THE EUROPEAN SOCIETY OF MEDICINE
Medical Research Archives, Volume 13 Issue 2

RESEARCH ARTICLE

Implementation of Cybersecurity systems in Teleradiology Services- Best Practices

Dr Neetika Mathur [1], Saravanan Seralathan [2], Dr Arjun Kalyanpur [3]

[1] Training and Research Coordinator, Teleradiology Solutions, Plot No. 7G, Opposite Graphite India, Whitefield, Bengaluru, Karnataka 560048, India
[2] CIO/CISO, Teleradiology Solutions, Plot No. 7G, Opposite Graphite India, Whitefield, Bengaluru, Karnataka 560048, India
[3] Chief Radiologist and CEO, Teleradiology Solutions, Plot No. 7G, Opposite Graphite India, Whitefield, Bengaluru, Karnataka 560048, India

OPEN ACCESS

PUBLISHED
28 February 2025

CITATION
Mathur, N., Seralathan, S., et al., 2025. Implementation of Cybersecurity systems in Teleradiology Services- Best Practices. Medical Research Archives, [online] 13(2). https://doi.org/10.18103/mra.v13i2.6237

DOI
https://doi.org/10.18103/mra.v13i2.6237

ISSN
2375-1924

ABSTRACT

Teleradiology services provides access to healthcare services by allowing radiologists to interpret medical images remotely particularly in rural or underserved regions, while enabling faster diagnostics and treatment. In the last twenty years, the increased internet penetration and digital infrastructure, technological advancements such as Radiology Information System, Picture Archiving and Communication Systems and application of deep learning algorithms in imaging technology has resulted in the significant growth in this field but has also engendered a significant cybersecurity concern. It is important for providers and users to be constantly vigilant and to implement strong information security practices to protect against cyber-threats and to ensure the confidentiality, integrity, and availability of patient data. With cyber threats evolving at an alarming rate, every employee plays a crucial role in protecting an organization from potential attacks. Employees are often the first line of defense, acting as gatekeepers against breaches, phishing scams, and other malicious activities. Therefore, regular employee training is a crucial aspect of the successful implementation of cybersecurity systems. This article provides an overview of the best practices that an ideal cybersecurity system of a teleradiology service provider should follow. An ideal cybersecurity workflow in a teleradiology reporting system should include risk assessment, policy and procedure development, network security through firewalls, data and image encryption, regular employee training, incidence response plan and continuous monitoring and evaluation of the cybersecurity system. A deep understanding of the topic is integral in ensuring the safe, secure and successful implementation of teleradiology in healthcare.

Keywords: Cybersecurity, Teleradiology, Best Practice, Cyberattacks, Healthcare

Introduction

In today's digital era of internet connectivity and advanced technologies, cyberthreats are widespread affecting the workflow of every sector. The healthcare sector, including hospital and pharmaceutical companies, is no exception and requires robust cybersecurity systems to stay protected. Teleradiology, a sub-discipline of telemedicine, where the transmission and interpretation of the radiological images from one site to another site via digital technology, is an integral part of modern healthcare system[1]. Teleradiology services provides access to healthcare services by allowing radiologists to interpret medical images remotely particularly in the emergency setting or in rural or underserved regions, thereby enabling faster diagnostics and treatment [2,3]. In the last twenty years, given increased internet penetration and digital infrastructure, technological advancements such as Radiology Information System (RIS), Picture Archiving and Communication Systems (PACS) and most recently the application of deep learning algorithms in imaging technology has resulted in the significant growth in this field. According to a report, the teleradiology market is predicted to grow from $7.3 billion in 2021 to $14.8 billion by 2026 globally with Compound Annual Growth Rate (CAGR) at 15.3%[4]. However, in India, it is expected to rise from 1.85 billion USD in 2023 to 2.43 billion USD by 2030 with a CAGR of 12.11% driven by the increasing demand for remote healthcare services and radiologist shortages in rural areas[5]. However, this digital revolution has in its wake brought significant cybersecurity concerns.

