
HIPAA SECURITY & PRIVACY ISSUES

The Health Insurance Portability and Accountability Act of 1996, was enacted as part of a broad Congressional attempt at incremental health care reform. The Title 2 of the HIPAA legislation outlines the security and privacy requirements:

- » Preventing healthcare fraud and abuse
- » Fraud and abuse controls
- » Administrative Simplification (AS) provisions (Subtitle)
- » Medical Liability Reform

Protecting the patients' right to the privacy of healthcare information has always been, and should remain a high priority. Reductions in fraud and abuse are definitely welcome, as they also affect bottom line. The article outlines the measures and practices to be followed for complying with HIPAA Security and Privacy issues.

HIPAA Security & Privacy

Everyone in the health care arena from clinicians to administrative staffs is expected to play some role in making sure that the individual's health information is kept secure.

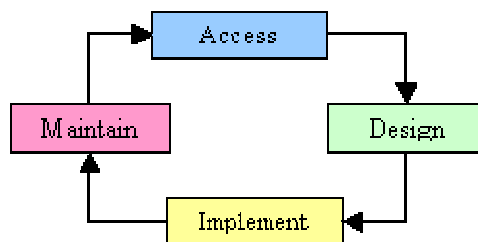
The HIPAA security and privacy rules are intended to reduce cost by detecting and penalizing fraudulent practices and protect patients' right to the privacy of healthcare information. And a good security and privacy policy by the Health care provider can save millions of dollars for their corporate clients, who are expected to get a 20% raise in health care expenditure next year.

HIPAA Security

HIPAA Security can be defined as the ability to control access and protect health care information from accidental or intentional disclosure to unauthorized entities and protect the information from any form of damage or loss.

The final security regulation was issued in the Fall of 2002.

The Security life cycle can be defined as follows:



The security requirements can be broadly classified as

Administrative Procedures

The administrative procedures for security include Certification, * Chain of trust, Contingency plans, Internal audit procedures, Security configuration management, Security incident procedures, Security management process – risk analysis, risk management, Termination procedures and Training.

* Documented formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of the personnel in relation to protection of the data.

Physical Safeguard

Protecting the physical computers systems and building containing data from fire, intrusion and any form of physical damage.

Technical Security Services

Processes put in place for protecting information and to control individual access of such information.

Guidelines include

- » Access Control.
- » Authorization Control
- » Audit Control.

Technical Security Mechanism

Processes that are put in place to guard against unauthorized access of data that are transmitted over a communication network.

Requirement for open networks

- » Access control.
- » Encryption
- » Audit trail
- » Message authentication
- » Integrity Control

SECURITY SAFEGUARDING *PHI

- » Establishing and maintaining reasonable and appropriate administrative and technical procedures for safe and easy accessibility of information.
- » Requirements are technology neutral – the organization can decide which technology to use to achieve required outcome.
- » Reasonable protection against unintentional and intentional violation.
- » Businesses must take cost into consideration and each business implementation might vary with size and type.

* *Protected Health Information*

HIPAA PRIVACY

HIPAA privacy defines who is authorized to access information (the right of individuals to keep information about themselves from being disclosed) and individual's rights. Privacy rules should be in place by April 2003.

HIPAA Privacy rules can be sketched out only after the security rules are in place as privacy is dependent on the security rules.

PRIVACY SAFEGUARDING PHI

- » Reasonable administrative and technical procedures for preserving the privacy of information.
- » Businesses must take privacy cost into consideration and each business implementation might vary with size and type.
- » Theft of PHI will not be a violation if the reasonable policies are in place.

WHAT ARE REASONABLE EFFORTS FOR PRIVACY?

- » Take into consideration the ability of the entity to configure itself for selective access.
- » Practicality of configuration
- » Recognize the limitation of parsing paper records.
- » Privacy in audit trails should record each time a sensitive record id altered.
- » Privacy accounting for disclosure is also essential like date of each disclosure, details of the person to which the disclosure are made and brief description of the disclosure.
- » Finally it's important to co-ordinate accounting for disclosures with audit trails in Security.

About the Author:

Mr. Vijay Krishnan is a senior member of Ultramatics management team. He is responsible for content management and web publications of Ultramatics. **Mr. Krishnan** holds a Bachelors Degree in Engineering from Bharathidasan University and a Masters Degree in Computer Science from Saint Joseph's University, Philadelphia.