This website is currently in the process of being updated. For guidance on the HIPAA Privacy Rule in research, please see: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

Educational Materials

Clinical Research

Authorizations

Institutional Review Boards

Privacy Boards

Information for Patients

HIPAA Privacy Rule Booklet for Research

Health Services Research and the HIPAA Privacy Rule

Research Repositories, Databases

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.

Datavant Exhibit 1020
Datavant v. Vigilytics, IPR2024-00382

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 "valueadded" 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.

Hybrid Entities

Under the Privacy Rule, any entity that meets the definition of a covered entity, regardless of size or complexity, generally will be subject in its entirety to the Privacy Rule. However, the Privacy Rule provides a means by which many covered entities may avoid global application of the Rule, through the hybrid entity designation provisions. This designation will establish which parts of the entity must comply with the Privacy Rule.

Any single legal entity may elect to be a hybrid entity if it performs both covered and noncovered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearinghouse. To become a hybrid entity, the covered entity must designate the health care components within its organization. Health care components must include any component that would meet the definition of covered entity if that component were a separate legal entity. A health care component may also include any component that conducts covered functions (i.e., noncovered health care provider) or performs activities that would make the component a business associate of the entity if it were legally separate. Within a hybrid entity, most of the requirements of the Privacy Rule apply only to the health care component(s), although the covered entity retains certain oversight, compliance, and enforcement obligations.

For example, a university may be a single legal entity that includes an academic medical center's hospital that conducts electronic transactions for which HHS has adopted standards. Because the hospital is part of the legal entity, the whole university, including the hospital, will be a covered entity. However, the university may elect to be a hybrid entity. To do so, it must designate the hospital as a health care component. The university also has the option of including in the designation other components that conduct covered functions or business associate-like functions. Most of the Privacy Rule's requirements would then only apply to the hospital portion of the university and any other designated components. The Privacy Rule would govern only the PHI created, received, or maintained by, or on behalf of, these components. PHI disclosures by the hospital to the rest of the university are regulated by the Privacy Rule in the same way as disclosures to entities outside the university.

Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the hybrid entity's health care component(s) and be subject to the Privacy Rule. However, research components that function as health care providers, but do not conduct these electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, if the university in the example above also has a research laboratory that functions as a health care provider but does not engage in specified electronic transactions, the university as a hybrid entity has the option to include or exclude the research laboratory from its health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are effectively not subject to the Privacy Rule.

The hybrid entity is not permitted, however, to include in its health care component, a research component that does not function as a health care provider or does not conduct business associate-like functions. For example, a research component that conducts purely records research is not performing covered or business associate-like functions and, thus, cannot be included in the hybrid entity's health care component.

Hybrid Entity – A single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. If a covered entity is a hybrid entity, the Privacy Rule generally applies only to its designated health care components. However, nonhealth care components of a hybrid entity may be affected because the health care component is limited in how it can share PHI with the non-health care component. The covered entity also retains certain oversight, compliance, and enforcement responsibilities.

Business Associates

The Privacy Rule also protects individually identifiable health information when it is created or maintained by a person or entity conducting certain functions on behalf of a covered entity—a business associate. A business associate is a person or entity, who is not a member of the workforce and performs or assists in performing, for or on behalf of a covered entity, a function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule, involving the use or disclosure of individually identifiable health information, or that provides certain services to a covered entity that involve the use or disclosure of individually identifiable health information. Because the HIPAA Administrative Simplification Rules do not directly regulate research activities, the Privacy Rule does not require a researcher or a research sponsor to become a business associate of a covered entity for research purposes. However, a covered entity may engage business associates to assist in de-identifying PHI, to prepare limited data sets, or to perform data aggregation. The Privacy Rule requires a covered entity to enter into a written contract, or another arrangement permitted by the Rule if both parties are government entities, with its business associates. The Rule's business associate provisions can be found in Sections 164.502(e) and 164.504(e). Generally, a covered entity may, for the purposes permitted by the Privacy Rule and specified in its written agreement with its business associate, disclose PHI to that business associate and allow the business associate to use, create, or receive PHI on its behalf. Before the covered entity discloses the PHI to the business associate, the covered entity must obtain satisfactory assurances, generally in the form of a contract, that the business associate will appropriately safeguard the information. With a few limited exceptions, the contract may not authorize the business associate to use or further disclose the PHI in a manner that would violate the Privacy Rule if done directly by the covered entity.

Business Associate – A person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

Determining Your Status Under the Privacy Rule

The determination of whether an individual researcher must comply with the Privacy Rule is a fact-sensitive, individualized determination. The answer to this question may depend on how the entity with which a researcher has a relationship is organized. Questions on a researcher's status under the Privacy Rule should be referred to the appropriate representatives within that organization. Neither the Federal Government nor this booklet makes, or should be construed to make, this determination. HHS has developed a set of tools to help an entity determine whether it is a health plan, a health care clearinghouse, or a covered

health care provider that will be subject to the Privacy Rule. These tools are available at the following link: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.