In order to deliver quick and quality care, teleradiology systems rely on a number of interconnected digital systems which are vulnerable to cyberattacks[6]. Furthermore, the healthcare industry, including teleradiology, is a main target for cyberattacks due to the valuable nature of medical data [7]. Hackers are increasingly interested in exploiting vulnerabilities in healthcare systems, leading to unauthorized access, data breaches, and ransomware attacks. Thus, cybersecurity plays a crucial role in safeguarding sensitive medical data and patient information. It has become a key requisite for ensuring the privacy, confidentiality, and integrity during the transmission, storage, and handling of patients' sensitive data such as dates of birth, medical history, and financial data. Cybersecurity provides protection to the internet-connected systems, networks, and programs from digital attacks [8,9]. The global Cybersecurity Market is estimated to rise from 190.4 billion USD in 2023 to 298.5 billion by 2028 at a CAGR of 9.4%.

The convergence of healthcare and technology in the teleradiology services, has given rise to several challenges which makes cybersecurity a mandatory requisite. Teleradiology services entail transmission of patient health data, referred to as Protected Health Information (PHI) and radiological images across networks, which are especially vulnerable to breaches. Moreover, RIS and PACS, which store, retrieve, and display medical images expose more entry points for cyberattacks. Mobile devices, cloud platforms, and remote access connections all present potential vulnerabilities that attackers can exploit.

Objectives

Having been involved with teleradiology for over two decades, and having provided teleradiology reporting services to over 150 institutions worldwide, we understand the vital importance of security and aim to capture initiatives that can be undertaken to help all organizations think through their security and protect the patients' data and thus positively impact patient care. Thus, the aim and scope of this article is to provide an overview of the cybersecurity challenges associated with the teleradiology practice and a review of the best practices that a teleradiology service should follow to protect patient data while ensuring compliance with healthcare regulations. A deep understanding of the topic is integral to ensuring the safe, secure, and successful implementation of teleradiology in healthcare.

The Research problem is as follows:

Healthcare is becoming increasingly dependent on information technology and its related infrastructure. Teleradiology is an example. Healthcare IT systems, including teleradiology systems are vulnerable to cybersecurity attacks. Cybersecurity attacks are on the rise worldwide and have recently been targeting healthcare IT systems.

The research question is what are the available best practices that a teleradiology service provider can employ in order to protect their ITR infrastructure and patient health information.

Methodology

In this review article, we have shared our own perspective and experience as a global teleradiology service provider over the last twenty years. We have shared best practices in cybersecurity, as are currently deployed within our organization, and which form a template that other organizations may benefit from and follow. This is combined with a review of the literature published on the subject. To generate this, a literature search was conducted on the Google search engine, focusing on articles on the subject, published in journals in the English language. Keywords used for the literature search were 'Cybersecurity in teleradiology' and 'Cybersecurity in healthcare'.

Results

According to a report, there were a record of 1.9 million cyberattacks against the healthcare industry in India in 2022 [10]. Another report discloses that the Indian healthcare sector has turned out to be a big target for cybercriminals, leading to a mean of 6,935 cyberattacks per week over the last six months, opposed to 1,821 attacks per organization internationally. This shocking trend draws attention on the elevated attack counts because of the quick acquisition of technologies such as electronic health records (EHRs), RIS, PACS, telehealth services, and smart Machine-to-Machine (M2M) devices [11]. According to a report listing the top ten most low-risk and top ten most high-risk countries based on a Cyber-Safety scoring system which integrates data from three important cybersecurity authorities, namely the National Cyber Security Index (NCSI) (updated on a live basis), the Global Cybersecurity Index (GCI) (2020), and the Cybersecurity Exposure Index (CEI) (2020), Belgium is the

lowest risk country while Afghanistan is the most high-risk country [12]. India holds 47th position along all 93 countries of the world with the cyber safety score of 65.85.

