**Saudi Journal of Medicine and Public Health**

https://saudijmph.com/index.php/pub
https://doi.org/10.64483/jmph-137

# Leveraging Blockchain Technology for Auditable and Privacy-Friendly Data Exchange in Teleradiology Networks

**Abdulelah Hassan Alhathiq[1], Abdullah Ahmed Rayyani[1], Mohammed Nasser Khawaji[1], Jebril Mohammed Mabuj[1], Akram Hadi Radwan[1], Lama Nasser Aloraini[2], Amjad Rashed Alorf[3], Heba Saad Alarifi[4], Sami Abdulaziz Alhuwaimel[5], Lina Abdulaziz Alrashed[6]**

[1]*Sabya General Hospital, Ministry of Health, Saudi Arabia*
[2]*Primary health care Hijrat Se'ed, health security, Ministry of Health, Saudi Arabia*
[3]*Al-Nahda West Health Center, Ministry of Health, Saudi Arabia*
[4]*Huraymla General Hospital, Health Security, Ministry of Health, Saudi Arabia*
[5]*Third Health Cluster Health Security, Ministry of Health, Saudi Arabia*
[6]*Huraymila General Hospital, Health Security, Ministry of Health, Saudi Arabia*

## Abstract

**Background:** Teleradiology, distant transmission and interpretation of medical images, has revolutionized healthcare by increasing diagnostic availability, particularly in underserved communities. However, its digital platform is vulnerable to threats of data breaches and invasions of privacy, with healthcare data breaches costing $2.1 million per breach in 2015. **Aim:** This review aims to address the history of safe data transmission and privacy protection in teleradiology, particularly through technological advancements, regulatory settings, ethical considerations, and challenges. **Methods:** A systematic review was conducted, and articles were fetched from PubMed, Scopus, IEEE, and ACM Digital Library. Keywords used were "teleradiology," "secure data exchange," and "privacy." Two tables of principal technologies and regulatory frameworks are given. **Results:** Advances in encryption, blockchain, AI, and IoMT provide security, but scalability, computational complexity, and regulation gaps pose obstacles. Ethical issues, including patient autonomy and trust, remain paramount. Case studies demonstrate that blockchain and AI are reducing tampering and data breaches. **Conclusion:** Security in teleradiology requires hybrid models, global regulatory harmonization, and patient-centric privacy frameworks to serve the requirements of access and protection. Scalability and equity must be tackled in future studies.

**Keywords:** Teleradiology, Secure Data Exchange, Privacy, Cybersecurity, Blockchain

## 1. Introduction

Teleradiology, which refers to the transmission of radiological images such as X-rays, CT scans, and MRIs through digital networks for remote interpretation, has become an established fixture of modern healthcare provision. By enabling radiologists to provide skilled diagnostic services regardless of geographic distance, teleradiology increases access to specialist care exponentially, particularly in disadvantaged rural and remote communities (White, 2002). This technology has revolutionized medical diagnosis to reduce turnaround time for image interpretation, improve patient outcomes, and facilitate collaboration among professionals. However, the electronic infrastructure that sustains teleradiology poses serious risks like data breaches, unauthorized access to sensitive patient information, and privacy invasion (Simplicio et al., 2014). The reputational and financial consequences of such vulnerabilities are significant, and healthcare data breaches cost $2.1 million on average per breach in 2015, according to an extensive study by the Ponemon Institute (2015). The expenses cover not only immediate cash losses but also regulatory fines, lost patient trust, and disruption to operations.

As teleradiology relies to a large extent on cloud platforms, internet-connected medical devices, and electronic health records (EHR) systems, the risk of cyberattacks has grown. Protected exchange of data and patient privacy have hence become healthcare providers', policymakers', and technology developers' highest agenda items. The present review provides an in-depth review of how secure data exchange and patient privacy protection evolved in teleradiology. It addresses technological advancements, such as encryption, blockchain, and artificial intelligence, the regulatory context, ethical considerations, and persistent challenges. The review attempts to elucidate how these elements interplay for securing confidential health data and identifying gaps, as well as recommending avenues for future research in enhancing teleradiology security. Two tables have been included to present principal technologies and


*Corresponding author e-mail: abady2012_6@hotmail.com (Abdulelah Hassan Alhathiq).
Receive Date: 16 September 2025, Revise Date: 3 October 2025, Accept Date: 14 October 2025

regulatory contexts for straightforward reference by researchers and practitioners.

