

Health Insurance Portability and Accountability Act (HIPAA) and Protected Health Information (PHI)

What is HIPAA?

HIPAA is an acronym for the Health Insurance Portability and Accountability Act, which is a federal law enacted by Congress. The law has many provisions designed to improve people's access to health care throughout the country, as well as requirements for health care providers and health plans (i.e., insurers/HMOs and self-insured employer group health plans) to more efficiently and securely share health care data and information. The HIPAA privacy regulations establish standards for protecting individuals' medical records and other personal health information.

Why is a federal law needed to protect health information?

Today, more and more health information is routinely shared electronically among health insurance companies, health care providers (e.g., doctors, hospitals, clinics), and employers who sponsor group health plans. The original intent of HIPAA was to establish standards for smooth, consistent, and secure electronic transmission of health care data among these parties. However, as the regulations were being prepared, the need for standards to protect personal identifiable health information was recognized.

What is Protected Health Information?

PHI is any confidential, personal, identifiable information, including demographic information, that is TRANSMITTED or MAINTAINED in any MEDIUM (electronic, paper, or spoken word) that is created or received by a health care provider, health plan, or health care clearinghouse that relates to or describes the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or future payment for the provision of healthcare to the individual. "Identifiable" means that a person reading this information could reasonably use it to identify an individual.

Following are some (but not all) of the elements that make a piece of health-related information into PHI:

- name
- address
- e-mail address
- birth date (except year)
- Social Security number
- employee number
- claim number
- health plan beneficiary number.

PHI includes written documents, electronic files, and verbal information. (Even information from an informal conversation can be considered PHI.) Examples of PHI include completed health care claim forms, detailed claim reports, explanations of benefits (EOB), and notes documenting discussions with plan participants.

Protected Patient Information is any information:

Associated with an individual patient's name, social security number, phone number, address, or any other piece or combination of pieces of such information which could effectively reveal the identity of the individual patient, and; relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. This may include, but **is not limited to**, information concerning the patient's:

- Medical history;
- Current medical condition;
- Test results and images;
- Psycho-social assessments;
- Correspondence between health care professionals about the patient;
- Histories of hospital admissions, discharges, and outpatient appointments;
- Health care insurance coverage and billing status, and;
- The names and specialties of physicians or care providers involved in the patient's prior care.

E-mailing Patient Information

HIPAA does not prohibit sending patient information through e-mail; however, HIPAA **does require** that you take reasonable precautions to protect the confidentiality of patient information and encrypt the information where appropriate. Due to the privacy and security risks that exist with using e-mail for communication, we recommend that you avoid sending patient information in an e-mail if there is another reasonable alternative that can be used. If it is necessary to send patient information by e-mail, it should be limited to only that information which is necessary. We recommend not including patient names when possible and using medical record numbers instead, just in case the e-mail is accidentally sent to the wrong person. While e-mail that is sent internally is encrypted, *any* e-mail messages going outside of the organization are **not encrypted** and have the same effect as sending information through the mail on a postcard.

Civil and Criminal Penalties

Congress provided civil and criminal penalties for covered entities that misuse personal health information. For civil violations of the standards, OCR may impose monetary penalties up to \$100 per violation, up to \$25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to \$50,000 and one year in prison for certain offenses; up to \$100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to \$250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.