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:

HIPAA required the federal Department of Health and Human Services (HHS) to develop regulations to implement privacy requirements, called the Privacy Rule, that would ensure the privacy of patient records and information. State statutes which provide more stringent protections of health care privacy remain in effect even after HIPAA. Relevant references to requirements in New York State's mental health confidentiality statute (section 33.13 of the Mental Hygiene Law) are include here.

General:

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.

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:
    1. as the Privacy Rule permits or requires; or
    2. 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**."
    1. **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.
    2. **Payment** includes activities of a health care provider to obtain payment or to receive reimbursement for the provision of health care to an individual.
    3. **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:
    1. 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.
    2. 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").
    3. 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").
    4. 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**
    1. **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**
    1. **programs providing public benefits** or for enrollment in government benefit
    2. programs if the sharing of information is required or expressly authorized by statute or regulation, or other limited circumstances

"Minimum Necessary" Rule:

The minimum necessary standard requires covered entities covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.

- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

Penalties for Violation of HIPAA:

Penalties for civil violations

- HIPAA violation: Unknowing Penalty range: $100 - $50,000 per violation, with an annual maximum of $25,000 for repeat violations
- HIPAA violation: Reasonable Cause Penalty range: $1,000 - $50,000 per violation, with an annual maximum of $100,000 for repeat violations
- HIPAA violation: Willful neglect but violation is corrected within the required time period Penalty range: $10,000 - $50,000 per violation, with an annual maximum of $250,000 for repeat violations
- HIPAA violation: Willful neglect and is not corrected within required time period Penalty range: $50,000 per violation, with an annual maximum of $1.5 million

Criminal penalties

- Criminal violations of HIPAA are handled by the DOJ. As with the HIPAA civil penalties, there are different levels of severity for criminal violations.
- Covered entities and specified individuals, as explained below, who "knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to 1 year.
- Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison
- Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 and imprisonment up to 10 years.

To view the entire Privacy Rule, or for other information about how it applies, visit: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html .