## Methodology

Literature was accessed using PubMed, Scopus, IEEE Digital Library, and ACM Digital Library with keywords such as "teleradiology," "secure data exchange," "privacy," "health security," and "cybersecurity." The inclusion criteria were peer-reviewed articles, conference proceedings, and reports from 2015 to 2025 with teleradiology security and privacy emphasis. Exclusion criteria were non-English literature and articles lacking empirical data or teleradiology applicability.

## Technological Advances in Secure Data Exchange

The rapid digitization of the healthcare sector has compelled the development of high-tech solutions to provide data exchange in teleradiology. These technologies reduce special vulnerabilities involved in exchanging large volumes of sensitive medical images via networks in a way that ensures confidentiality, integrity, and availability.

### Secure Communication and Encryption Protocols

Encryption is the foundation of secure data exchange in teleradiology, protecting medical images and associated metadata from unauthorized access. PKI-based asymmetric encryption, dependent on public and private key pairs, guarantees that authorized receivers alone can decrypt and retrieve the data in transit. Digital signatures also add security in that they authenticate and verify data integrity, and there is no tampering during transmission (Simplicio et al., 2014). PKI systems are often used on teleradiology platforms to secure communication between remote radiologists and imaging facilities.

A more advanced solution, homomorphic encryption (HE), enables computations over ciphertext without the need to decrypt data, ideal for cloud-based teleradiology systems where data processing occurs outside of servers (Acar et al., 2018). Radiologists are able to view encrypted images using HE and preserve patient confidentiality. But HE also has drawbacks. Noise accumulation, a phenomenon where successive computations on encrypted data introduce errors, can interfere with encryption quality and diagnostic accuracy (Filkins et al., 2016). Against this, techniques like bootstrapping, which refreshes encrypted data to reduce noise, have evolved, though at enormous cost in computational complexity, making them unusable in real time (Gentry, 2019). Researchers are still looking for lightweight HE algorithms to balance security and performance in teleradiology pipelines.

### Blockchain Technology for Secure Data Sharing

Blockchain technology, being a decentralized and distributed ledger, has proven to be a secure one for secure data sharing in teleradiology. Unlike the conventional centralized databases, blockchain's distributed data storing framework does not provide any point of failure, hence it's tamper-proof and safe from unauthorized access. Permissioned blockchain networks that restrict access to authenticated users are particularly well-suited to healthcare applications, enabling secure sharing of EHRs and medical images among radiologists, hospitals, and other stakeholders (Hossain et al., 2020). A prime example is the blockchain architecture proposed by Zhang et al. (2018), which uses smart contracts—digital contracts on the blockchain that execute automatically—to enforce patient-defined rules for access. These smart contracts ensure that medical images can be viewed and modified only by authorized staff members, enhancing patient control over information.

Blockchain's immutable audit logs provide an open chain of all data exchanges such that medical image access and modification can be tracked by healthcare providers, thereby enhancing traceability and accountability (Esposito et al., 2018). This attribute finds great application in teleradiology, where multiple parties like radiologists, technologists, and third-party vendors can review a common dataset. Though it has many advantages, the application of blockchain technology comes with high computational loads and scalability concerns. With a greater number of medical images, blockchain networks take a long time to execute transactions, thus data acquisition is delayed (Lakhan et al., 2022). Recent research aims to develop sharding and off-chain storage blockchain architectures that can address these issues.

### Cybersecurity using Artificial Intelligence

Artificial intelligence emerged as a useful technology for enhancing cybersecurity in teleradiology using the power of machine learning (ML) and predictive analytics for detecting and evading risks. AI-driven systems search for access patterns of data to identify anomalies such as unauthorized logon and suspicious data transfer in real time (Xie et al., 2022). For instance, ML models are capable of detecting man-in-the-middle (MITM) attacks, where attackers intercept and alter communication between radiologists and teleradiology systems, by recognizing outliers from normal network traffic (Kruse et al., 2017). AI-driven systems enable threat blocking proactively, reducing the likelihood of data breaches.

