Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Protection of Health Information Under HIPAA and the FTC Act: A Comparison

July 28, 2022

On June 24, 2022, the Supreme Court decided *Dobbs v. Jackson Women's Health Organization*, overturning *Roe v. Wade*, and holding that the U.S. Constitution does not confer a right to abortion. Following the decision, individual states may begin to prohibit abortions or enforce preexisting bans on abortion, including through the imposition of criminal penalties. This has raised concerns by some regarding the privacy of medical information from law enforcement investigations, particularly reproductive health information held by providers, health plans, smartphone apps, and others. Although Congress is considering legislation to establish a nationally applicable consumer privacy framework for digital information generally, current federal laws addressing the privacy of health information are not uniform and may depend on the type of entity holding such data. Specifically, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) generally applies only to protected health information (PHI) held by certain health-care-related entities, known as *HIPAA covered entities*. In contrast, some non-HIPAA covered entities' privacy practices may be regulated by the Federal Trade Commission Act (FTC Act).

HIPAA Privacy Rule

Authorized by HIPAA, the Privacy Rule was first promulgated by the Department of Health and Human Services (HHS) in 2001. The Rule generally governs the use or disclosure of PHI held by HIPAA covered entities or their *business associates*. On June 29, 2022, following the *Dobbs* decision, HHS's Office of Civil Rights (OCR) issued new guidance addressing HIPAA's protection of reproductive health information. On July 8, 2022, President Biden issued an executive order directing the Secretary of HHS to consider taking actions, including providing additional guidance, to strengthen the protection of reproductive health care services under the HIPAA Privacy Rule. HIPAA's definitions of covered entities and PHI are important to understanding the scope of protections offered by the Privacy Rule. This section describes these definitions and discusses relevant exceptions to the general prohibition against disclosure without consent, as well as the potential impact HHS's new guidance may have on such exceptions.

Congressional Research Service
https://crsreports.congress.gov
LSB10797

Definition of Covered Entities

Under HIPAA, a covered entity includes three categories of entities: health care providers that transmit claims information electronically, health insurers, and health care clearinghouses. A business associate of a covered entity generally includes a person who creates, receives, maintains, or transmits PHI on behalf of a covered entity, or a person who receives PHI while providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a covered entity. Generally, business associates must comply with all Privacy Rule requirements in the same manner as a covered entity. (For purposes of this Legal Sidebar, the term "covered entity" will be used to refer to both HIPAA covered entities and their business associates.)

Following the *Dobbs* decision, some employers have announced an intention to reimburse employees for expenses related to abortion, such as the costs of traveling to another state to obtain a legal abortion. This has caused some to ask whether information submitted to an employer for reimbursement would be protected by the HIPAA Privacy Rule. Because the definition of a covered entity includes health plans, the answer may depend upon the manner in which the employer has offered such a benefit. If it is offered as part of a group health plan offered to its employees, information submitted to the employer in its capacity as plan sponsor would likely be protected by the HIPAA Privacy Rule. In contrast, if the benefit is offered through a different mechanism, such as an employee assistance program, the employer would not appear to qualify as a covered entity, and the information would likely be outside the scope of HIPAA Privacy Rule protection.

Definition of Protected Health Information

Information in any form or medium that a covered entity creates or receives generally is considered PHI if it is individually identifiable and relates to (1) the physical or mental health of an individual, (2) the provision of health care to an individual, or (3) the payment for the provision of health care to an individual. For example, the results of a pregnancy test administered by a provider, the fact that an individual received an abortion, or the fact that a claim for reimbursement of abortion expenses was filed with an insurer would all be considered PHI.

Information that has been "de-identified" is no longer considered PHI. De-identification can be accomplished through two means. The HIPAA Privacy Rule includes a de-identification "safe harbor" that requires the removal of eighteen enumerated data elements (such as names, telephone numbers, email addresses, street addresses, account numbers, IP addresses, and photographs). Alternatively, a covered entity may utilize some other method of anonymization that a qualified expert formally determines has a "very small" risk of re-identification.