Various cybersecurity incidents which affected teleradiology and healthcare organizations in general, have been reported in several studies [5,10,11]. These cases highlight the vulnerabilities and consequences of inadequate cybersecurity measures. On 23rd Nov 2022, All India Institute of Medical Sciences (AIIMS) Delhi, India's premier medical institute, research centre and hospital, was attacked by cyber hackers on its server, shutting it down. In this malicious attack, health services including registration, admission, billing and discharge were disrupted, the patient data was compromised, emphasizing the need for stronger cybersecurity measures to protect sensitive information. This is by a long shot, the latest ransomware attack in India which surprised the whole healthcare industry [13]. WannaCry Ransomware Attack (2017) was another damaging cyberattacks in history, targeted healthcare institutions globally, including the UK's National Health Service (NHS), where hospitals were forced to cancel appointments, and radiologists could not access patient data or images, significantly delaying care. The attack exposed the vulnerability of legacy systems and the critical need for cybersecurity updates in healthcare [14]. A common type of targeted ransomware attack involves encrypting an organization's entire disk assets through remote activation, rendering them inaccessible. The attackers then demand payment, typically in cryptocurrency, in exchange for a decryption key. Faced with significant service disruptions, the affected organization may feel compelled to comply [15]. In 2020, the University of Vermont Medical Center experienced a ransomware attack that severely disrupted its teleradiology services. Radiologists were unable to access PACS, delaying diagnosis and treatment for patients. The attack highlighted the importance of regular backups, disaster recovery plans, and robust cybersecurity protocols to mitigate the effects of ransomware [16].

Best practices by an ideal cybersecurity system of a teleradiology service provider

As a teleradiology service provider, it is paramount to be mindful of the various cybersecurity threats such as malware, ransomware attacks, phishing attacks etc., lurking the industry. Hackers may try to gain access to electronic health records (EHR) or protected health information (PHI) in order to steal sensitive patient data or disrupt the operations of teleradiology service provider/ healthcare organization. It is essential for the organization to stay vigilant and implement strong information security practices to protect against these threats and to ensure the confidentiality, integrity, and availability of the patient data. An ideal cybersecurity workflow in a teleradiology reporting system should include risk assessment, policy and procedure development, network security through firewalls, data and image encryption, regular employee training, incidence response plan and continuous monitoring and evaluation of the cybersecurity system (Figure 1).