However, the performance of AI depends largely on the diversity and quality of training data. Biasedness or incompleteness in these data may lead to false positives or missed threats, compromising system reliability (Nifakos et al., 2021). To address this, researchers advocate for federated learning, where AI models are learned institution by institution without using raw data, preserving privacy while improving model accuracy. Additionally, integrating AI with blockchain technology creates a synergistic effect, combining AI's real-time threat detection with blockchain's secure data-sharing capabilities. Bigini and Lattanzi (2022) proposed a hybrid AI-blockchain framework that automates threat response by triggering smart contracts to revoke access when suspicious activity is detected. Such innovations hold promise for strengthening teleradiology security but require further validation in real-world settings.

**Internet of Medical Things (IoMT)**

Internet of Medical Things (IoMT), comprising networked devices such as imaging scanners and wearable sensors, plays a central role in teleradiology by enabling real-time data collection and transmission. Light-weight crypto protocols, which are designed for low-resource devices, enable secure communication between IoMT devices and teleradiology platforms (Razaque et al., 2022). Such protocols minimize low computation overhead while enabling strong encryption, making them ideal for low-computing-power devices.

Despite these advances, IoMT devices are still vulnerable to sophisticated cyberattacks, such as multiple-input multiple-output (MIMO) attacks, where attackers employ multiple antennas to capture wireless signals (Sinha et al., 2017). To counter this, continuous authentication mechanisms have been developed to verify device identities dynamically in a session rather than relying on single-time authentication. Newaz et al. (2020) proposed a persistent authentication system using behavioral biometrics, such as device usage patterns, to detect unauthorized access. Though effective, the implementation of such schemes into large-scale teleradiology networks is complex and comes with intensive infrastructure investment. The future needs to focus on standardizing IoMT security protocols to enable compatibility across multiple devices and platforms. Table 1 and Figure 1 represent the technological advances in teleradiology security.

**Table 1. Key Technologies for Secure Data Exchange in Teleradiology**

| Technology | Description | Advantages | Challenges | References |
|---|---|---|---|---|
| **Encryption (PKI, HE)** | Asymmetric encryption and homomorphic encryption for secure data transmission. | Ensures confidentiality, integrity, and authenticity. | High computational overhead; noise accumulation in HE. | Simplicio et al., 2014; Acar et al., 2018; Gentry, 2019 |
| **Blockchain** | Decentralized ledger for secure EHR sharing and access control. | Immutable audit trails; patient-controlled access. | Scalability issues; high computational costs. | Zhang et al., 2018; Hossain et al., 2020; Lakhan et al., 2022 |
| **AI-DrivenAnalytics** | Machine learning for anomaly detection and threat prevention. | Real-time threat detection; predictive capabilities. | Requires robust datasets; potential for bias. | Kruse et al., 2017; Xie et al., 2022; Nifakos et al., 2021 |
| **IoMT Protocols** | Lightweight cryptography for connected medical devices. | Enables real-time data exchange; secure device communication. | Vulnerable to MIMO attacks; complex implementation. | Razaque et al., 2022; Sinha et al., 2017; Newaz et al., 2020 |

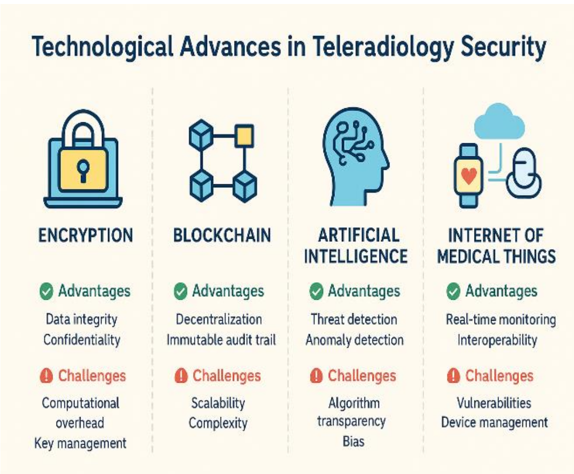


**Figure 1. Technological Advances in Teleradiology Security.**

**Privacy Challenges in Teleradiology**

While technological advancement has improved security in teleradiology, significant privacy concerns persist, driven by the confidential aspect of medical images and the complexities of electronic healthcare systems.

