to disclosures required by law or for law enforcement purposes (as outlined in the section above). Additionally, cell phone service providers are not covered by HIPAA, and communications via a mobile device, whether calls, texts or emails, generally will not be protected by HIPAA. For these reasons, it will be important for individuals to consider whether and how to electronically communicate with providers for activities such as appointment scheduling, and if privacy is a concern, to limit the amount of personal information shared through mobile devices, including apps that may provide health-related services but are not offered through Covered Entities.

OTHER FEDERAL INITIATIVES IN THE WAKE OF *DOBBS*

OCR's guidance is one of several initiatives arising from HHS's Reproductive Access Task Force, launched prior to the *Dobbs* decision to

address access to reproductive health care. As part of the Reproductive Access Task Force, Secretary Becerra expressed the goal of ensuring access to medication abortion and the ability for individuals to travel safely from states where abortion is banned to states where abortion is legal. Among other things, Secretary Becerra indicated that he is directing HHS to examine the authority of the Emergency Medical Treatment and Labor Act ("EMTALA") to assure that appropriate stabilizing care is provided to all patients, and the Center for Medicare and Medicaid Services to take steps to protect access to family planning care, including emergency and long-term contraceptives.

NOTES

1. Remarks by Secretary Xavier Becerra at the Press Conference in Response to President Biden's Directive Following Overturning of *Roe v. Wade* (Last reviewed July 07, 2022), *https://www.hhs.gov/about/news/2022/06/28/remarks-by-secretary-xavier-becerra-at-the-press-conference-in-response-to-president-bidens-directive-following-overturning-of-roe-v-wade.html*.

2. U.S. Dept. of Health and Human Services, HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care (Last reviewed June 29, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html* (hereinafter, "HIPAA Reproductive Health Care Guidance").

3. *See* HIPAA Reproductive Health Care Guidance, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html*.

4. U.S. Dept. of Health and Human Services, Protecting the Privacy and Security of Your Health Information When Using Your Cell Phone or Tablet (Last reviewed June 29, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html* (hereinafter, "Guidance on Protecting Your Health Information When Using Personal Devices").

5. HIPAA Reproductive Health Care Guidance, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html*.

6. *Id*. (emphasis in original).

7. *Id*. (emphasis in original).

8. *Id*.

9. *Id*.

10. The American College of Obstetricians and Gynecologists ("ACOG") and the American Medical Association ("AMA") cite their respective opposition to interference with the legal and ethical requirement to protect private medical information and the fundamental tenet of the patient-physician relationship of respecting the patient's privacy and confidentiality. *See https://www.acog.org/clinical-information/policy-and-position-statements/position-statements/2017/decriminalization-of-self-induced-abortion* and AMA, Patient Rights, Code of Medical Ethics Opinion 1.1.3. *https://policysearch.ama-assn.org/policyfinder/detail/E-1.1.3?uri=%2FAMADoc%2FEthics.xml-E-1.1.3.xml*.

11. Guidance on Protecting Your Health Information When Using Personal Devices, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html*.

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*