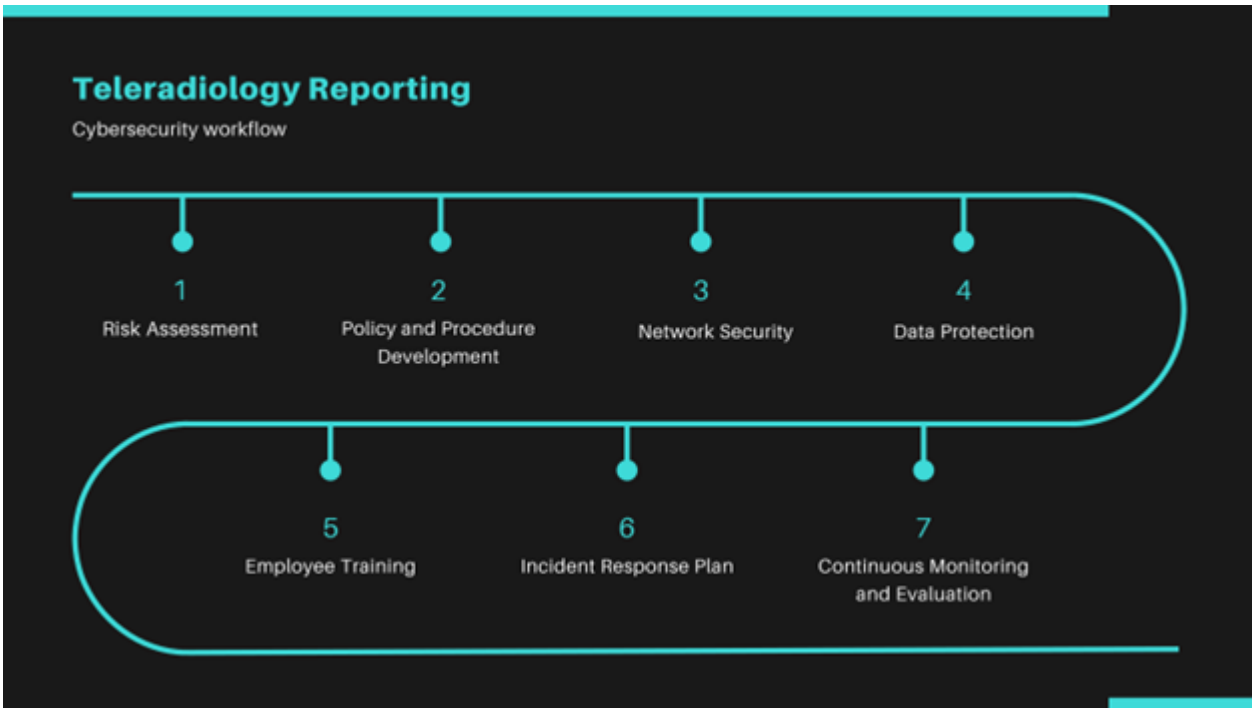

Figure 1. An ideal Cybersecurity workflow in a teleradiology reporting system

Cybersecurity services should be implemented and integrated with modern teleradiology system in such a way that confidentiality, integrity, accessibility, liability, non-repudiation of information, are demonstrated when information is created, updated, revised, transferred, stored, deleted, archived, and destructed[17-19]. The best practices that an ideal cybersecurity system of a teleradiology service provider should follow are as follows (Figure 2):

1. **Network security through Firewalls:** Robust firewalls should be installed and maintained to safeguard teleradiology systems by regulating the incoming and outgoing network traffic, ensuring data integrity and patient confidentiality. Web Application Firewall (WAF) is required for layer 7 security for RIS and PACS applications. SSL (Secure Sockets Layer), Virtual private network (VPN): Site to Site IPsec (Internet Protocol Security) tunnel is required to build secure

data transfer communication between client and teleradiology service provider networks. They serve as a shield for the radiology networks from unauthorized access and potential cyber threats [19-21].

