Justice and Health CONNECT
A national resource for justice and health data sharing

The HIPAA Privacy Rule

What is the HIPAA Privacy Rule?

- The Privacy Rule sets national standards for the privacy and security of protected health information (PHI) that is created, maintained, or used by an organization that is a covered entity, a business associate of a covered entity, or performs a range of covered transactions.

- The Privacy Rule requires covered entities to obtain authorization (i.e. informed consent) before disclosing protected health information, unless one of a number of exceptions applies.

- The Privacy Rule also ensures individuals access to their personal health information from covered entities.

What is protected health information?

- HIPAA defines "protected health information" as:

    - Any oral, paper, or electronic information related to: (1) the past, current, or future medical or mental health information about an individual; (2) the provision of health care to the individual; or (3) payment for healthcare; and
    - Anything that is "individually identifiable," meaning any information that could be used to identify him or her. There are no restrictions on the use or disclosure of de-identified health information.

Which entities are subject to the Privacy Rule?

- Any organization that:

    - Qualifies as a "covered entity"—this refers to individuals, organizations, and agencies that regularly transmit or disclose protected health information; and meet the definition of a: (1) healthcare provider, (2) health plan, and (3) healthcare clearinghouse;
    - Is a "business associate" of a covered entity. A "business associate" works for or on behalf of a covered entity, performing functions that involve use or disclosure of personal health information (e.g. accounting, claim processing); or

- Performs a set of “covered transactions.” A covered transaction involves transmitting information between covered entities or a covered entity’s business associates to carry out certain financial or administrative activities related to health care.

What is an authorization?

- An authorization is a document that grants covered entities permission to use or disclose health information for a specific reason, when not otherwise permitted or required. The Privacy Rule defines the elements of a valid authorization, which include a description of the PHI to be disclosed and its intended use, parties involved, expiration date and purpose of the disclosure.

In what situations does the Privacy Rule not require authorization?

- The Privacy rule permits covered entities to use and disclose PHI without authorization for purposes related to:

  - Treatment, payment, or health care operations. This provision in the Privacy Rule permits healthcare organizations to transmit patient information without consent. It is designed to provide healthcare entities the necessary level of discretion to share personal health information and carry out routine healthcare delivery. It therefore applies to organizations in charge of coordinating treatment, performing case management, processing payments, and improving the quality of care in a facility to share personal health information;
  - Public Health Activities. This provision allows disclosure of PHI for things such as reporting statistics that allow health departments to compile population levels of certain diseases (i.e. disease prevention, surveillance, and control);
  - Court orders and subpoenas. A covered entity can disclose protected health information when required by an order or subpoena from a court or administrative agency. Any order must clearly describe the information being sought and the purpose. Thus, the covered entity can only disclose the information as it is specifically described in the order.
  - Law enforcement purposes. Covered entities can disclose limited information to police when necessary to identify or locate suspects, fugitives or victims, to investigate a crime, and in response to emergency situations where someone is at risk of serious injury. A covered entity may also release such information if an individual admits to committing a violent crime and the entity believes that this person may have caused serious physical harm to the victim; or when there is an instance of suspected abuse or neglect of a child or disabled person (see more below); and
  - De-identified data. Consent is not required if protected health information is de-identified and used for research purposes. HIPAA provides a set of rules and standards for de-identifying data.

Which criminal justice entities are not considered "covered entities" under HIPAA?

- Law enforcement
- Courts
- Probation and parole
- Defense lawyers and prosecutors

When can covered entities share information with law enforcement without a patient's consent?

The Privacy Rule permits law enforcement to access protected health information from a covered entity without consent in a number of scenarios.

- **When required by law.** A covered entity may disclose protected health information to law enforcement officials if it is required to do so by law; for example, when a state law mandates medical providers to report certain types of physical injuries;
- **An order from a judge.** Law enforcement officials may obtain protected health information from a covered entity if they have a court order, warrant, subpoena or summons issued by a judicial officer or a grand jury subpoena;
- **Locating a suspect or fugitive.** Law enforcement can request limited information from covered entities to further a criminal investigation. Without consent, the covered entity is only permitted to disclose a person's (1) name and address, (2) date and place of birth, (3) social security number, (4) blood type, (5) type of injury, 6) date and time of treatment, (7) date and time of death if applicable, and (8) description of distinguishing physical characteristics;
- **Crime victims.** Health care entities are permitted to provide law enforcement agencies with an individual's protected health information when an individual is a suspected victim of a crime. But, only if (1) the individual agrees to disclosure; or (2) the covered entity cannot obtain the individual's agreement because of incapacity or an emergency. In the latter scenario, law enforcement is required to show that disclosure is essential to their investigation and the healthcare providers must exercise professional judgment to determine whether disclosure is in the best interest of their patient;
- **Crime on premises.** If a covered entity believes that protected health information is important evidence of a crime that was committed on the premises of the covered entity, then it may disclose the information to a law enforcement official; and
- **Victims of abuse, neglect or domestic violence.** Subject to some restrictions, a covered entity that believes an individual has been the victim of abuse may disclose the individual's protected health information to a government agency that is authorized by law to receive reports of abuse, neglect or domestic violence.

Click here to read more on law enforcement exceptions.

Does HIPAA apply to jails and prisons?

> Like any other organization, jails and prisons are subject to the Privacy Rule when they perform certain functions related to the delivery of healthcare, including providing and paying for health services and receiving and transmitting protected health information. It certainly applies to correctional "health providers" that deliver services to patients in correctional facilities, but also often applies directly to employees of a department of corrections. For a more detailed explanation, click here.

Can a health provider in the community share health data about an individual with a jail or prison?

> HIPAA does not preclude information-sharing between health and justice systems. Generally, HIPAA allows covered entities to share protected health information with correctional facilities when a person is in custody and doing so is necessary to permit continuity of care. While it is always best to obtain consent when feasible, HIPAA does provide an exception to allow sharing between health providers and correctional facilities.

> The "lawful custody exception" provides that when a correctional institution or law enforcement agency has custody of an individual, HIPAA permits them access to health information without consent, if the information is necessary to: (1) provide healthcare to the individual; (2) ensure the health and safety of the inmate or others housed or working in the facility; (3) protect health and safety of any law enforcement officer transporting an inmate between facilities; (4) protect those involved in the transfer or transporting of the individual; (5) promote law enforcement on the premises of the correctional institution; or (6) maintain and administer safety, security and good order in the correctional facility. See 45 CFR 164.512(j)(1)(ii)(B))

> The lawful custody exception no longer applies once a person is released from custody, including on probation or parole.