HIPAA Privacy Rule and Relevant Exceptions

The general default established by the HIPAA Privacy Rule is that a covered entity may only use or disclose PHI for treatment, billing, or health care operations without authorization. All other disclosures require authorization from the individual or providing the individual with an opportunity to agree or object, unless 1 of 12 exceptions applies. Notably, these exceptions describe situations in which a provider *may* disclose PHI without violating the HIPAA Privacy Rule; the Rule does not impose an independent obligation on providers to make a disclosure simply because it may qualify for an exception. Many of these exceptions are not particularly relevant to reproductive health information. For example, the list of exceptions includes disclosures for identifying decedents, for organ donation purposes, and for workers' compensation programs. However, three exceptions address disclosures that may be of particular relevance to concerns about reproductive health privacy.

Disclosures Required by Law

First, the HIPAA Privacy Rule permits covered entities to make disclosures that are required by law, including state law, without authorization. In its June 29 Guidance, HHS reiterated that this exception only applies where disclosure is *required*, and not merely permitted, by another law. Specifically, the phrase "required by law" is defined by the Rule to mean "a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law." For example, many states require certain persons, including health care providers, to alert state or local officials when evidence indicating child abuse or firearms violence are present. Many states also require health care providers to provide regular reports to state officials on abortions performed. To the extent that these laws *require* such disclosures be made, the HIPAA Privacy Rule does not stand as an independent obstacle to such disclosures.

Disclosures to Law Enforcement

Second, the HIPAA Privacy Rule permits a covered entity to disclose PHI, without authorization, to law enforcement in certain circumstances. Covered entities may disclose PHI in response to a warrant, subpoena, or similar process that is part of a legitimate law enforcement inquiry. The HIPAA Privacy Rule also permits a covered entity to disclose PHI to law enforcement in limited circumstances related to criminal activity, such as when a covered entity has a good faith belief that the PHI constitutes evidence of a crime that occurred on the premises. Health care providers responding to a medical emergency may also disclose PHI that appears necessary to alert law enforcement to the commission of a crime, the location of such crime or the victim, and the identity, description, or location of the perpetrator.

Threats to Health or Safety

Third, the HIPAA Privacy Rule permits uses and disclosures of PHI, without authorization, to avert a serious threat to health or safety. Specifically, a covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI 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 is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. In its June 29 Guidance, HHS OCR stated that "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 does not qualify as a serious and imminent threat to the health or safety of a person or the public."

Enforcement of the HIPAA Privacy Rule

The HIPAA Privacy Rule is primarily enforced by HHS OCR, although state attorneys general may also pursue civil monetary penalties for violations. Federal courts of appeal have universally held that the Privacy Rule does not create an individual private right of action for persons whose information may have been inappropriately disclosed. Potential penalties for disclosures of PHI in violation of the HIPAA Privacy Rule include per-incident civil monetary penalties between $100 and $50,000 (depending on the degree of culpability), subject to annual maximums. Knowing violations of the HIPAA Privacy Rule may also be subject to criminal penalties.

FTC Act

Many entities that collect consumers' health information are not required to comply with HIPAA because they are not HIPAA covered entities or business associates. In particular, there are a wide array of smartphone apps that monitor users' health data. Some of these apps focus on reproductive health by, for

example, tracking users' menstrual cycles or pregnancies. Unless overseen by a health care provider, these apps are not subject to HIPAA. Furthermore, health information collected by these apps may be sold to or collected by other third parties, such as data brokers, whose business model typically involves compiling troves of data on individuals from various sources and reselling that data.