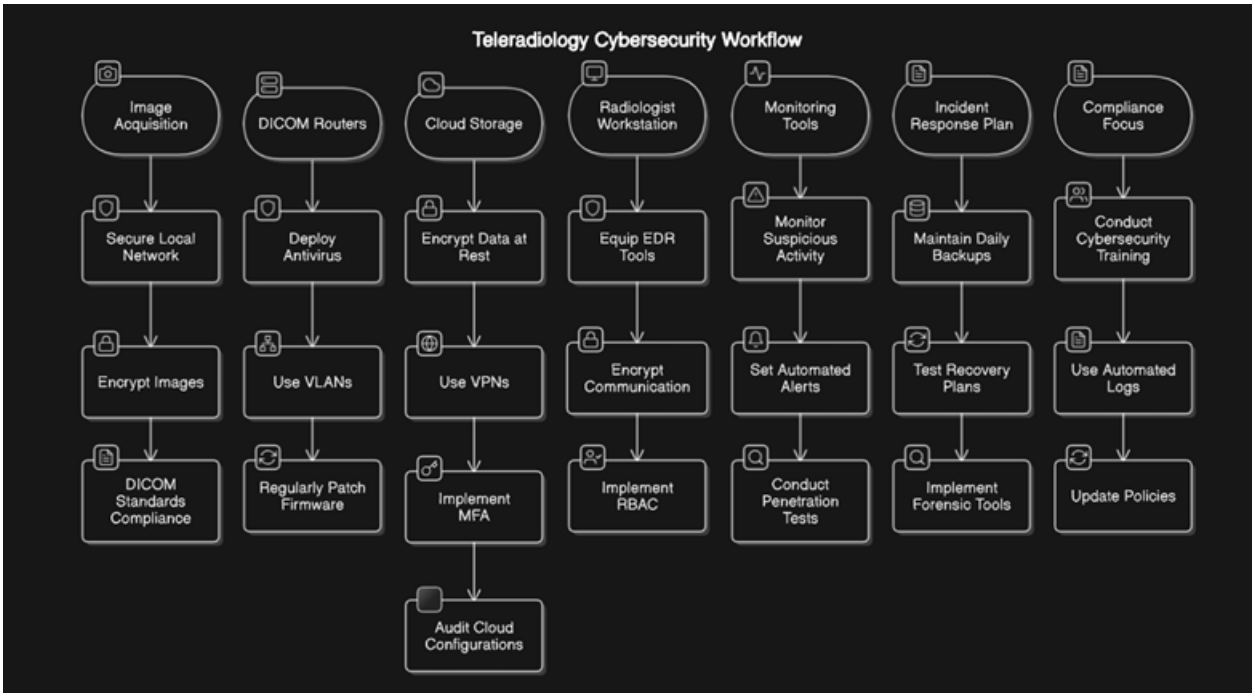

Figure 2. Cybersecurity detailed workflow demonstrating best practices to be followed

2. **Data Protection:** Encryption is one of the cutting-edge resolutions to protect data in transit (between devices and over networks) and at rest (stored on computers and storage devices). It involves converting data into unreadable code, which can only be deciphered through the use of a specific key. Moreover, keeping keys apart from encrypted data provides an additional layer of protection. Encryption also allows collaborative working over the encrypted data between multiple healthcare providers and radiologists. Teleradiology platforms should implement strong encryption protocols, such as SSL/ Transport Layer Security (TLS) for data in transit and Advanced Encryption Standard (AES)-256 for data at rest [22-24].
3. **User Authentication:** It is a critical component for preventing unauthorized access to teleradiology systems. Implementing Multi-Factor Authentication (MFA) creates an extra layer of security for the users, by verifying their identity through a password and a one-time code sent to their phone. Moreover, it is also advisable to change passwords periodically and avoid sharing them with others. It can significantly reduce the risk of compromised accounts due to phishing attacks or weak passwords[23].
4. **Digital Signatures:** Implementing digital signatures and time stamps provide an additional layer of security for PACS systems by verifying the authenticity and integrity of data. It ensures that the medical images and reports are not altered or tampered[15].
5. **Role-Based Access Control (RBAC):** Implementation of RBAC limits the data access based on user roles in the organization to minimize exposure and misuse of patients' sensitive data[25].
6. **Regular Software Updates and Patches:** The teleradiology systems, including all hardware and software, RIS, PACS and DICOM servers should be regularly updated provided patches for known vulnerabilities. Older systems should be replaced or upgraded to ones supporting modern cybersecurity features[19].
7. **Continuous Monitoring and Evaluation through IDS and IPS solutions:** In teleradiology, deployment of Intrusion Detection Systems (IDS) which scans network traffic for potential threats, help in alerting administrators to malicious attacks and unauthorized access to patient data. Intrusion Prevention Systems (IPS) in radiology actively intervene to block or mitigate cyberattacks, safeguarding sensitive medical information and ensuring the integrity of diagnostic processes[24,26,27].
8. **Endpoint Detection & Response (EDR) Solutions:** EDR scans endpoint devices such as virtualized desktops, laptops, mobile phones, and workstations to identify the signals of a cyberattack, audit contextualized information on threats to determine their root cause and fix them by automated remediation or by alerting a human stakeholder. Real-time monitoring and advanced encryption fortify the digital perimeter of imaging systems, protecting them from illegal access and prospective breaches[28].
9. **Incident Response Plan:** An extensive and effective incident response plan should be prepared defining procedures for detecting, detorting to, and mitigating data breaches or security incidents efficiently. Prompt actions like containment of the compromised systems, replacing the credentials, and restricting user access, enforcing updated security policies, and conducting regular audits and assessments prevents spreading of the incident. It thereby reduces downtime, and maintains quality standards in diagnostic imaging services. A teleradiology service provider and network healthcare organizations must have a HIPAA-compliant incident response plan for handling patient data security breaches [29,30].

