Chapter 30
Standards and Guides for Implementing Security and Privacy for Health Information Technology

Francis E. Akowuah
Syracuse University, USA

Jonathan Land
The University of Tennessee at Chattanooga, USA

Xiaohong Yuan
North Carolina A&T State University, USA

Li Yang
The University of Tennessee at Chattanooga, USA

Jinsheng Xu
North Carolina A&T State University, USA

Hong Wang
North Carolina A&T State University, USA

ABSTRACT

In this chapter, the authors survey security standards and guides applicable to healthcare industry including control objective for information and related technologies (COBIT), ISO/IEC 27001:2005 (which has been revised by ISO/IEC 27001:2013), ISO/IEC 27002:2005 (which has been revised by ISO/IEC 27002:2013), ISO 27799:2008 (which has been revised by ISO 27799:2016), ISO 17090:2008 (which has been revised by ISO 17090:2015), ISO/TS 25237:2008, HITRUST common security framework (CSF), NIST Special Publication 800-53, NIST SP 1800, NIST SP 1800-8, and building code for medical device software security. This survey informs the audience of currently available standards that can guide the implementation of information security programs in healthcare organizations, and provides a starting point for IT management in healthcare organizations to select a standard suitable for their organizations.

DOI: 10.4018/978-1-7998-7705-9.ch030

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

National Institute of Standards and Technology (NIST) defines Health Information System (HIS) as a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of health information (NIST, 2009). Usually, HIS is made up of one central main hospital information system, which covers basic Enterprise Resource Planning (ERP)-like functionality, such as patient registration, billing, documentation, inventory, and other functions required at the corporate level. Also, ancillary systems such as laboratory, pharmacy and x-ray components may be included or connected. Administrative personnel and clinicians (physicians and nurses) use or access HIS by workstations and mobile devices running several applications to view or collect medical and/or administrative information (Luethi & Knolmayer, 2009).

Health information systems improve the quality of healthcare delivery by increasing the timeliness and accuracy of records and administrative information. The information maintained by these systems is often faced with security threats from a wide range of sources including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Security incidents such as computer hacking, malicious code and denial of service attacks have not only become common but also increasingly sophisticated. Organizations, especially healthcare organizations, should devote adequate resources to ensure the protection of their information assets. Many governments demand certain security requirements from healthcare organizations and custodians of personal health information by enacting laws and other regulations (Akowuah, Yuan, Xu, & Wang, 2012). These security requirements levied on healthcare organizations can be achieved by implementing one or more information security standards.

Standards help to ensure an adequate level of security is attained, resources are used efficiently and the best security practices are adopted (HKSAR, 2008). Standard is defined as a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose (ISO, 2013). Information security standards specify security controls that help organizations to attain acceptable level of security. "Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information" (NIST, 2009). In this paper, we survey current security standards applicable to the healthcare industry. For each standard, a brief description of the standard, the background and challenges in applying the standard are discussed. This survey informs the audience currently available standards that can guide the implementation of information security programs in healthcare organizations, and provides a starting point for IT management in healthcare organizations to select a standard suitable for their organizations.

We describe the standards that are generic in nature first and move on to standards that are geared toward the healthcare industry. The standards and guides are summarized in Table 1 including COBIT, ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO 27799:2008, ISO 17090:2008, ISO/TS 25237:2008, HITRUST Common Security Framework (CSF), NIST Special Publication 800-53, NIST SP 1800, NIST SP 1800-8, and Building Code for Medical Device Software Security. The applicability of these standards, and issues related to the implementation of a security standard are also discussed.

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/standards-and-guides-for-implementing-security-and-privacy-for-health-information-technology/270620

Related Content

Biomarker Identification From Gene Expression Based on Symmetrical Uncertainty
Emon Asadand Ayatullah Faruk Mollah (2021). *International Journal of Intelligent Information Technologies (pp. 1-19).*
www.irma-international.org/article/biomarker-identification-from-gene-expression-based-on-symmetrical-uncertainty/289966

Personalized Decision Support Systems
Neal Shambaugh (2009). *Encyclopedia of Artificial Intelligence (pp. 1310-1315).*
www.irma-international.org/chapter/personalized-decision-support-systems/10409

Association Analysis of Alumni Giving: A Formal Concept Analysis
Ray R. Hashemi, Louis A. Le Blanc, Azita A. Bahrami, Mahmood Baharand Bryan Traywick (2009). *International Journal of Intelligent Information Technologies (pp. 17-32).*
www.irma-international.org/article/association-analysis-alumni-giving/2449

Urban Intelligence and IoT-UAV Applications in Smart Cities: Unmanned Aerial Vehicle-Based City Management, Human Activity Recognition, and Monitoring for Health
Prince R., Navneet Munothand Neha Sharma (2022). *Unmanned Aerial Vehicles and Multidisciplinary Applications Using AI Techniques (pp. 113-145).*
www.irma-international.org/chapter/urban-intelligence-and-iot-uav-applications-in-smart-cities/310542

The Potential Impact of Chatbots on Student Engagement and Learning Outcomes
Oluwabunmi D. Bakareand Omeiza Victor Jatto (2023). *Creative AI Tools and Ethical Implications in Teaching and Learning (pp. 212-229).*
www.irma-international.org/chapter/the-potential-impact-of-chatbots-on-student-engagement-and-learning-outcomes/330838