The Network for Public Health Law

Snap Shot

HIPAA Privacy Rule

Federal Law: Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Citation: 42 U.S.C. § 1320d et al., 45 C.F.R. Parts 160 and 164

HIPAA Privacy Rule limits uses and disclosures of identifiable health information by covered entities and business associates.

THE LAW

What does the law do?

The HIPAA Privacy Rule limits uses and disclosures of identifiable health information by covered entities and their business associates, and it provides certain rights to individuals regarding to their information.

To whom does the law apply?

The HIPAA Privacy Rule only applies to covered entities, defined as health plans, health care clearinghouses, and health care providers who electronically transmit health information in connection with certain transactions (e.g., billing for health care services). HIPAA Privacy Rule also applies to the business associates of covered entities.

is "identifiable" information defined?

The HIPAA Privacy Rule only regulates "protected health information" (PHI). PHI is individually identifiable health information that is "created or received" by a covered entity and relates to the past, present, or future health of an individual. Information is identifiable if it identifies the individual or if there is "a reasonable basis to believe the information can be used to identify the individual."

SHARING OF IDENTIFIABLE DATA

Does this law allow identifiable data to be shared?

HIPAA permits covered entities to share identifiable information in a variety of contexts. The general rule is that an individual's consent is required for a covered entity to disclose PHI. However, there are many exceptions to this general rule. Generally, HIPAA permits covered entities to share PHI for treatment, payment, or health care operations. An individual's consent is generally required for using or disclosing psychotherapy notes and using or disclosing PHI for marketing. In some circumstances, a covered entity can use or disclose PHI but must provide an opportunity for the individual to agree or object (e.g., facility directories, family involved in the individual's care, disaster relief purposes).

HIPAA also contains many provisions that permit covered entities to use or disclose PHI without providing an individual with an opportunity to agree or object, including uses and disclosures required by law, uses and disclosures relating to certain individuals (i.e., decedents and victims of abuse, neglect or domestic violence), and uses and disclosures for specific purposes or activities (i.e., public health, health oversight, research, judicial and administrative proceedings, law enforcement, workers' compensation, specialized government functions, and to avert health or safety threats). Subject to limitations, HIPAA permits covered entities to use and disclose PHI for fundraising and health plan underwriting.

Among who?

HIPAA regulates certain uses and disclosures of PHI. The many HIPAA provisions that permit using or disclosing PHI for specified purposes either explicitly or implicitly indicate who can use or receive disclosed PHI, including other covered entities, business associates, researchers, public health authorities, a school (e.g., proof of immunization), law enforcement, health oversight agencies, employers, medical examiners, and organ procurement organizations.

What are the prerequisites and conditions?

With limited exceptions, HIPAA limits all uses and disclosures of PHI to the "minimum necessary" information to accomplish the purpose of the use or disclosure. As an alternative to a "minimum necessary" disclosure, covered entities can also disclose a limited dataset for research, public health, and health care operations. A covered entity can create a limited dataset by removing certain specified identifiers; however, a covered entity must have a data use agreement with limited dataset recipients.

With limited exceptions (i.e., group health plans, inmates), covered entities must provide individuals with a notice of the PHI uses and disclosures by the covered entity and the individual's rights with respect to PHI. The HIPAA Privacy Rule also contains specific administrative requirements for covered entities, including personnel designations (e.g., a privacy official), implementation of policies and procedures, workforce training, and appropriate administrative, technical, and physical safeguards.

SHARING OF DE-IDENTIFIED DATA

Does this law allow de-identified information to be shared?

HIPAA only protects identifiable information. Covered entities are free to share information that is not legally identifiable or information that has been legally de-identified.

Does this law define de-identification or standards to render the data de-identified?

HIPAA provides two legal standards to de-identify PHI (i.e., to remove restrictions on use and disclosure). HIPAA permits an expert "with appropriate knowledge and experience" to apply "generally accepted statistical and scientific principles and methods" to make information legally de-identified. Under this standard, the expert must make, and document, a determination that there is a "very small" risk the information could be used to identify an individual. HIPAA also contains a safe harbor de-identification method. Under this method, information is legally de-identified if 18 types of identifiers are removed and the "covered entity does not have actual knowledge that the information could be used… to identify an individual."

DATA SHARING IMPLICATIONS FOR PUBLIC HEALTH

Does this law support data sharing to improve the health of communities?

HIPAA contains many provisions that permit sharing PHI to promote the health of communities, including exceptions permitting PHI disclosure and use for public health purposes and research. The statutory provisions of HIPAA are clear that HIPAA does not invalidate or limit any law providing for public health reporting, surveillance, investigation or intervention.

How does this law hinder data sharing to improve the health of communities?

HIPAA permits states to enact more stringent data protection standards, which creates inconsistencies between state laws and can limit the use of HIPAA provisions that allow PHI use and disclosure to promote community health. The many HIPAA protections, administrative requirements, conditions, prerequisites are frequently cited as actual or perceived barriers to data sharing.

Does this law establish prerequisites, conditions, or limitations for data sharing, not previously identified?

HIPAA requires covered entities to enter agreements to share PHI under certain circumstances. For example, covered entities must have business associate agreements to share data with business associates and data use agreements to share limited datasets.

What other terms apply to sharing this data?

HIPAA also grants individuals certain rights relating to their PHI, including the right to request additional restrictions on use or disclosure, reasonable accommodations for alternative means for confidential communications, and access to their own PHI.

What remedies or solutions might be employed to support data sharing while complying with this law?

In many cases, HIPAA is not an actual barrier to data sharing, but misconceptions of the law create perceived barriers to sharing data. In these cases, clear educational materials can help address perceived barriers to data sharing. Additionally, creating template data use agreements (e.g., for disclosing limited data sets) can help facilitate data sharing for research and public health purposes.

HIPAA permits some organizations to become a hybrid entity. A hybrid entity limits its HIPAA obligations to the parts of the organization that perform the functions of a health plan, health care clearinghouse, or health care provider. The hybrid designation permits the non-covered components of the organization to function outside of the HIPAA requirements.

What ethical considerations apply to the exercise of discretion to share data under this law?

The HIPAA Privacy Rule protects information that originates from the interactions between health care providers and the patients seeking their help. This relationship, and the confidential traditions underlying it, are intended to encourage patients to be open and honest with health care professionals. Inappropriate uses and

disclosures of this information could undermine the trust patients have and affect the information they choose to disclose when seeking care.

Additional federal guidance on the HIPAA Privacy Rule can be found here.

SUPPORTERS

The Network for Public Health Law is a national initiative of the Robert Wood Johnson Foundation.

This document was developed by Cason Schmit, Research Assistant Professor, Texas A&M University and reviewed by Jennifer Bernstein, Deputy Director, Mid-States Region of The Network for Public Health Law. The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.

October, 2018