Chapter 50
Data Security and Privacy Assurance Considerations in Cloud Computing for Health Insurance Providers

Amavey Tamunobarafiri
Concordia University of Edmonton, Canada

Shaun Aghili
Concordia University of Edmonton, Canada

Sergey Butakov
Concordia University of Edmonton, Canada

ABSTRACT

Cloud computing has been massively adopted in healthcare, where it attracts economic, operational, and functional advantages beneficial to insurance providers. However, according to Identity Theft Resource Centre, over twenty-five percent of data breaches in the US targeted healthcare. The HIPAA Journal reported an increase in healthcare data breaches in the US in 2016, exposing over 16 million health records. The growing incidents of cyberattacks in healthcare are compelling insurance providers to implement mitigating controls. Addressing data security and privacy issues before cloud adoption protects from monetary and reputation losses. This article provides an assessment tool for health insurance providers when adopting cloud vendor solutions. The final deliverable is a proposed framework derived from prominent cloud computing and governance sources, such as the Cloud Security Alliance, Cloud Control Matrix (CSA, CCM) v 3.0.1 and COBIT 5 Cloud Assurance.

INTRODUCTION

Cloud computing aims to incorporate the evolutionary development of many existing computing approaches and technologies such as distributed services, application, information and infrastructure consisting of a pool of computers, network, information, and storage resources (Meli & Grance, 2011; Gavrilov & Trajkovik, 2012; Takabi & Joshi, 2012). Although cloud computing is still evolving, it has

DOI: 10.4018/978-1-5225-8176-5.ch050

shown potential to enhance collaboration, agility, scale, and availability, although its definitions, issues, underlying technologies, risks, and values need to be carefully considered (Gavrilov & Trajkovik, 2012). According to the National Institute of Standards and Technology (NIST), cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing has five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. It is also made up of three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud computing can further be broken down into four deployment models, namely private, public, community, and hybrid cloud (Meli & Grance, 2011).

For healthcare, cloud computing provides opportunities such as reduced IT service costs, optimizing resources, and improving clinical and quality of service for patients (Ahuja, Mani, & Zambrano, 2012). The Cloud Standards Customer Council (CSCC, 2017) described the benefits of cloud computing in healthcare from different perspectives including economic, operational, and functional advantages, consisting of reduced costs, scalability, ability to adjust to demand rapidly, a potential for broad inter-operability, and integration. Kuo (2011) also discussed opportunities for cloud computing with management, legal, technology, and security considerations. Opportunities include increase in scalability, flexibility, and cost-effectiveness of infrastructure. Despite the benefits of cloud computing, there are security and privacy issues that should be considered when adopting cloud computing, particularly when dealing with healthcare data. Protecting healthcare data is crucial because it involves the collection, storage, and use of personally identifiable health information, according to the Institute of Medicine (IOM, 2009). Insurance providers pay part or all of the expenses when one visits a healthcare professional, spends time in a hospital, or purchases covered health care services or products (CLHIA). In order for a health insurance company to process medical claims, personally identifiable information is obtained from its customers. Ensuring the protection of personal data is crucial; because if exposed, it can cause financial loss and damages to the healthcare provider's reputation, as well as aggravation to the patients. Common related fraud schemes may range from prescription fraud to identity theft, and impersonation of the victim for healthcare insurance benefits, as healthcare information also contains government-issued ID numbers (Mennes, 2016).

A case in point is that of Anthem Inc., the second largest healthcare insurer in the United States in 2015, which experienced a breach of a database involving 80 million customer records. The records contained sensitive information such as emails, medical IDs, names, insurance membership numbers, income data, and social insurance numbers, although there were no actual medical or financial records stolen. The breach was caused by a compromised login credential exploited by cyber-attackers to gain unauthorized access to Anthem's IT system. It was later discovered that Anthem failed to encrypt their files (InfoSec Institute, 2017). The breach cost Anthem Inc., 115 million dollars in settlement (REUTERS, 2017). To avoid attacks, the healthcare industry needs increased security and privacy levels when considering cloud computing. Cloud computing can improve the performance of healthcare organizations, but cloud infrastructures require a highly suitable and auditable computing platform to meet statutory and regulatory requirements governing the handling of protected health information (Intel IT Center, 2013).

According to Identity Theft Resource Centre (2017), over twenty-five percent (25%) of data breaches in the US have targeted the healthcare industry. The HIPAA Journal (2017) reported an increase in the number of healthcare data breaches in the US in 2016, exposing over 16 million health records. The