Chapter 6
Managing Risks and Ensuring Compliance in Healthcare Cloud Migration:
An Information Systems Auditing and Security Perspective

Nishanth Holla Raghavendra
https://orcid.org/0009-0005-9195-7688
University at Buffalo, SUNY, USA

Vijay Kumar Banoth
University at Buffalo, SUNY, USA

ABSTRACT

This chapter addresses the digital transformation of the healthcare sector as it moves from on-premises legacy infrastructure to the cloud. The drivers are enhanced scalability, lower costs, and real-time analysis of data for providing improved patient care. Despite the benefits, the transformation raises issues about the confidentiality, integrity and availability of patient data, as if patient data is compromised, companies face HIPAA and GDPR investigations. Without proper security controls, breaches may occur, causing financial loss and reputational damage to organizations. This chapter covers compliance regulations, most critical risks, migration plans, and emerging AI/ML technologies combined with key security principles for optimal best practices. The chapter also provides a checklist for migrating to the cloud to

DOI: 10.4018/979-8-3373-3078-5.ch006

allow healthcare organizations to walk through each phase of the migration process and ensure operational resilience and regulatory compliance for ease of practical implementations.

1.0 INTRODUCTION

Cloud computing is reshaping how businesses approach IT infrastructure and service delivery, offering scalable, on-demand resources with minimal upfront investment (Ahmad & Babar, 2014; Amazon Web Services, 2023a). Defined by the US National Institute of Standards and Technology (NIST) as "…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources…," this technology has become a cornerstone for organizations seeking agility and cost efficiency (Ahmad & Babar, 2014). Healthcare organizations have embraced cloud adoption to address scalability, reduce operational complexities, and enhance data accessibility, all while focusing on providing quality patient care (Argaw et al., 2020; Kuo, 2011). However, transitioning to the cloud—commonly referred to as cloud migration—requires careful consideration of data security, compliance, and operational risks (Takabi et al., 2010; Fernandez et al., 2012). For healthcare providers, where patient data is highly sensitive, migrating from traditional databases to cloud solutions is not merely a technological shift but also a process requiring robust governance (Argaw et al., 2020; Ray et al., 2013).

This section explores cloud migration and its implications for healthcare organizations, focusing on the differences between traditional on-premises databases and cloud-based systems. Furthermore, the importance of Information Systems (IS) auditing in ensuring secure and compliant migration will be discussed, providing a roadmap for healthcare organizations aiming to leverage cloud technology without compromising on trust or efficiency (Deloitte, n.d.).

Cloud migration refers to the process of moving data, applications, and IT processes from on-premises infrastructure to cloud environments (Ahmad & Babar, 2014; Kuo, 2011). In healthcare, the shift is motivated by the promise of enhanced scalability, operational efficiency, and reduced costs (Argaw et al., 2020; Amazon Web Services, 2023a). By leveraging the elasticity of the cloud, organizations can scale their resources based on demand, avoiding the limitations and maintenance costs of legacy infrastructure (Amazon Web Services, 2023b; Kuo, 2011).

Real-world examples highlight the significance of cloud migration for healthcare. For instance, Mayo Clinic's adoption of Google Cloud allowed for seamless collaboration, research advancements through data analytics, and improved patient care delivery (Kuo, 2011). Such cases underline the transformative potential of cloud