



# Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule



**Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule** and its companion documents explain the Privacy Rule in the research context. They are not intended to be legal documents and should not be construed to be legal advice. The specific Privacy Rule requirements are contained in the relevant laws and regulations.







## What Are the Purpose and Background of the Privacy Rule?

### Key Points:

- **The Privacy Rule establishes minimum Federal standards for protecting the privacy of individually identifiable health information. The Rule confers certain rights on individuals, including rights to access and amend their health information and to obtain a record of when and why their PHI has been shared with others for certain purposes.**
- **The Privacy Rule establishes conditions under which covered entities can provide researchers access to and use of PHI when necessary to conduct research. The Rule is not intended to impede research.**
- **Compliance with the Privacy Rule is required on and after April 14, 2003, for most covered entities. (Small health plans have an extra year to comply.)**

The purpose of the Privacy Rule is to establish minimum Federal standards for safeguarding the privacy of individually identifiable health information. Covered entities, which must comply with the Rule, are health plans, health care clearinghouses, and certain health care providers. Covered entities may not use or disclose PHI except as permitted or required under the provisions of the Privacy Rule. The Rule also confers certain rights on individuals, including rights to access and amend certain health information and to obtain a record of when and how their PHI has been shared with others for certain purposes. In addition, the Rule establishes administrative requirements for covered entities. Covered entities that fail to comply with the Privacy Rule may be subject to both civil monetary penalties, criminal monetary penalties, and/or imprisonment.

The Privacy Rule recognizes that the research community has legitimate needs to use, access, and disclose individually identifiable health information to carry out a wide range of health research protocols and projects. In the course of conducting research, researchers may create, use, and/or disclose individually identifiable health information. The Privacy Rule protects the privacy of such information when held by a covered entity but also provides various ways in which researchers can access and use the information for research.

The term “Privacy Rule” is often preceded by “HIPAA,” an acronym for the Health Insurance Portability and Accountability Act of 1996. The Department of Health and Human Services (HHS) issued the Privacy Rule in December 2000 to carry out HIPAA’s mandate that HHS establish Federal standards for safeguarding the privacy of individually identifiable health information. To clarify certain provisions, address unintended negative effects on health care, and relieve unintended administrative burdens, HHS amended the Privacy Rule on August 14, 2002. Most covered entities must comply with the Privacy Rule by April 14, 2003. Small health plans have an extra year, until April 14, 2004, to comply. Entities that become covered entities after these dates must be in compliance with the Privacy Rule at such time that they become covered.

**Covered Entity** – A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.

**Protected Health Information** – PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

**Health Information** – Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) 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.

**Individually Identifiable Health Information** – Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Research** – A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research.





## To Whom Does the Privacy Rule Apply and Whom Will It Affect?

### Key Points:

- **The Privacy Rule applies only to covered entities. Many organizations that use, collect, access, and disclose individually identifiable health information will not be covered entities, and thus, will not have to comply with the Privacy Rule.**
- **The Privacy Rule does not apply to research; it applies to covered entities, which researchers may or may not be. The Rule may affect researchers because it may affect their access to information, but it does not regulate them or research, per se.**
- **To gain access for research purposes to PHI created or maintained by covered entities, the researcher may have to provide supporting documentation on which the covered entity may rely in meeting the requirements, conditions, and limitations of the Privacy Rule.**

The Privacy Rule applies only to covered entities; it does not apply to all persons or institutions that collect individually identifiable health information. It may, however, affect other types of entities that are not directly regulated by the Rule if they, for instance, rely on covered entities to provide PHI. It is important that researchers be aware of how the Rule might affect them in the various types of organizations in which they operate, and what they may have to do in order to continue their research or begin new research efforts on and after the compliance date for the Privacy Rule.

### Covered Entities

Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or persons.

Researchers are covered entities if they are also health care providers who electronically transmit health information in connection with any transaction for which HHS has adopted a standard. For example, physicians who conduct clinical studies or administer experimental therapeutics to participants during the course of a study must comply with the Privacy Rule if they meet the HIPAA definition of a covered entity.

**Health Plan** – With certain exceptions, an individual or group plan that provides or pays the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). The law specifically includes many types of organizations and government programs as health plans.

**Health Care Clearinghouse** – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

**Health Care Provider** – A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

**Health Care** – Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.













































