

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (*HIPAA*) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and

others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Under what circumstances may a HIPAA covered entity disclose PHI to law enforcement?

A HIPAA covered entity may disclose PHI to law enforcement with the individual's signed HIPAA authorization.

A HIPAA covered entity also may disclose PHI to law enforcement without the individual's signed HIPAA authorization in certain incidents, including:

- To report PHI to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the premises of the covered entity.
- To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- When responding to an off-site medical emergency, as necessary to alert law enforcement to criminal activity.
- To report PHI to law enforcement when required by law to do so (such as reporting gunshots or stab wounds).

- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used).
- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person, but the information must be limited to basic demographic and health information about the person.
- To respond to a request for PHI about an adult victim of a crime when the victim agrees (or in limited circumstances if the individual is unable to agree). Child abuse or neglect may be reported, without a parent's agreement, to any law enforcement official authorized by law to receive such reports.

For More Information

This is a summary of the relevant provisions and does not include all requirements that are found in the HIPAA Privacy Rule. For complete information, please visit the U.S. Department of Health and Human Service's Office for Civil Rights HIPAA web site at <http://www.hhs.gov/ocr/privacy>.