

AT A GLANCE:

HIPAA stands for Health Insurance Portability and Accountability Act.

Congress passed HIPAA in 1996.

HIPAA is made up of five (5) separate titles, which address such issues as preventing fraud and abuse, enforcing group health plan requirements, and protecting individuals' medical information.

HIPAA's Security Rule was finalized in 2003 and outlines the information security standards that health care providers, health plans, and healthcare clearinghouses must adhere to.

Electronic Protected Health Information (EPHI), covered under the Security Rule, is any information that could identify the individual or the patient.

THINK YOU'RE IN COMPLIANCE WITH HIPAA? THINK AGAIN.

Unauthorized access to electronic health information, whether obtained by negligence or malevolence, has raised significant questions regarding the confidentiality of individual health records.

In response to this legitimate concern, Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), with the goals of reforming the health insurance industry and simplifying health care administration.

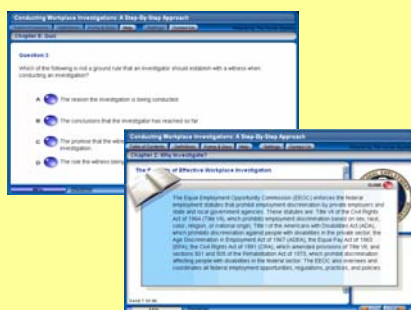
Prior to HIPAA, any organization operating in the healthcare industry was required to comply with its own state's laws as well as those in any other states in which it operated, making compliance particularly difficult for healthcare organizations with multi-state operations.

HIPAA is a far-reaching law that can be found throughout the United States Code, including such federal statutes as the Employee Retirement Income Security Act (ERISA); the Internal Revenue Code; the Social Security Act; and the Public Health Service Act.

HIPAA is made up of five separate titles, but it is Title II's Administrative Simplification provisions that address how organizations must comply with HIPAA. Business entities covered by HIPAA health insurers, HMOs, Medicare/Medicaid providers, health care billing companies, and, of course, health care providers. HIPAA's Security Rule, finalized in 2003, sets the standards for the security of "electronic protected health information" (EPHI) and applies only to protected health information that is transmitted or maintained in electronic media.

While the law allows organizations of different sizes and structures flexibility in how they comply with HIPAA's Security Rule, all covered entities must comply with HIPAA's standards at all times. However, standards may include implementation specifications that are either required or addressable. If an implementation specification is required, it must put into practice. An "addressable" specification requires an organization to assess whether it is a reasonable and appropriate safeguard, and, if determined to be so, must also be implemented; if it is not, the organization must document why the safety measure cannot be implemented and must demonstrate that an alternative measure of similar efficacy has been taken.

Of course, the devil is in the details of HIPAA's many security requirements, and it is these that are covered in the course in depth.



COURSE FEATURES INCLUDE:

- Self-paced learning
- Clear, concise explanations of HIPAA
- Links to definitions, questions and answers, case law, and documents
- Appealing graphics