Chapter 13
Securing Patient Rights and Safety in a Digitally Transformed Healthcare Environment

Sudamini Saproo
IQVIA, India

Parul Goela
https://orcid.org/0009-0004-4699-4087
IQVIA, India

Jayathra Datla
https://orcid.org/0009-0002-9442-7680
IQVIA, India

Kanishak Gautam
https://orcid.org/0009-0006-0073-0152
IQVIA, India

ABSTRACT

The healthcare industry is transforming with advanced technologies like EHRs, telemedicine, and AI, promising improved patient outcomes and streamlined processes. However, increased digitization has led to a surge in data breaches, exposing vulnerabilities and raising concerns about patient data confidentiality. Regulatory frameworks struggle to keep up with rapid technological changes, highlighting significant gaps. This chapter calls for a holistic approach to protect patient rights, proposing robust policies, advanced technology use, and ongoing staff training. Key findings include a 42% rise in breaches, regulatory non-compliance, and underused

DOI: 10.4018/979-8-3693-7210-4.ch013

AI security solutions. Emphasizing stringent regulations, encryption, and ethical data management, it aims to integrate innovation with oversight to safeguard patient information and trust.

INTRODUCTION

In the ever-evolving landscape of modern healthcare, the infusion of digital technology promises transformative advancements alongside formidable challenges. This paradigm shift necessitates a nuanced understanding and proactive management to maximize benefits while mitigating the risks that are posed by the digitization of healthcare industry.

Digital technology has evolved significantly over time and, since its introduction to the healthcare industry, has revolutionized patient care and operational efficiency. Key advancements include enhanced patient care through technologies such as electronic health records (EHRs) and telemedicine, which have improved the quality and accessibility of care. Additionally, digital technology has improved operational efficiency through automation and data analysis, streamlining administrative tasks and clinical workflows, reducing errors, and increasing productivity. Concurring to a study published in the Journal of the American Medical Association, the execution of EHRs has diminished pharmaceutical mistakes by 55% (Bates et al., 1998). Furthermore, digitization has advanced the diagnosis and treatment of diseases at early stages using artificial intelligence (AI) and machine learning (ML) algorithms.

However, despite the benefits that come with the digitization of the healthcare industry, there are risks involved that force us to weigh whether the adoption of digital technology in healthcare is a wise decision. One of the foremost challenges is the data security and privacy of patients. The exponential growth in digital data storage and transmission heightens vulnerabilities to data breaches and unauthorized access. Protecting this sensitive health information across diverse platforms and interconnected systems presents an ongoing challenge, demanding robust cybersecurity measures and stringent privacy protocols.

Another major challenge is the vulnerability to cyber-attacks. Organizations in the healthcare domain are prime targets of cybercriminal activities. The proliferation of malware and ransomware poses significant threats to the data integrity and operational stability of organizations. A survey by the Ponemon Institute reported that 83% of healthcare organizations experienced a data breach in 2021 (Burks, n.d.). The IBM Cost of a Data Breach Report 2024 states that, for the 14th straight year, healthcare had the highest average breach recovery cost at $9.77 million (Bonderud, 2024).