Chapter 4
Data Quality, Privacy, and Security Concerns in Healthcare

J. Shajeena
https://orcid.org/0009-0008-8332-2588
SRM Institute of Science and Technology,Tiruchirapalli, India

Shiny R. M.
https://orcid.org/0000-0002-0473-9852
St. Joseph's College of Engineering, Chennai, India

A. Bindhu
https://orcid.org/0000-0002-4453-8609
Infant Jesus College of Arts and Science for Women, Mulagumoodu, India

ABSTRACT

Healthcare organizations use technology to enhance patient care and streamline their operations in the modern digital world. However, worries about data security and privacy have grown as more clinics and hospitals store patient records electronically. Important information such as a person's medical history, current treatments, and personal data are contained in medical records. This information could result in fraud, identity theft, or health insurance abuse if it ends up in the wrong hands. Because medical data is valuable, cybercriminals frequently target healthcare organizations. Strong security measures like encryption, secure access controls, and routine system checks to stop unwanted access are necessary for hospitals to protect patient privacy. Healthcare providers must make investments in

DOI: 10.4018/979-8-3373-2787-7.ch004

cutting-edge security technologies and enhance data management procedures due to the rise in cyber threats. By taking such steps, they will be able to protect patient data, foster trust, and improve healthcare for everybody.

INTRODUCTION

The rapid digital transformation of healthcare has ushered in unprecedented opportunities for improving patient care, operational efficiency, and medical research. Central to this transformation is the increasing reliance on data-driven systems such as Electronic Health Records (EHRs), Health Information Exchanges (HIEs), wearable health devices, and Artificial Intelligence (AI) tools. While these technologies promise enhanced decision-making and personalized treatment, they also raise critical concerns related to data quality, privacy, and security. In addition to security, healthcare data quality is crucial. Patient records that are inaccurate or incomplete can result in incorrect diagnoses, inappropriate treatments, and even major health hazards. Doctors may become confused and treatment delays may result from data entry errors, duplicate records, or missing information. Healthcare organizations should use well-structured data management systems that guarantee accuracy and consistency in order to prevent such mistakes. The most recent information about a patient helps the doctor make the right choices and provide the right care, which enhances patient care. Errors can be avoided and expenses can be reduced with proper data management, improving the medical field's safety and effectiveness. Healthcare data security is increasingly being aided by artificial intelligence (AI). AI-powered solutions can recognize security risks, spot odd activity, and act fast to safeguard patient data. By keeping an eye on who has access to the data and making sure that only those with permission can see it, AI can also assist hospitals in adhering to stringent data protection regulations like HIPAA and GDPR

High-quality data is foundational for effective healthcare delivery. Inaccurate, incomplete, or inconsistent data can lead to diagnostic errors, inappropriate treatments, and compromised patient outcomes (Weng and Weiskopf, 2013). Ensuring data accuracy, timeliness, and completeness is particularly challenging in environments with multiple data sources and varied documentation practices. Simultaneously, the sensitive nature of healthcare data makes privacy a paramount concern. Healthcare information often includes personal identifiers, genetic information, and behavioral data—elements that, if mishandled or exposed, can lead to discrimination, stigma, or identity theft (Cohen, I. G. and Mello, M. M, 2018).The growing use of cloud computing, mobile health applications, and telemedicine services further complicates the privacy landscape, exposing patient data to new vectors of risk.