Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

September 10, 2024

# The HIPAA Privacy Rule: Overview and Issues

The final HIPAA Privacy Rule (the Rule) was first issued in December 2000, and a final modified rule was issued in August of 2002, pursuant to authority in the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191). HIPAA was enacted to improve the availability and continuity of health insurance coverage; promote long-term care insurance and the use of health savings accounts; and combat waste, fraud, and abuse, particularly in Medicare and Medicaid. HIPAA also included a series of requirements under the subtitle "Administrative Simplification" to improve the efficiency of, and decrease costs within, the health care system by supporting a transition to standardized electronic administrative and financial transactions. Among these requirements, the law directed the Department of Health and Human Services (HHS) Secretary to promulgate privacy standards should legislation addressing privacy of personal health information not be enacted within a specified timeframe. The HIPAA Privacy Rule established for the first time a set of federal standards for the protection of personal health information.

As part of Administrative Simplification [42 U.S.C. §§1320d et seq.], HIPAA required promulgation of both privacy and security standards in recognition of the increased risk to health data posed by broadly promoting electronic data use and exchange within the health care system. More than a decade later, the Health Information Technology for Economic and Clinical Health Act (HITECH, P.L. 111-5) incentivized the shift away from paper patient records to electronic patient records, building on the earlier shift to standard electronic financial and administrative transactions. These shifts—both on the administrative and patient care side—were considered by many to be a necessary precursor to broader health care reform efforts that culminated in the Patient Protection and Affordable Care Act of 2010 (ACA, P.L. 111-148, as amended). Privacy (and security) of personal health data was to some extent a second-order policy priority in service of broader reform of the health care system.

The Privacy Rule applies to specific entities—covered entities and their business associates—and to certain health information, termed *protected health information (PHI)*. The requirements of the Rule primarily address (1) the use and disclosure of PHI, (2) individual rights with respect to PHI, and (3) administrative requirements (e.g., workforce training, data safeguards). The Rule is interpreted and enforced by the Office for Civil Rights (OCR) within HHS.

## Entities Subject to the Privacy Rule

The HIPAA Privacy Rule applies to three specific types of entities, referred to as "*covered entities*." These include (1) health care clearinghouses, (2) health plans, and (3) health care providers who carry out HIPAA-covered electronic transactions. Health care clearinghouses may serve as intermediaries between plans and providers and often convert standard to nonstandard data (and vice versa) in that role. In addition, pursuant to authority in the HITECH Act, the Privacy Rule governs business associates'—entities that perform certain work on behalf of covered entities—use and disclosure of protected health information (PHI). Business associates must enter into contractual arrangements ("business associate agreements") in order to perform certain work on behalf of covered entities that requires disclosure and use of PHI (e.g., claims processing, data analysis, utilization review). A covered entity may be a business associate for another covered entity; for example, health care clearinghouses are often acting as a business associate working on behalf of health plans and health care providers. Finally, the Rule establishes *hybrid entities*, which are single legal entities that perform both covered and noncovered functions. If a covered entity elects to establish hybrid entity status, the Rule's requirements apply only to the component carrying out covered functions, and PHI may not be shared between the components except as permitted by the Rule (as it would be permitted to be disclosed to a noncovered entity, generally).

## Information Protected by the Privacy Rule

PHI is individually identifiable health information (IIHI) that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. IIHI is defined as health information that identifies an individual and that is created, maintained, or received by a covered entity or an employer that "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." PHI includes a wide range of information, including among other information demographic data (e.g., name, social security number), medical test results and diagnoses, vaccination status, and family health history.

The Privacy Rule *does not apply* to deidentified PHI, with the Rule specifying two acceptable methods for deidentification: (1) expert determination and (2) safe harbor. To meet the first standard, an expert in "statistical and scientific principles and methods for rendering information not individually identifiable" must determine and document that there is a very small risk that the information could be used to identify an individual who is the subject of the information. For the safe harbor method, the data must be stripped of 18 specific identifiers (e.g., name, email address) listed in the Rule.

