practical security

PO Box 8021
Rancho Santa Fe
California 92067
858.259.6204 tel
858.259.0309 fax
www.practicalsecurity.com

Packaged HIPAA Security and Privacy Support Services

Overview

The Health Insurance Portability and Accountability Act of 1996 provides for the protection of patients' health care information. In response to growing demand for security expertise in health care, Practical Security Inc. (PSI) provides a full line of HIPAA support services for small and medium sized health care organizations. The services are focused around self-certification support using published HIPAA security criteria.

Practical Security, Inc., has established a fixed price offering to assist small providers in addressing HIPAA requirements for privacy and security. The intent of this offering is to provide a reasonably priced HIPAA compliance support service to smaller covered entities.

Background on HIPAA

The Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986 is also known as the Kennedy-Kassebaum Act.

Title II includes a section, Administrative Simplification, requiring improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards.

The bottom line: sweeping changes in most healthcare transaction and administrative information systems.

HIPAA Self-Certification

The final privacy rule was released February 20, 2003. At this time, there are no specific organizations that are "authorized" to perform certifications and this is not expected to change after release of the final security rule. However, there are some basic recommendations that can be followed to create a self-certification to meet the requirements of the HIPAA security rule.

Following these recommendations, PSI acts as an external party with adequate training regarding generally accepted security guidelines and principles. Although the recommendations suggest that self-certification work may be done by an internal party, this internal party would also need to have adequate training and be individuals who are not responsible for the maintenance, supervision, or execution of the specified IT controls. Typically, when small organizations have someone with the proper training these are the same individuals responsible for the management of the systems being certified. Objectivity is crucial to the validity of the self-certification.

Self-certification is documented in a letter in management representation form signed by the organization's executive management and compliance officer that states 1) the compliance status by each HIPAA requirement and element, 2) management's action plans to address areas of control deficiency, and 3) any

practical security

instances in which management is aware of security related control issues or deficiencies. This letter clearly states management's responsibility for the effectiveness of the information security control structure.

Specific Services Provided by PSI

The HIPAA Audit is the first step of a three-step process towards self-certification. The second step is for the self-certifying entity to correct required items and the third step is to have PSI confirm that all required items have been corrected before creating and signing a self-certification letter.

HIPAA Security Audit

This security audit includes a HIPAA gap analysis and Business Impact Analysis (BIA) based on the security provisions of sections 164.308, 164.310, and 164.312 of HIPAA. This section describes the administrative, physical, and technical control measures required to protect confidentiality (security), integrity, and availability of protected health information (PHI).

HIPAA Self-Certification Checkup

PSI returns periodically to reassess security controls and processes. This meets the expectation of due diligence recommended in the published HIPAA guidance documents.

Third Party Review

Objectivity is crucial to the validity of the self-certification. The Department of Health and Human Services (HHS) has strongly recommended outside review of compliance in self-certification. Practical Security, Inc. acts as an external party with adequate training regarding generally accepted security guidelines and principles.

Privacy Support

Protecting patients' health care information is a primary goal of HIPAA. To this extent, PSI provides guidance in defining procedures for the disclosure of PHI related to payment for services, as well as guidance on the appropriate use of PHI in research. PSI also provides assistance with:

- Review and development of notification and authorization procedures.
- Review and development of privacy for oral communications.
- Guidance and procedures for understanding the rules of health-related communications and marketing.

Security Support

Part of the HIPAA services provided by PSI includes the review and development of various policies and procedures, including those required for access control, internal auditing, personnel security, security configuration, and security incidents.

PSI also provides your organization with the following:

- Support for self-certification including a boilerplate letter that may be used for documenting self-certification.
- A contingency plan tailored to your organization.
- A documented security management process.
- Creation of a tailored security awareness program.
- Assist in the selection and training of the individual with security responsibility.

All of the above is tailored to your organization's specific needs.