s HIPAA Home
PHI Protection
Disclaimer
Privacy Policy Manual
Preemption Analysis
HIPAA FAQs

HIPAA Privacy Rules for the Protection of Health and Mental Health Information

(Note: *The information provided below is a summary and intended for general informational purposes. Mental health providers and other covered entities should not rely on this summary as a source of legal information or advice and should consult with their own attorney or HIPAA Privacy Officer for specific guidance*.)

Introduction:

This document provides guidance about key elements of the requirements of the Health Insurance Portability and Accountability Act (HIPAA), federal legislation passed in 1996 which requires providers of health care (including mental health care) to ensure the privacy of patient records and health information. HIPAA required the federal Department of Health and Human Services (HHS) to develop regulations to implement these privacy requirements, called the Privacy Rule, which became effective on April 14, 2003. State statutes which provide more stringent protections of health care privacy remain in effect even after HIPAA, and therefore this document includes a few relevant references to requirements in New York State's mental health confidentiality statute (section 33.13 of the Mental Hygiene Law).

General:

The HIPAA Privacy Rule (45 CFR Parts 160 and 164) provides the first comprehensive Federal protection for the privacy of health and mental health information. The Rule is intended to provide strong legal protections to ensure the privacy of individual health information, without interfering with patient access to treatment, health care operations, or quality of care.

The Privacy Rule applies to "*covered entities*" which generally includes health plans and health care providers who transmit health information in electronic form. Covered entities include almost all health and mental health care providers, whether they are outpatient, residential or inpatient providers, as well as other persons or organizations that bill or are paid for health care.

Basic Principles of the Privacy Rule:

1. The Privacy Rule protects all "*protected health information"* **(PHI)**, including individually identifiable health or mental health information held or transmitted by a covered entity in any format, including electronic, paper, or oral statements.
2. A major purpose of the Privacy Rule is to define and limit the circumstances under which an individual's PHI may be used or disclosed by covered entities. Generally, a covered entity may not use or disclose PHI to others, except:
    a. as the Privacy Rule permits or requires; or
    b. as authorized by the person (or personal representative) who is the subject of the health information. A HIPAA-compliant Authorization must contain specific information required by the Privacy Rules.
3. A covered entity must provide individuals (or their personal representatives) with access to their own PHI (unless there are permitted grounds for denial), and must provide an accounting of the disclosures of their PHI to others, upon their request.
4. The Privacy Rule supersedes State law, but State laws which provide greater privacy protections or which give individuals greater access to their own PHI remain in effect.

(**Note:** One must consult not only HIPAA but also other relevant federal privacy laws (such as regulations pertaining to Medicaid and federally funded substance abuse treatment programs), as well as State privacy laws (including the Mental Hygiene Law- section 33.13, the Public Health Law, the Education Law licensing provisions, and the Civil Practice Laws and Rules), to determine whether a disclosure of medical information is permissible in a given circumstance.)

Permitted Uses or Disclosures of PHI Without Authorization:

Extensive provisions of the Privacy Rule describe circumstances under which covered entities are permitted to use or disclose PHI, without the authorization of the individual who is the subject of the protected information. These purposes include, but are not limited to, the following:

1. A covered entity may disclose PHI **to the individual who is the subject of the information.**
2. A covered entity may use and disclose protected health information for its own "**treatment, payment, and health care operations**."
    a. **Treatment** is the provision, coordination, or management of health care and related services for an individual, including consultation between providers and referral of an individual to another provider for health care.
    b. **Payment** includes activities of a health care provider to obtain payment or to receive reimbursement for the provision of health care to an individual.
    c. **Health care operations** include functions such as: (a) quality assessment and improvement; (b) competency assessment,, including performance evaluation, credentialing, and accreditation; (c) medical reviews, audits, or legal services; (d) specified insurance functions; and (e) business planning, management, and general administration.
3. **Permission may be obtained from the individual who is the subject of the information** or by circumstances that clearly indicate an individual with capacity has the opportunity to object to the disclosure but does not express an objection. Providers may also rely on an individual's informal permission to disclose health information to an individual's family, relatives, close personal friends, or to other persons identified by the individual, limited to information directly related to such person's involvement.
4. When an **individual is incapacitated** or **in an emergency**, providers sometimes may use or disclose PHI, without authorization, when it is in the best interests of the individual, as determined by health care provider in the exercise of clinical judgment. The PHI that may be disclosed under this provision includes the patient's name, location in a health care provider's facility, and limited and general information regarding the person's condition.
5. Providers may use and disclose PHI without a person's authorization when the use or disclosure of PHI is **required by law**, including State statute or court order.
6. Providers generally may disclose PHI to State and Federal **public health authorities** to prevent or control disease, injury, or disability, and to government authorities authorized to receive reports of child abuse and neglect.
7. Providers may disclose PHI to appropriate government authorities in limited circumstances regarding **victims of abuse, neglect, or domestic violence**.
8. Providers may disclose PHI to **health oversight agencies**, (e.g., the government agency which licenses the provider), for legally authorized health oversight activities, such as audits and investigations.
9. PHI may be disclosed in a **judicial or administrative proceeding** if the request is pursuant to a court order, subpoena, or other lawful process (note that "more stringent" NYS Mental Hygiene law requires a court order for disclosure of mental health information in these circumstances).
10. Providers may generally disclose PHI to **law enforcement** when:
    a. Required by law, or pursuant to a court order, subpoena, or an "administrative request," such as a subpoena or summons (Note: the "more stringent" NYS Mental Hygiene Law section 33.13 requires a court order for disclosure of mental health information in these circumstances)**.** The information sought must be relevant and limited to the inquiry.
    b. To identify or locate a suspect, fugitive, material witness or missing person (Note: under Mental Hygiene Law section 33.13 this information is limited to "identifying data concerning hospitalization").
    c. In response to a law enforcement request for information about a victim of a crime (Note: under Mental Hygiene Law section 33.13 this information is limited to "identifying data concerning hospitalization").
    d. To alert law enforcement about criminal conduct on the premises of a HIPAA covered entity.
11. Providers may disclose PHI that they believe **necessary to prevent or lessen a**
    a. **serious and imminent physical threat** to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).
12. An authorization is not required to use or disclose PHI to **certain government**
    a. **programs providing public benefits** or for enrollment in government benefit
    b. programs if the sharing of information is required or expressly authorized by statute or regulation, or other limited circumstances

“Minimum Necessary” Rule:

A covered entity must make reasonable efforts to use, request, or disclose to others only the minimum amount of PHI which is needed to accomplish the intended purpose of the use, request or disclosure. When the minimum necessary standard applies, a covered entity may not use, disclose, or request a person's entire medical record, unless it can specifically justify that the entire record is reasonably needed.

The minimum necessary standard does not apply under the following circumstances:

a. disclosure to a health care provider for treatment;
b. disclosure to an individual (or personal representative) who is the subject of the information;
c. use or disclosure made pursuant to an Authorization by the person (or personal representative);
d. use or disclosure that is required by law; or
e. disclosure to HHS for investigation, compliance review or enforcement.

Penalties for Violation of HIPAA:

1. **Civil monetary penalties**: HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement- not to exceed $25,000 per calendar year for multiple violations of the same Privacy Rule requirement. Generally, HHS may not impose civil monetary penalties when a violation is due to reasonable cause, there was no “willful neglect,” and the covered entity corrected the violation within 30 days of when it knew (or should have known) of the violation.
2. **Criminal Penalties.** A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA could face a fine of $50,000 and imprisonment for up to one year. If the wrongful conduct involves “false pretenses” the criminal penalties could increase up to a fine of $100,000 and up to five years imprisonment. A fine of up to $250,000 and up to ten years imprisonment could be imposed if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information “for commercial advantage, personal gain, or malicious harm.”

To view the entire Privacy Rule, or for other information about how it applies, visit the website of the HHS, Office of Civil Rights at: http://www.hhs.gov/ocr/hipaa/.
Read more about HIPAA.

Office of Mental Health