**Data Breaches and Cybersecurity Threats**

Teleradiology systems, via which highly sensitive medical images and patients' information are transmitted, are being targeted by cybercrime syndicates. Hacking ranked as the leading cause of healthcare data breaches in 2015, where every breached record cost $363, including remediation expenses, legal expenses, and reputational damage (Meisner, 2017). The MITM attacks pose an especially menacing threat because attackers are able to tap into, intercept, and alter communications between radiologists and imaging centers, leading to misdiagnoses or unplanned data exposure (Kumar et al., 2023). Insider threats, such as hospital workers obtaining unauthorized access to patient records, also contribute to these risks. Research in 2015 showed that insider threats accounted for a large proportion of healthcare data breaches, occasionally due to inadequate access controls and employee lack of training (Kruse et al., 2015). Countering these threats needs an all-encompassing approach, including efficient encryption, real-time monitoring, and end-to-end cybersecurity training for health professionals.

**Patient Confidentiality and Informed Consent**

Teleradiology's reliance on remote data transmission disrupts the traditional physician-patient relationship, jeopardizing confidentiality concerns of patients. As compared to personal consultations, in which patients enjoy a direct interaction with their providers, teleradiology often involves third-party intermediaries and cloud infrastructure, stripping patients of their control over who accesses their medical images (White, 2002). Informed consent processes in teleradiology are frequently suboptimal, with patients being unaware of the manner in which their data is shared or stored (Hameed et al., 2021). The General Data Protection Regulation (GDPR), effective in the European Union since 2018, mandates open patient consent for data processing and affords patients access, correction, and erasure rights on their data (El Majdoubi, 2022). Even so, GDPR adherence in teleradiology networks is not standardized, particularly for cross-border transfers, where inconsistencies in regulation have gaps in enforcement. Creating standardized consent processes and patient education initiatives is crucial to confidentiality and trust.

**Interoperability and Data Sharing**

Interoperability, or the ability of various healthcare systems to exchange data feasibly, is essential to facilitate teleradiology to deliver timely and accurate diagnoses. Standards like Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) facilitate data sharing among platforms but are privacy risks if security is lax (Shrivastava et al., 2021). Decentralized data-sharing sites, while more difficult to monitor, have single points of failure exposed to gargantuan breaches. On the other hand, decentralized platforms such as blockchain-based ones enhance privacy by distributing data to numerous nodes so that centralized attacks are less probable (Tong et al., 2013). Decentralized platforms are constrained in terms of scalability because the mass processing of medical images requires rich computational resources. Ensuring interoperability while preserving privacy poses a chief challenge, which requires the development of hybrid models that combine centralized monitoring with decentralized storage.

**Ethical and Regulatory Frameworks**

Patient privacy protection and safe information exchange in teleradiology are governed by the complex dynamic of regulatory demands and ethical guidelines. The frameworks possess the dual aims of providing safeguards for sensitive medical information, as well as protecting the necessity for accessibility and interoperability of healthcare systems around the globe. The next part presents the major regulatory standards and ethics that control teleradiology, outlining their implications, challenges, and development potential.

Regulatory frameworks provide the law as the ground on which protected health information (PHI) security can be guaranteed in teleradiology, mandating obligatory requirements for data security, privacy, and breach response. In the USA, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 remains a cornerstone of healthcare data protection. HIPAA mandates a comprehensive system of protection of PHI, including encryption in transmitting data, stringent access controls to limit access, and breach notification for the purpose of informing patients and the authorities in the event of a data breach (Amatayakul, 2000). The safeguards ensure that teleradiology systems are confidential and unviolated as far as transmission and storage of medical images are concerned. However, HIPAA's enforcement is mainly left to healthcare providers and their direct business associates, leaving loopholes in coverage for vendors of technology that is not healthcare-related, such as vendors of cloud services that are essential to teleradiology infrastructure (Kruse et al., 2015). It leaves compliance more difficult because third-party vendors are not subject to the same rigorous regulations, allowing more loopholes in the sharing of data.

