# HIPAA OVERVIEW

This overview will help you understand the key privacy aspects of the *Health Insurance Portability and Accountability Act* (HIPAA) and introduce you to the contents of this Privacy Toolkit.

The Toolkit will provide you with the following materials to help you comply with HIPAA Privacy regulations:

- A HIPAA Privacy Checklist
- A Policies and Procedures Reference Set
- A Series of Sample Forms, Templates and Documents
- Employee Training Materials
- Additional Resources (including a complete set of the privacy regulations)

The following sections provide an overview of HIPAA privacy concepts and their applicability to providers in Minnesota. The materials contained in this section have been written and organized in a manner that can also be extracted and used for general employee training purposes.

Let's start with the three most important initial questions about HIPAA:

## Who Is Covered by the Regulations

As required by HIPAA, the final regulations cover health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., submission of claims and requests for eligibility information) electronically.

## What Information is Protected

All health and medical records and other protected health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally, is covered by the regulations.

## What are the Core Requirements of HIPAA Privacy

The HIPAA Privacy regulations cover five major areas:

- Consumer Control over Health Information
- Boundaries on Health Information Use and Disclosure
- Security of Health Information
- Establishing Accountability for the Use and Disclosure of Health Information
- Balancing Public Responsibility with Privacy Protections

## Consumer Control over Health Information

Under the HIPAA Privacy regulations, individuals have significant new rights to understand and control how their health information is used:

- Individual education on privacy protections. Providers and health plans are required to give individuals a clear written explanation of how they can use, keep, and disclose their health information.
- Ensuring individual access to their medical records. Individuals must be able to see and get copies of their records, and request amendments. In addition, a history of most disclosures must be made accessible to individuals.
- Requiring individual authorization before health information is disclosed for certain non-routine uses and most non-health care purposes, such as releasing information to financial institutions determining mortgages and other loans or selling mailing lists to interested parties such as life insurers. Individual authorization to disclose information must meet specific requirements.
- Individuals have the right to request restrictions on the uses and disclosures of their information.
- Ensuring that authorization is not coerced. Providers and health plans generally cannot condition treatment on an individual's agreement to disclose health information for non-routine uses.
- Providing recourse if privacy protections are violated. People have the right to complain to a covered provider or health plan, or to the US Secretary of Health and Human Services, about violations of the provisions of these regulations or the policies and procedures of the covered entity.

Individual rights under HIPAA encompass and, in some instances, exceed what is now required under Minnesota state laws governing an individual's right to access health records (M.S. § 144.335) and what is required under the existing Minnesota Government Data Practices Act (M.S. § 13.04). However, in other instances, Minnesota state laws are more stringent and are still applicable. For example, health care providers are required to obtain individual consent before disclosing health information for treatment, payment, and health care operations purposes.

Specifically, consumers will be afforded with the following rights:

- Right to a written notice that describes how a covered entity uses and discloses the individual's protected information.
- Right to prohibit the sharing of health care information about the individual except as permitted by the individual, or allowed for by the regulations. (The law allows for certain disclosures, such as child abuse reporting and health care oversight.)
- Right to request a restriction on the uses and disclosures of an individual's identifiable health information for health care operations, payment and treatment; although covered entities do not need to agree with these restrictions.
- Right to inspect and obtain copies of individual health information.
- Right to amend the health record when appropriate.
- Right to receive an accounting of when and where the individual's protected health information was disclosed.
- Right to complain to a specified person, or office, of the covered entities and to the office of civil rights.

## Boundaries on Health Information Use and Disclosure

*Under HIPAA, the use and disclosure of health information will change.* With few exceptions, an individual's health information can be used for health purposes only:

- Ensuring that health information is not used for non-health purposes. Individual information can be used or disclosed by a health plan, provider or clearinghouse only for purposes of health care treatment, payment and operations. Health information cannot be used for purposes not related to health care - such as use by employers to make personnel decisions, or use by financial institutions - without explicit authorization from the individual.
- Providing the minimum amount of information necessary. Disclosures of information must be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the transfer of medical records for purposes of treatment, since physicians, specialists, and other providers need access to the full record to provide the best quality care.
- Ensuring informed and voluntary consent. Non-routine disclosures with individual authorization must meet standards that ensure the authorization is truly informed and voluntary.

HIPAA Privacy regulations will ensure that, with few exceptions, protected health information can be used for health purposes only. Disclosures of health information will be limited to the minimum amount necessary for the purpose of a disclosure. Furthermore, health information will not be used for purposes unrelated to health care without an individual's explicit authorization that is truly informed and voluntary, unless allowed for by the regulations. However, all health information may continue to be shared or disclosed for treatment purposes and to facilitate the provision of quality health care. HIPAA includes both civil and criminal penalties for misuse of personal health information. These requirements complement but are not entirely consistent with current requirements under Minnesota state law.

## Ensuring the Security of Personal Health Information

Organizations entrusted with health information will be responsible for protecting it against deliberate or inadvertent misuse or disclosure. Under HIPAA, these organizations will be required to establish clear procedures to protect individuals' privacy, including designating an official to establish and monitor the entity's privacy practices and training.

The regulations establish the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity. In this way, implementation of the standards will be flexible and scalable, to account for the nature of each entity's business, and its size and resources. Covered entities must:

- Adopt written privacy procedures. These must include who has access to protected information, how it will be used within the entity, and when the information would or would not be disclosed to others. They must also take steps to ensure that their business associates protect the privacy of health information.
- Train employees and designate a privacy official. Covered entities must provide sufficient training so that their employees understand the new privacy protections procedures, and designate an individual to be responsible for ensuring the procedures are followed.
- Establish grievance processes. Covered entities must provide a means for individuals to make inquiries or complaints regarding the privacy of their records.

## Establishing Accountability for Medical Records Use and Disclosure

Penalties for covered entities that misuse personal health information are provided for in HIPAA.

- Civil penalties. Health plans, providers and clearinghouses that violate these standards would be subject to civil liability. Civil money penalties are $100 per incident, up to $25,000 per person, per year, per standard.
- Federal criminal penalties. There are federal criminal penalties for health plans, providers and clearinghouses that knowingly and improperly disclose information or obtain information under false pretenses. Penalties are higher for actions designed to generate monetary gain. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

## Balancing Public Responsibility with Privacy Protections

After balancing privacy and other social values, US Department of Health and Human Services has established rules that would permit certain existing disclosures of health information without individual authorization for the following national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. Within certain guidelines found in the regulations, covered entities may disclose information for:

- Oversight of the health care system, including quality assurance activities
- Public health
- Research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board
- Judicial and administrative proceedings
- Limited law enforcement activities
- Emergency circumstances
- For identification of the body of a deceased person, or the cause of death
- For facility directories
- For activities related to national defense and security

The regulations permit, but do not require these types of disclosures. If there is no other law requiring that information be disclosed, providers may be allowed to make, in limited instances, judgments about whether to disclose information, in light of their own policies and ethical principles. These requirements are similar to, if not entirely consistent with, current requirements under existing Minnesota state law.

## Preserving Existing, Strong State Confidentiality Laws

Stronger state laws (like those covering mental health, HIV infection, & AIDS information) continue to apply. These confidentiality protections are cumulative; the HIPAA Privacy regulations set a national "floor" of privacy standards that protect consumers, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information for civic purposes, we do not preempt these mandates. The result is to give individuals the benefit of all laws providing confidentiality protection as well as to honor state priorities.