Requirements in the Privacy Rule are generally the same for all PHI; that is, the Rule does not apply heightened protections for subsets of health information that may be considered to be more sensitive (e.g., genetic information). One exception to this is psychotherapy notes, which are subject to heightened requirements for individual written authorization prior to disclosure (but are also stored separately from the designated record set, making operationalizing these requirements easier). Recent rulemaking modified requirements around certain permissible disclosures for "PHI that is potentially related to reproductive health care" to require the requester's "attestation" that the disclosure or use would not be for a prohibited purpose, essentially creating a "purpose-based prohibition." Relevant disclosures include those for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, and about decedents to coroners or medical examiners. The final rule notes, however, that "the Department did not propose, and is not finalizing, a newly defined subset of PHI."

## Privacy Rule Requirements

The Privacy Rule includes requirements that broadly address the use and disclosure of PHI and that govern administrative actions to protect PHI, as well as individual rights pertaining to an individual's own PHI.

**Use and Disclosure.** The Rule generally prohibits using or disclosing PHI except as the Rule expressly permits or requires. For all uses or disclosures of PHI that are not otherwise permitted or required by the Rule, covered entities and business associates must obtain a patient's written authorization. The Rule specifies two circumstances when a disclosure of PHI is *required*: (1) to the individual at their request and (2) to the HHS Secretary for purposes of investigation of compliance with, or a possible violation of, the Rule.

In terms of *permitted* uses and disclosures, the Rule establishes categories of disclosures that may be made without authorization, upon patient permission short of authorization (i.e., opportunity to object), or upon assurance from the requester (i.e., attestation). In general, the Rule permits covered entities to, between and among themselves, use or disclose PHI for the purposes of (1) treatment, (2) payment, and (3) other routine health care operations without patient authorization and with few restrictions. This foundational category of permissive disclosure was established to facilitate normal operations within the health care system while limiting broader disclosure of PHI—if a doctor needs to speak with another doctor about a patient's treatment, or if a plan needs information about care administered in order to provide payment, for example. In addition, the Rule, under certain circumstances (e.g., disclosures to family members and friends involved with the patient's care) permits disclosure of PHI without written authorization but requires the individual to have the opportunity to first object or agree to the disclosure. The Rule also generally permits disclosure of PHI, without authorization or the opportunity to agree or object, for 12 public interest or national priority purposes that are not directly connected to the treatment of the individual (e.g., public health activities, health oversight activities, judicial and administrative hearings). These disclosures are generally made to entities that are not HIPAA-regulated, and therefore the disclosed PHI will no longer be subject to the Rule. Finally, disclosures of PHI that is potentially related to reproductive health care made for certain of these purposes (e.g., judicial and administrative proceedings) require attestation by the requester that the PHI will not be used for a prohibited purpose.

**Individual Access Rights**. The Rule gives individuals certain rights of access with respect to their PHI. These include the right to inspect and amend their information, receive an accounting of disclosures, and the right to review and obtain a copy of PHI in the designated record set.

**Administrative Requirements.** The Rule requires covered entities to have physical, administrative, and technical safeguards to protect PHI from unauthorized access, use, or disclosure, and to meet workforce training requirements, as well as requirements for complaint handling, sanctions, and mitigation of harm subsequent to a violation of the Rule.

## HIPAA Privacy Rule Enforcement

OCR administers and primarily enforces the Privacy Rule. HIPAA established, and the HITECH Act amended, civil monetary penalties for failure to comply with the Administrative Simplification standards, including the privacy and security standards. It also created criminal penalties for certain instances involving the wrongful acquisition or disclosure of IIHI in violation of the standards. OCR refers such cases to the Department of Justice (DOJ) for criminal prosecution. The HITECH Act also added an audit authority requiring the HHS Secretary to conduct periodic audits of covered entities to ensure compliance.

## Issues for Consideration

Congress and other stakeholders are considering numerous issues that touch on the Privacy Rule, including the following:

- How does the Privacy Rule, in conjunction with the Common Rule (45 C.F.R. Part 46), apply to secondary research with health data used to develop and train AI applications? Are current requirements sufficient or fit for purpose?
- More digital health data are unprotected by the Privacy Rule because of, for example, subsequent data flow to third parties or data generation by wearables and other non-HIPAA-regulated entities. Does this new data ecosystem raise considerations around the scope of the Privacy Rule?
- OCR has undertaken rulemaking to consider how to modify the Privacy Rule in light of the need for increased care coordination within the health care system. Is the Privacy Rule able to be modified to meet the needs of an evolving health care system? Is a new approach to privacy needed?

**Amanda K. Sarata**, Specialist in Health Policy

IF12759

## Disclaimer