

HIPAA FAQ (Frequently Asked Questions)

Here are some of the more commonly-asked questions over time pertaining to HIPAA compliance:

Q. What businesses must comply with HIPAA laws?

A: Any healthcare entity that electronically processes, stores, transmits, or receives medical records, claims or remittances. The keyword here is electronic.

Q. What is Protected Health Information (PHI)?

A: Information collected from an individual by a covered entity that relates to the past, present or future health or condition of an individual and that either identifies the individual or there is basis to believe that the information can be used to identify the individual...and thus must be protected.

Q. What is HITECH and when does it go into effect?

A: Stands for the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act provides over \$30 billion for healthcare infrastructure and the adoption of electronic health records (EHR). According to the Act, physicians are eligible to receive up to \$44,000 per physician from Medicare for meaningful use of a certified EHR system starting in 2011.

Q. What is a Covered Entity (CE)?

A: Any business entity that must by law comply with HIPAA regulations, which include healthcare providers, insurance companies, and clearinghouses. In this context, health care providers include doctors, medical, dental, vision clinics, hospitals, and related health caregivers.

Q. Does the HIPAA Security Rule require data encryption over a network?

A: The HIPAA Security Rule require encryptions only when individually-identifiable health information is sent over a public network, such as the Internet. Encryption is not be required for other network connections, such as Intranets.

Q. What are the penalties for HIPAA non-compliance?

A: Fines can be up to \$250,000 for violations or imprisonment up to 10 years for knowing abuse or misuse of individual health information.

Q. HIPAA-ready v. HIPAA-compliant – what is the difference?

A: HIPAA-ready refers to software and other products used by the healthcare industry that complies with HIPAA guidelines. HIPAA-compliant refers to the actual physicians, clinics, and insurance companies that are in compliance with HIPAA regulations.