Chapter 67
HIPAA Security and Privacy Rules Auditing in Extreme Programming Environments

Mahmood Alsaadi
Princess Sumaya University for Technology, Jordan

Malik Qasaimeh
Princess Sumaya University for Technology, Jordan

Sara Tedmori
Princess Sumaya University for Technology, Jordan

Khaled Almakadmeh
Hashemite University, Jordan

ABSTRACT

Healthcare business is responsible of keeping patient data safe and secure by following the rules of the federal Health Insurance Portability and Accountability Act of 1996, (HIPAA). Agile software organizations that deal with healthcare software system face a number of challenges to demonstrate that their process activities conform to the rules of HIPAA. Such organizations must establish a software process life cycle and develop procedures, tools, and methodologies that can manage the HIPAA requirements during the different stages of system development, and also must provide evidences of HIPAA conformity. This paper proposes an auditing model for HIPAA security and privacy rules in XP environments. The design of the proposed model is based on an evaluation theory which takes as its input the work of Lopez ATAM, and the standards of common criteria (CC) concepts. The proposed auditing model has been assessed based on four case studies. The auditing result shows that the proposed model is capable of capturing the auditing evidences in most of the selected case studies.

DOI: 10.4018/978-1-7998-1204-3.ch067

1. INTRODUCTION

In a world of increasingly global competition, the competitive demands on companies and organizations in the healthcare industry become more intense (Wall, 2009). This has induced healthcare organisations to exploit new opportunities to gain competitive advantage (Reina, Lacroce, Cetani, & Ventura, 2012).

Regulatory compliance has become visible in healthcare industries. The federal Health Insurance Probability and Accountability Act of 1996 (HIPAA), passed by the United States Congress and signed by President Bill Clinton, is the first comprehensive federal guideline for the privacy of patients and health information (Brian & Daniel, 1997). HIPAA is a set of rules aimed at strengthening patients' rights, whilst decreasing administrative costs in the healthcare industry. Failure to comply with HIPAA could lead to large penalties and in extreme cases could lead to loss of medical licenses. Organizations that deal with protected health information (PHI) and wishing to be HIPAA certificated must follow the rules of HIPAA (i.e. physical requirements, network requirements, and security and privacy requirements).

HIPAA is designed to: 1) improve the quality of health insurance; 2) improve the portability, and continuity of health insurance coverage in the group and individual market; 3) simplify the administration of health insurance; 4) prevent fraud and corruption in health insurance and health care companies; 5) protect a subset of sensitive information known as protected health information (PHI); and 6) protect health data created, received, maintained or transmitted electronically, also known as electronic protected health information (ePHI) (Brian & Daniel, 1997).

Organizations that deal with health information must comply with the HIPAA rules. In general, compliance means conforming to the authoritative rules in order to get certification for specific use (Ahmed, 2014). HIPAA rules apply to both covered entities and business associates. For that, industries or organizations that handle protected health information (PHI) or electronic protected health information (ePHI) are related to any of the covered entities or business associates. Next is a description of entities involved in the HIPAA compliance process, see Figure 1.

- **Covered Entities (CE):** According to HIPAA, the term "covered entity" refers to three specific businesses including: health plans, health care clearinghouses, and health care providers that transmit health information electronically (U.S. Department of Health & Human Services, 2014). Examples include software organizations (third parties), hospitals, pharmacies, academic medical centers, and other health care providers. Covered entities can be institutions, organizations, or persons.
- **Business Associates (BA):** The Department of Health and Human Services (U.S. Department of Health & Human Services, 2014) defined the term business associate as "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity". Examples of business associates include individuals who perform services as part of the workforce of a covered entity, financial and banking institutions when performing payment processing activities, medical transcription companies, and others such as: auditors, consulting firms, or software vendors and consultants.

Extreme programming (XP) is an agile software development process that is designed to simplify and expedite the process of developing software products by favouring close collaboration between software development and business teams via face-to-face communication, as opposed to putting an emphasis on written documentation.