


Chapter 1

Ensuring Confidentiality in Telemedicine: A Comprehensive Study on Secure Transmission of Bio–Medical Images and Pharmacy Data

Manish Kumar Thimmaraju

*Department of Pharmaceutical Analysis, Balaji Institute of Pharmaceutical
sciences, Warangal, India*

Divya Pingili


 <https://orcid.org/0000-0001-5951-8910>

*Department of Pharmaceutical Chemistry, Sri Venkateshwara College of
Pharmacy, India*

Gampa Vijaya Kumar

*Department of Pharmacy, KGR Institute of Technology and Management,
Rampally, India*

Mukundan Appadurai Paramashivan

 <https://orcid.org/0009-0009-5608-4788>

Champions Group, Singapore

ABSTRACT

Access and convenience for both patients and providers have been significantly improved as a result of the rapid development of telemedicine, which has revolutionized the delivery of healthcare. The growing reliance on digital technologies for patient interactions, on the other hand, leads to significant concerns regarding the confidentiality and security of patient information. With a particular emphasis

DOI: 10.4018/979-8-3693-9821-0.ch001

on a variety of privacy-protecting strategies and multi-layered security solutions, this study investigates the critical need for robust security measures in the field of telemedicine. At the same time that it discusses the fundamental security principles of confidentiality, integrity, and availability, the research highlights the vulnerabilities that are associated with the transmission and storage of sensitive medical data, such as biomedical images and pharmacy records, through an in-depth analysis.

INTRODUCTION

The ability to diagnose, treat, and manage patients remotely, telemedicine has completely transformed the delivery of healthcare. In spite of this, there are significant concerns regarding the confidentiality of sensitive data, such as images of biomedical procedures and information about pharmacies. With the goal of preserving the trust of patients and adhering to ethical and legal standards, it is essential to guarantee the safe transmission of this information. In the process of being transmitted between patients and healthcare providers, biomedical images, which include X-rays, CT scans, and MRIs, contain sensitive personal health information (PHI) that must be safeguarded. Data breaches, interception by unlawful parties, and tampering are examples of common types of threats. The protection of this data is largely dependent on the utilization of encryption methods, including symmetric and asymmetric encryption, particularly. Beginning with the sender and continuing all the way through to the receiver, end-to-end encryption (E2EE) ensures that the data is protected from any unauthorized access by a third party. In addition, secure transmission protocols such as SSL/TLS offer additional layers of protection by establishing secure communication channels (Sheela, M. S. et al., 2025) between different electronic systems. Due to the fact that pharmacy data is connected to patient records, prescriptions, and medical history, it is also necessary to implement stringent security measures. Encryption, access control, and compliance with regulations such as HIPAA and GDPR are all necessary components in the process of protecting sensitive data. Through the provision of immutable records that improve data integrity and security, blockchain technology is emerging as a powerful solution for securely sharing pharmacy data. Secure application programming interfaces (APIs) guarantee that only authorized systems and personnel are able to access and share pharmacy data, thereby reducing the likelihood of data breaches (Satheesh, N. et al., 2025).

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/ensuring-confidentiality-in-telemedicine/382846

Related Content

Classification Based on Unsupervised Learning

Yu Wang (2009). *Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection* (pp. 348-395).

www.irma-international.org/chapter/classification-based-unsupervised-learning/29702

A Secure Three Factor-Based Authentication Scheme for Telecare Medicine Information Systems With Privacy Preservation

Kakali Chatterjee (2022). *International Journal of Information Security and Privacy* (pp. 1-24).

www.irma-international.org/article/a-secure-three-factor-based-authentication-scheme-for-telecare-medicine-information-systems-with-privacy-preservation/285017

A Compliance-Driven Framework for Privacy and Security in Highly Regulated Socio-Technical Environments: An E-Government Case Study

Ayda Saidaneand Saleh Al-Sharieh (2021). *Research Anthology on Privatizing and Securing Data* (pp. 933-962).

www.irma-international.org/chapter/a-compliance-driven-framework-for-privacy-and-security-in-highly-regulated-socio-technical-environments/280211

A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security

Ranjeet Kumar Singhand Dilip Kumar Shaw (2018). *International Journal of Information Security and Privacy* (pp. 1-12).

www.irma-international.org/article/a-hybrid-concept-of-cryptography-and-dual-watermarking-lsbdct-for-data-security/190852

A Mutual Authentication Protocol with Resynchronisation Capability for Mobile Satellite Communications

Ioana Lasc, Reiner Dojenand Tom Coffey (2013). *Privacy Solutions and Security Frameworks in Information Protection* (pp. 35-51).

www.irma-international.org/chapter/mutual-authentication-protocol-resynchronisation-capability/72736