

## **What Is EPHI and Are You a Covered Entity?**

January 18, 2011

William G. Perry, Ph.D.

You need to know the answer to each of the above questions; otherwise, you could be in real trouble if you are found to have a fiduciary obligation to comply with HIPAA's "Security Rule" and failed to do so. A compliance audit by the federal government could be disastrous for your organization.

HIPAA's security rule, also known as "Electronic Protected Health Information" or EPHI, became effective for "covered entities" on April 20, 2006. Those individuals and organizations that are subject to EPHI regulations must be able to document that required information processing procedures are in place and reasonably implemented so as to provide for an appropriate level of administrative, physical and technical safeguards.

EPHI and related revisions establish a full range of security standards for the administrative, physical and technical safeguards to assure protected healthcare information. The scope of EPHI is significant.

What is a covered entity? A covered entity is any provider of healthcare services or business associates who hold (store) or transmit any protected healthcare information in a digital or electronic format. Any health care plan provider, for example, would be considered a "covered entity". Healthcare professionals including physicians, dentists, psychologists and psychiatrists are all covered entities. So are any business associates who have access to the EPHI information (including home healthcare organization and medical supply companies).

There are five (5) main categories or sections that are included in EPHI. The following broad topical areas are covered:

- a. Administrative Safeguards - which examine formal actions taken by the covered entity to manage and affect the security of EPHI. There are nine (9) standards and twenty-one (21) Implementation Specifications.
- b. Physical Safeguards - refer to those measures taken that relate to physically protecting EPHI. There are four (4) standards and eight (8) Implementation Specifications.
- c. Technical Safeguards - which include the manner in which technology is used to secure EPHI. There are five (5) standards and seven (7) Implementation Specifications.
- d. Organizational Requirements - which refer to the way in which an organization operates while providing security for EPHI. There are two (2) standards and three (3) Implementation Specifications.
- e. Policies and Procedures and Documentation Requirements - which relate to the existence and viability of policies and procedures to protect EPHI in the threat environment. There are two (2) standards and three (3) Implementation Specifications.

Each broad category mentioned above has a number of "Implementation Specifications" that are either "Addressable" or "Required" of the covered entity. Discerning the exact meaning of the implementation specifications as well as the difference between "addressable" and "required", is a significant challenge. All of the sub-categories are auditable by an agency of the federal government.

The implications of the EPHI security rule are staggering for those individuals who are responsible for providing for information assurance. The enforcement agency at the time of this writing is the Office of Civil Rights. Both criminal and civil penalties exist for intentional misuse, willful non-compliance and failure to correct noted deficiencies.

Protecting the information of one's own organization is one thing. Assuring the manner in which employees and business associates handle EPHI is an additional manner. Purchasing an EPHI compliance template or hiring a third-party organization for the purpose of complying still leaves you responsible. An organization is ultimately unable to assign its compliance obligations and liability.

The bottom line: You are responsible for EPHI compliance if you are a covered entity.

Dr. William G. Perry is an information security specialist with significant experience as a university professor, author and service provider to various federal agencies including the Office of the Director of National Intelligence, the Department of Defense and the Federal Bureau of Investigation.

Dr. Perry is the owner of Alliant Digital Services. It provides high quality information security services to individuals, and organizations that must plan for the protection of mission critical information in an asymmetric threat environment while complying with national and international information security standards (i.e. COBIT, ISO 17799, ISO 27000, FISMA, HIPAA, EPHI and the new passed High Tech Act).

Alliant Digital Services also operates a free public web site, <http://www.computer-security-glossary.org>.

Article Source: [http://EzineArticles.com/?expert=William G. Perry, Ph.D.](http://EzineArticles.com/?expert=William_G._Perry,_Ph.D.)