In the EU, the General Data Protection Regulation (GDPR) implemented in 2018 sets an international standard for data privacy by putting patients' rights and organizations' accountability first. GDPR demands unambiguous patient consent for the processing of personal data, including medical images, and grants rights to data portability (the right to transfer their data to another provider) and the right to erasure (the right to request deletion of their data) (El Majdoubi, 2022). These provisions allow patients to exercise control over their health data in accordance with the principles of autonomy and transparency. However, GDPR's stringent rules pose problems to global teleradiology networks where adhering to similar jurisdictional norms becomes cumbersome. For instance, transmitting medical images from an EU hospital to a non-EU country radiologist requires adherence to GDPR's cross-border data transfer rules, which are generally implemented with complex legal agreements and additional security measures (Goelz et al., 2021). The lack of harmonization between HIPAA, GDPR, and other local legislation creates operational inefficiency and increases compliance expenses for global teleradiology networks.

In the United Kingdom, the Caldicott Principles impose yet another governance layer in the form of the appointment of data guardians to oversee patient confidentiality and ensure practices of data sharing are ethical in nature (White, 2002). These principles demand justification for the use of data, minimization of data sharing, and strict access controls, which improve accountability among teleradiology networks. However, the principles are largely advisory without the legally binding weight of HIPAA or GDPR and are vulnerable to inconsistent application among healthcare facilities (Goelz et al., 2021). The interplay of the regulatory systems highlights the need for global standardization to allow for ease of compliance and ensure consistent protection of patient data in teleradiology.

**Ethical Problems**

Ethical problems in teleradiology are still concerned with preserving patient autonomy, confidentiality, and trust in patient-provider relationships. The remote environment of teleradiology, where radiologists may never see patients in person, compromises the traditional physician-patient relationship, leading to loss of trust potentially (Strehle & Shabde, 2006). Ethical principles guide patient-centered policies, such as clear communication of storage, sharing, and safeguarding medical images (Hsu et al., 2015). Patients, for example, should be informed about the role of third-party vendors in teleradiology procedures and the procedures for safeguarding their information.

One of the greatest ethical challenges is obtaining informed consent in teleradiology. Unlike with usual healthcare settings, where consent is obtained outright, teleradiology may involve multiple actors, including imaging facilities, cloud servers, and distant radiologists, complicating the process of consent. Ethical guidelines require user-centric data-sharing patterns in which patients have fine-grained control over who can see their medical images and why (Jaiman & Urovi, 2022). Consent management platforms based on blockchain, for instance, allow patients to enter permission for viewing or processing their data through smart contracts, so that only the appropriate parties can view or process it. Such models provide maximum patient control and adhere to ethical guidelines of self-determination.

The application of AI-based diagnoses in teleradiology presents new ethical considerations, particularly transparency and accountability. AI algorithms deployed for imaging analysis need to be explainable to radiologists and patients in order to ensure that there is no loss of trust in diagnostic results (Williamson & Prybutok, 2024). For instance, when an AI system identifies a potential abnormality from an X-ray, radiologists must know the reasoning behind the recommendation of the AI in order to verify its accuracy. Likewise, patients should be notified if their diagnostic process involves AI in order to ensure transparency. There are also ethical guidelines that call for precautions against prejudice in AI systems, which could be generated by biased training data and yield erroneous or discriminatory diagnoses, particularly among underrepresented groups (Nifakos et al., 2021). Addressing these ethical issues requires continuous interaction among technologists, medical professionals, and ethicists to develop frameworks that guarantee patient well-being and trust. Table 2 and Figure 2 provide an overview of the regulatory & ethical frameworks comparison.

