
IGI PUBLISHING ITB15022
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, **Information Systems and Healthcare Enterprises**
edited by R. Rada © 2008, IGI Global

Chapter X

Security

Learning Objectives

- Recognize that the Security Rule covers only electronic protected health information
- Develop a risk analysis
- Understand the requirements for a security officer and for staff training
- Plan for administrative safeguards to include management, workforce, access, and contingency plans
- Plan for technical safeguards that address encryption but focus on audit and access
- Plan for physical safeguards that include facility access and media controls
- Describe a model of security in terms of real-world policy, computer models, and technical mechanisms
- Develop a role-based access control model that indicates several roles and their permissions for a healthcare entity
- Design a system for encrypting communications for a healthcare entity that includes a public key infrastructure

Privacy and security of health information is a global concern. However, this chapter will focus on approaches to security in the United States. In particular, the federal regulation of security in the form of the Security Rule will be studied. The HIPAA *Security Rule* details the system and administrative requirements that a covered entity must meet in order to assure that health information is safe from people without authorization for its access. By contrast, the Privacy Rule describes the requirements

that govern the circumstances under which protected health information must be used or disclosed with and without patient involvement and when a patient may have access to his or her protected health information. The implementation of reasonable and appropriate security measures supports compliance with the Privacy Rule.

Introduction

Security of healthcare information systems is substandard. The solution to the problem is not the acquisition of a new technology but the improvement of an organization's *workflow*. A security framework shows that human policies come first and then drive a computer policy that in turn uses technical mechanisms.

The Problem

Security is inadequate. How many hospital-based organizations have developed at least minimally adequate health information security structures to date? In the private sector such information is hard to reliably obtain. If a hospital knows that its information systems are easily breached by hackers, then will the hospital announce that information to the public? Probably not. Experts estimate that the majority of private healthcare organizations have *inadequate security* (Dechow et al., 2005).

The federal government is sometimes more forthcoming with its own internal analyses than the private sector is. The Government Accounting Office under the direction of the U.S. Congress has performed various security audits of federal government agencies. In a report to the U.S. Congress from the *Government Accounting Office,* the title tells the story (Government Accounting Office, 2000a): "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies." An audit of the *Veterans Health Administration* (VHA) speaks more precisely to the problems with healthcare information. A September 2000 report about the VHA contains the following (Government Accounting Office, 2000b):

Access control and service continuity problems are placing financial and sensitive veteran medical information at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and/or destruction. …we found additional access control and service continuity problems at these facilities and serious weaknesses at the VA Maryland Healthcare System. Similar security problems also persist throughout VHA and the department. One reason for the VA's continuing information system control problems is that it had not established an effective, integrated computer security management program throughout the department…it remains important