Chapter 7
IoT Governance in Healthcare: Privacy, Security, and Regulatory

Renu Mishra
https://orcid.org/0000-0002-5211-8751
Department of CSE, SSCSE, Sharda University, India

Adarsh Tiwari
Sharda University, India

Sneha Sinha
Sharda University, India

Anmol Kr. Sah
Sharda University, India

Mamta Narwaria
https://orcid.org/0000-0001-8941-5824
Sharda University, India

ABSTRACT

The Internet of Things (IoT) has changed how patients are cared for by making it possible to monitor patients from a distance, connect smart diagnoses, and even do real-time nursing analytics. It also creates new problems with privacy, security, and following the rules. This paper states the current IoT governance models in healthcare and evaluates the integration of privacy-preserving technologies, cybersecurity frameworks, and legal compliance relationship. A thorough literature review of twenty empirical studies identifies best practices and gaps in the gover-

DOI: 10.4018/979-8-3373-5636-5.ch007

nance of secure IoT health systems and proposes a comprehensive, evidence-based governance model for the implementation of IoT technologies that integrates both technical and policy-related approaches to the governance of IoT health systems.

INTRODUCTION

Healthcare has evolved significantly in recent years, particularly due to the increasing proliferation of the Internet of Things (IoT). Patient monitoring devices are worn 24/7, and diagnostic devices engage real-time monitoring data to enhance clinical decision-making processes (Dover, 2021; Horn Iwaya et al., 2020). Collectively, these connected devices—sometimes referred to as the Internet of Medical Things (IoMT)—are breaking new ground in modern healthcare systems. Whether it is improving system efficiency or assisting in advancing active participation by patients, the advantages are evident. While it is now possible to leverage connected systems and data, serious concerns are also emerging. As hospitals and clinics shift to relying more on interconnected medical devices and notification devices, there are increasing threats to their operations—such as privacy violations, inadequate process controls, or the application of existing regulations on medicine and data flows (Salman & Ahmad, 2023; Salahuddin et al., 2018). By nature, healthcare data are personal, often citing a sensitive personal identification factor within the data. This complexity is exacerbated not only by the various devices that interface or create the data but also by broadband availability and speed, and the fact they rarely adhere to a single, platform-independent architecture. Even technology with its security claims can provide false data to regulatory requirements like the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR) (Rehman et al., 2022; Nabha et al., 2025).

To address these challenges, experts have proposed several concepts that look promising. Blockchain has been proposed to improve the reliability of the data-sharing process (Rehman et al., 2022). Federated learning has been suggested as a method to train AI models while still protecting patient privacy (Pajouh et al., n.d.). Based on the literature, AI-based threat detection (Cvitić et al., 2022) and privacy-supporting engineering (Stergiou et al., 2021) have also been introduced. What is absent in the existing literature is consistency. These approaches rarely exist in unison, and there is additionally no harmonized way to bring together technology, policy, and patient rights.

In this chapter, we will thoroughly explore the current state of IoT governance in healthcare. We will compile findings from 20 leading studies to assess the manner in which privacy and security are addressed, the way regulation is enforced, and where gaps still remain. Ultimately, we will offer a pragmatic framework to