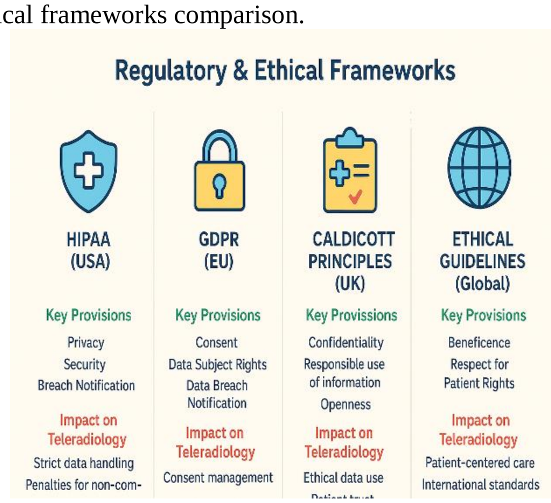


**Figure 2. Regulatory & Ethical Frameworks Comparison**

**Table 2. Regulatory and Ethical Frameworks for Teleradiology Privacy**

| Framework | Region | Key Provisions | Impact on Teleradiology | References |
|---|---|---|---|---|
| **HIPAA** | USA | Mandates encryption, access controls, and breach notifications for PHI. | Ensures secure data exchange but lacks coverage for non-healthcare tech. | Amatayakul, 2000; Kruse et al., 2015 |
| **GDPR** | EU | Requires explicit consent, data portability, and right to erasure. | Enhances patient control but complicates global compliance. | El Majdoubi, 2022; Jaiman & Urovi, 2022 |
| **Caldicott Principles** | UK | Appoints guardians to protect patient confidentiality. | Strengthens accountability in teleradiology networks. | White, 2002; Goelz et al., 2021 |
| **Ethical Guidelines** | Global | Emphasizes autonomy, transparency, and trust in healthcare. | Promotes user-centric data sharing and trust in AI diagnostics. | Hsu et al., 2015; Williamson & Prybutok, 2024 |

**Case Studies and Practical Implementations**

Practical uses of secure data exchange and privacy preservation in teleradiology provide insightful information on the practical implementation of theoretical techniques and models.

**Blockchain in Teleradiology Networks**

In 2020, Berlin demonstrated the viability of a blockchain-based teleradiology network and identified its capacity to enhance security and patient confidence (Goelz et al., 2021). The solution employed a permissioned blockchain to securely transfer medical images among authorized radiologists, hospitals, and imaging centers. Smart contracts were utilized to enforce patient-specified rules of access control so that only authorized individuals would be able to view designated images. This approach not only reduced the risk of tampering with data but also promoted GDPR's data minimization and explicit consent requirements. The study showed high patient trust, as patients were being informed about who was viewing their data and could revoke consent whenever necessary. The system was problematic in terms of scalability, as it required a high level of computational power to scan high-resolution medical images in bulk, and optimization in this area was crucial.

**AI-Driven Threat Detection**

In 2022, a pilot project in one of the biggest US hospitals implemented an artificial intelligence-powered cybersecurity solution to protect teleradiology workflow from unauthorized access attempts (Xie et al., 2022). The solution utilized machine-learning-based algorithms for real-time network traffic analysis and anomaly detection, such as unusual login behavior or spikes in data transmission. By identifying potential threats, such as man-in-the-middle attacks, the system reduced cases of data breaches by 30% in six months. However, the AI system had to be updated continuously with the training data in order to fight evolving cyber threats, such as new phishing tactics or emerging ransomware variants. The pilot emphasized integrating AI with other security controls, such as encryption and blockchain, to create a comprehensive defense strategy. It also emphasized the need to maintain ongoing investment in cybersecurity infrastructure to keep pace with fast-changing threat landscapes.

**Future Directions**

The future of secure data exchange and privacy in teleradiology lies in the unification of cutting-edge technologies, coordinated regulations, and patient-centric approaches. This section outlines primary directions for future development to overcome current limitations and make teleradiology systems more secure and accessible.

Blockchain, AI, and HE integration is a powerful means of developing secure frameworks that protect privacy and performance. They take advantage of each technology's strength: blockchain immutable audit trails for guaranteed data integrity, AI predictive analytics for real-time threat identification, and HE for privacy-preserving computations over encrypted data (Esposito et al., 2018). For example, the hybrid solution could utilize blockchain for access control, AI for anomaly detection, and HE for medical imaging in the cloud without compromising sensitive data. These architectures, however, are faced with computational efficiency as combining several energy-intensive technologies may introduce latency in teleradiology procedures. Future research should focus on developing lightweight algorithms and streamlined architectures to ensure hybrid models become viable for real-time diagnosis applications.

Regulatory non-harmonization between frameworks, such as HIPAA and GDPR, presents enormous challenges to the implementation of teleradiology worldwide. Differing requirements for data protection, consent, and cross-border data flows render compliance challenging for healthcare providers delivering services across different jurisdictions (Goelz et al., 2021). International frameworks of health data governance have been promoted by global organizations, such as the Organisation for Economic Co-operation and Development (OECD), to make it simple to abide by and also enable safe data exchange (OECD, 2013). Such frameworks could consist of standardized encryption, access controls, and breach notification protocols to enable the smooth operation of teleradiology networks across borders. Collaboration between governments, healthcare organizations, and technology vendors is required to develop and apply such standards so that patient information is stored securely wherever in the world.