Such activities, while not regulated by HIPAA, are subject to the FTC Act. The FTC Act applies to all "persons, partnerships, and corporations," other than a handful of exempt entities such as nonprofits, banks, and common carriers. The Act prohibits these persons and entities from engaging in "unfair or deceptive acts or practices" in commerce. Per FTC guidance, an act or practice is "deceptive" if it involves a material representation or omission that is likely to mislead a reasonable consumer. For an act or practice to be "unfair," the FTC Act states that it must cause a substantial injury to consumers that is not reasonably avoidable and not outweighed by "countervailing benefits."

In contrast to the HIPAA Privacy Rule, the FTC Act does not impose specific data privacy standards on covered companies, such as a requirement to obtain consumers' consent before disclosing their data. However, the FTC Act's prohibition on "unfair or deceptive" acts or practices generally requires companies to abide by whatever promises they make to consumers about how they will handle personal data; the FTC often brings enforcement actions when companies fail to live up to these promises. For example, in 2021, the FTC announced a settlement with the developer of a fertility tracking app, Flo Health Inc. The settlement resolved allegations that the company violated the FTC Act by disclosing sensitive health information to third parties, despite representations that it would keep users' information private.

Following *Dobbs*, the FTC may increasingly focus on reproductive privacy. Some Members of Congress and President Biden have recently urged the FTC to use its authority to protect the privacy of consumers' reproductive health information. On July 11, 2022, the FTC published a blog post saying that it would use the "full scope of its legal authorities" to protect consumers' privacy and would "vigorously enforce the law" upon discovering the misuse of consumers' sensitive health data.

Considerations for Congress

The HIPAA Privacy Rule and the FTC Act regulate health data in very different ways. The HIPAA Privacy Rule imposes a broad prohibition on covered entities sharing PHI without an individual's authorization, subject to specific exceptions spelled out in the regulations. In contrast, the FTC Act does not create any bright-line limitations on the use of health data. Under the FTC Act, companies generally may do as they wish with consumers' data, as long as they are not acting deceptively or unfairly.

Whether health data falls under HIPAA's Privacy Rule or the FTC Act does not turn on the nature or the sensitivity of the data itself but on the entity that has it. If a company is not a HIPAA covered entity, then its privacy practices may be regulated at the federal level only by the FTC Act. Further, some entities that may receive reproductive health information from individuals may fall outside of both the HIPAA Privacy Rule and the FTC Act. For instance, some nonprofit entities, often referred to as "crisis pregnancy centers," may offer a limited range of free pregnancy options, such as counseling, but may not provide licensed medical services. Such entities might receive information about visitors' reproductive health such as pregnancy status and length of gestation. However, such an entity may not be subject to the HIPAA Privacy Rule if it does not qualify as a health care provider, and may not be covered by the FTC Act if it is a nonprofit.

Several bills have been introduced in the 117th Congress that would create stricter privacy requirements for non-HIPAA covered entities that maintain health data. Some of these bills would create comprehensive data privacy regimes that are not limited to health data. For instance, the American Data Privacy and Protection Act (ADPPA) (H.R. 8152) would give consumers various rights to access, correct,

and delete their data, and would apply to most entities, including nonprofits. It also would require, absent a specific exception, entities to obtain consumers' consent before transferring their "sensitive covered data," which includes health information, to a third party.

Other bills are narrower in scope, specifically focusing on health data maintained by non-HIPAA covered entities. For example, the Protecting Personal Health Data Act (S. 24) would direct HHS to issue data privacy and security regulations governing non-HIPAA covered devices, services, applications, and software that are marketed to consumers with the "substantial use or purpose" of collecting health information. The My Body, My Data Act of 2022 (H.R. 8111/S. 4454) is narrower still, as it focuses only on reproductive data. It would apply to most non-HIPAA covered entities, including nonprofits, and would create various privacy protections for "personal reproductive or sexual health information," including a requirement that entities only collect and use these data if the individual has consented or if they are strictly necessary to provide a service or product that the individual has requested.

Author Information

Chris D. Linebaugh
Legislative Attorney

Edward C. Liu
Legislative Attorney

Disclaimer