ABSTRACT

The purpose of this article is to examine the passwords selected by health care professionals and the security and privacy standards in relationship to those passwords as addressed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Examinations of these passwords have illustrated the connectivity between password length and strength and the need to educate employees as to the importance of their password choices. Through an empirical analysis, this article examines whether the passwords created by employees of a health care agency followed “strong” or “weak” password practices. The results should indicate to health care agencies the importance of comprehensive password policies and employee training.

Keywords: IS security; HIPAA; passwords; user behavior

INTRODUCTION

Every health care agency in the United States that handles protected patient health information is required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA security standards require health care agencies to adopt policies and procedures that will show how security methods will be implemented that are “reasonable and appropriate.”

Like most organizations, health care agencies who want to protect their information have employed processes, such as password authentication methods, that act as barriers between the “outside world” and most of their computer systems. If a hacker is able to determine a valid userid and password, then it is likely that they can impersonate the employee and have admittance into the agencies’ computerized system. Unfortunately, if valid credentials are presented, this intrusion often goes unnoticed.

In this article, we examined the passwords that were created by employees of a health care agency. There are numerous problems
that can make password authentication a poor line of defense, including weak passwords, improper password storage, and passwords that are captured through social engineering techniques. These problems can lead to unauthorized access of computerized systems and could potentially compromise a patient’s information and privacy.

Through an empirical analysis of the passwords, the factors of length, strength, and crack times were observed. Examination of these passwords illustrates the need for good password practices, especially because they are included both directly and indirectly within the HIPAA security standards. The analysis is both interesting and important, as it analyzes employees’ actual self-selected passwords in an organization that has implemented no password rules or restrictions.

**Literature Review**

HIPAA consists of three sets of standards which include: 1) transactions and code sets, 2) privacy, and 3) security. The objectives of these standards are to simplify the management and administration of health insurance claims, lower costs, and give patients more control and access to their medical information while protecting their information from real or potential threats of disclosure or loss.

HIPAA also requires that health care organizations take reasonable and appropriate steps to limit the disclosure of an individual’s personal health information, including training employees to follow privacy procedures, designating an individual to oversee the organization’s privacy initiatives, and securing access to electronic patient records. The privacy deadline for HIPAA was April 2003, and the security deadline was April 2005.

There are distinct differences between privacy and security. Privacy is the patient’s control over the use and disclosure of their own personal health information (PHI), whereas security is defined as the “policies, practices, and technology that must be in place for an organization to transact business electronically via networks with a reasonable assurance of safety” (Volonino & Robinson, 2004, p. 1).

Personal health information, or PHI, is the HIPAA term for health information in any form (i.e., paper, electronic, or verbal) which personally identifies a patient. This includes individually identifiable health information in paper records that have never been electronically transmitted (http://www.medstarstystems.com/hipaa.html). Privacy may also include the right to determine when, how, and to what degree PHI is shared with others. The HIPAA privacy rules grant new rights to patients to gain access and control of the use and disclosure of their personal health information (United States Department of Health and Human Services, 2003).

HIPAA addresses security and privacy measures in relationship to passwords, either directly or indirectly, in the following standards (http://www.hhs.gov/news/facts/privacy.html). These standards, as listed below, include management processes, user education and training, and access control.

**Security Management Process**

(161.308(a)(1)) Healthcare organizations must show that they have a consistent set of internal processes, with implementation that is widespread and institutionalized. Processes range from establishing criteria for who has access to what, and who can request certain resources; to ensuring that access rights are revoked immediately upon employee termination. Also required are security policies that should be established and implemented.

**Security Awareness and Training**

(161.308(a)(5)) HIPAA requires that staff members be trained and educated concerning the proper handling of PHI. This basic-level security training should include measures such as password management.

**Access Control**

(161.312(a)) HIPAA security regulations require a definition of who has access to PHI within the organization, as well as the rules determining an individual’s right of access, and the reasons for denying access to some individuals.