Empowering patients as masters of their medical information is an important step towards enhancing privacy and trust in teleradiology. Dynamic consent models, facilitated through the use of blockchain, allow patients to manage permissions in real-time, allowing or disallowing access to specific providers or sets of data as and when necessary (Jaiman & Urovi, 2022). For example, a patient might utilize a blockchain-based app to choose specifically just a certain radiologist and for a specified time frame to view their MRI scan. M-health apps integrated into teleradiology platforms can also facilitate real-time consent management, providing patients with user-friendly interfaces for monitoring and managing data access (Alhammad et al., 2024). Patient-focused models are more consistent with autonomy and transparency principles, and they encourage trust and higher utilization of teleradiology services. Easy-to-use technology must be the area of future innovation to enable consent management for patients with any technical aptitude.

**Challenges and Limitations**

There has been significant progress, but several challenges hinder the large-scale deployment of secure teleradiology systems. Scalability is a significant issue with blockchain and homomorphic encryption, both of which require significant computational resources to process high volumes of medical images (Dai et al., 2022). That is particularly an issue in high-throughput settings, such as big hospitals or imaging centers, where tardiness in data processing can become an issue for diagnostic timeliness. Regulatory discontinuities across borders create additional barriers, with providers needing to navigate a mosaic of compliance regimes, increasing cost and complexity (Goelz et al., 2021). Furthermore, the prohibitive cost of deploying complex technology, such as AI-powered cybersecurity infrastructure and blockchain networks, may limit access in lower-resource settings, exacerbating healthcare inequities (Burghard, 2012). Addressing these challenges requires concerted efforts to develop low-cost, scalable solutions and standard regulatory templates that promote equity and access.

**Conclusion**

Teleradiology has transformed healthcare by making diagnostic expertise available remotely, but its reliance on digital infrastructure introduces stark security and privacy concerns. Improvements in encryption, blockchain, and AI provide promising alternatives to protect medical images and patient information, but challenges related to scalability, regulatory harmonization, and the cost of implementation remain. Ethical principles, such as patient autonomy, confidentiality, and trust, should inform the development and deployment of teleradiology technologies. Future studies should focus on the development of hybrid security models that combine blockchain, AI, and homomorphic encryption to enable secure, efficient, and privacy-preserving systems. They require global regulatory alignment and patient-centric privacy frameworks, supported by ease-of-use technologies, to render teleradiology secure, equitable, and accessible. The healthcare industry can unlock the full potential of teleradiology with patient trust and data privacy safeguarded by overcoming these issues using new-generation technologies.

**References**


1. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, *51*(4), 1-35. https://doi.org/10.1145/3214303
2. Alhammad, N., Alajlani, M., Abd-Alrazaq, A., Epiphaniou, G., & Arvanitis, T. (2024). Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: systematic review. *Journal of Medical Internet Research*, *26*, e50715. doi: 10.2196/50715
3. Amatayakul, M. (2000). Security measures required for HIPAA privacy. *Journal of Healthcare Information Management: JHIM*, *14*(4), 5-12. PMID: 11190262.
4. Bigini, G., & Lattanzi, E. (2022). Toward the interplanetary health layer for the internet of medical things with distributed ledgers and storages. *IEEE Access*, *10*, 82883-82895. doi: 10.1109/ACCESS.2022.3196933.
5. Burghard, C. (2012). Big data and analytics key to accountable care success. *IDC health insights*, *1*, 1-9.
6. El Majdoubi, D., El Bakkali, H., Sadki, S., Maqour, Z., & Leghmid, A. (2022). The systematic literature review of privacy-preserving solutions in smart healthcare environment. *Security and Communication Networks*, *2022*(1), 5642026. https://doi.org/10.1155/2022/5642026
7. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, *5*(1), 31-37. doi: 10.1109/MCC.2018.011791712
8. Filkins, B. L., Kim, J. Y., Roberts, B., Armstrong, W., Miller, M. A., Hultner, M. L., ... & Steinhubl, S. R. (2016). Privacy and security in the era of digital health: what should translational researchers know and do about it?. *American journal of translational research*, *8*(3), 1560. PMID: 27186282; PMCID: PMC4859641
9. Gentry, C. (2019). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st ACM Symposium on Theory of Computing*, 169–178. https://doi.org/10.1145/1536414.1536440
10. Goelz, L., Arndt, H., Hausmann, J., Madeja, C., & Mutze, S. (2021, December). Obstacles and solutions driving the development of a national teleradiology network. In *Healthcare* (Vol. 9, No. 12, p. 1684). MDPI. https://doi.org/10.3390/healthcare9121684
11. Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science*, *7*, e414. DOI: 10.7717/peerj-cs.414
12. Hossain, M., Islam, S. R., & Ali, M. (2020). Blockchain-based secure data sharing in healthcare systems. *Journal of Medical Systems*, *44*(12), 1–12. https://doi.org/10.1007/s10916-020-01634-6
13. Hsu, W. W. Q., Chan, E. W. Y., Zhang, Z. J., Lin, Z. X., Bian, Z. X., & Wong, I. C. K. (2015). Chinese medicine students' views on electronic prescribing: A survey in Hong Kong. *European Journal of Integrative Medicine*, *7*(1), 47-54. https://doi.org/10.1016/j.eujim.2014.09.134
14. Jaiman, V., Pernice, L., & Urovi, V. (2022). User incentives for blockchain-based data sharing platforms. *Plos one*, *17*(4), e0266624. https://doi.org/10.1371/journal.pone.0266624

15. Kruse, C. S., Argueta, D. A., Lopez, L., & Nair, A. (2015). Patient and provider attitudes toward the use of patient portals for the management of chronic disease: a systematic review. *Journal of medical Internet research*, *17*(2), e40. [doi: 10.2196/jmir.3703](https://doi.org/10.2196/jmir.3703)
16. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263
17. Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics*, *12*(9), 2050. https://doi.org/10.3390/electronics12092050
18. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., ... & Wang, W. (2022). Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE journal of biomedical and health informatics*, *27*(2), 664-672. doi: 10.1109/JBHI.2022.3165945
19. Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73. https://doi.org/10.12775/CJFA.2017.017
20. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), 1-44. https://doi.org/10.1145/3453176
21. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119
22. OECD. (2013). Data-driven healthcare innovation, management and policy, DELSA/HEA (2013) 13.
23. Razaque, A., Amsaad, F., Abdulgader, M., Alotaibi, B., Alsolami, F., Gulsezim, D., ... & Hariri, S. (2022). A mobility-aware human-centric cyber–physical system for efficient and secure smart healthcare. *IEEE Internet of Things Journal*, *9*(22), 22434-22452. doi: 10.1109/JIOT.2021.3140090
24. Shrivastava, U., Song, J., Han, B. T., & Dietzman, D. (2021). Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics*, *148*, 104401. https://doi.org/10.1016/j.ijmedinf.2021.104401
25. Simplicio, M. A., Iwaya, L. H., Barros, B. M., Carvalho, T. C., & Näslund, M. (2014). SecourHealth: a delay-tolerant security framework for mobile health data collection. *IEEE journal of biomedical and health informatics*, *19*(2), 761-772. doi: 10.1109/JBHI.2014.2320444
26. Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017, July). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In *2017 International Conference on Signal Processing and Communication (ICSPC)* (pp. 288-293). IEEE. doi: 10.1109/CSPC.2017.8305855
27. Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics?. *Archives of disease in childhood*, *91*(12), 956-959. https://doi.org/10.1136/adc.2006.099622
28. Tong, Y., Sun, J., Chow, S. S., & Li, P. (2013). Cloud-assisted mobile-access of health data with privacy and auditability. *IEEE Journal of biomedical and health Informatics*, *18*(2), 419-429. doi: 10.1109/JBHI.2013.2294932
29. White, P. (2002). Legal issues in teleradiology—distant thoughts!. *The British Journal of radiology*, *75*(891), 201-206. https://doi.org/10.1259/bjr.75.891.750201
30. Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences*, *14*(2), 675. https://doi.org/10.3390/app14020675
31. Xie, Y., Zhang, K., Kou, H., & Mokarram, M. J. (2022). Private anomaly detection of student health conditions based on wearable sensors in mobile cloud computing. *Journal of Cloud Computing*, *11*(1), 38. https://doi.org/10.1186/s13677-022-00300-x
32. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in computers* (Vol. 111, pp. 1-41). Elsevier. https://doi.org/10.1016/bs.adcom.2018.03.006