10. **Employee Training:** Employees are often the first line of defense, acting as gatekeepers against breaches, phishing scams, and other malicious activities. Therefore, regular employee training is a crucial aspect for successful implementation of cybersecurity system. Regular cybersecurity training and awareness programs should be conducted for all employees i.e. radiologists, technicians, and staff, to reinforce best practices, build phishing detection skills, and practical tips should be provided to identify and mitigate or thwart potential cyber threats in future scenarios. Compliance-oriented employee training is required to ensure the meticulous follow-through of safety procedures and regulatory standards, minimizing risks related to medical imaging procedures[20].
11. **Data Backup and Disaster Recovery:** Regular data backups are essential for recovering from ransomware attacks or other data loss incidents. The teleradiology service provider and client healthcare institutions should implement automated backup systems that store copies of radiological data in secure, offsite locations. A robust disaster recovery plan should be in place to ensure that radiological services can be restored quickly in the event of a cyberattack[22,31].
12. **Vendor Risk Management:** Teleradiology services providers must carefully evaluate the cybersecurity practices of third-party vendors that provide healthcare. This includes conducting regular security assessments, ensuring compliance with regulations like HIPAA and GDPR, and requiring vendors to implement strong security measures, such as encryption and MFA[22].
13. **Compliance with Legal and Regulatory Standards:** Teleradiology system must comply with ethical and regulatory requirements. Teleradiology services providers should emphasize on working in compliance with regulations such as Health Insurance Portability and Accountability Act (HIPAA) (U.S.) and The General Data Protection Regulation (GDPR) (EU) for protecting confidentiality, integrity, and availability of patients' electronic Protected Health Information (ePHI) data and implement an information security management system (ISMS) in line with international standards ISO/IEC 27001(32,33). It should have clear protocols for data breach detection, reporting, and notification[19]. Digital Personal Data Protection Act, 2023 (DPDP Act) is the first ever comprehensive and union-wide data protection law enacted on August 11, 2023 in India[34].
14. **Cloud Security Audit:** Cloud security audits authenticate organizations' compliance with laws, regulations, frameworks, and standards such as the GDPR, HIPAA, and PCI DSS, assisting mitigate prospective data breaches and consequential financial loss and reputational damage[35].

Emerging Technologies in Strengthening Cybersecurity

AI and Machine Learning: Artificial intelligence (AI) and machine learning (ML) have the potential to significantly enhance cybersecurity in teleradiology. These technologies can be used to detect and respond to cyber threats in real-time, detect anomalies in network traffic, identify patterns of suspicious activity, and automate threat detection and security tasks[36].

Blockchain for Data Integrity: Blockchain is defined as a decentralized peer-to-peer (P2P) network that conserves, pools, and records patients' data. It is emerging as a new paradigm in maintaining the integrity and traceability of radiological data[37,38].

Secure Cloud Solutions: Cloud security is the combination of cloud technology, procedures, and best practices with built-in security for data storage and analysis. Leveraging cloud-based solutions can help protect data stored in the cloud from unauthorized breaches[39].

Conclusion:

Cybersecurity in teleradiology is a critical issue that a teleradiology service provider must address to protect sensitive patient data from malicious attacks and assure the safe delivery of radiological services. By advanced planning and implementing cybersecurity best practices such as encryption, multi-factor authentication, regular software updates, and AI-driven threat detection, adopting a "Zero Trust" security framework to defend every access attempt, even within the network and regular cybersecurity training, teleradiology service provider and healthcare institutions can mitigate cyberattacks and risks, continue to provide high-quality care to patients and build a Cyber-Resilient Teleradiology Ecosystem. A coordinated and collaborative effort by designing common cybersecurity policies, contract and tools that covers all partners and entities viz-a-viz teleradiology service provider, healthcare providers, technology vendors, and cybersecurity experts, is essential in establishing cybersecurity. This approach preserves the privacy, confidentiality, and integrity of data, while preventing data breaches or unauthorized data access and ensures that patients may continue to hold trust in the systems that store and protect their healthcare information while simultaneously protecting their health.

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

References

1. Kalyanpur A, Nair HTS, Mathur N. Teleradiology Service is Indispensable in the Indian Healthcare Sector. *International Journal of Health Technology and Innovation*, 2023; 2(2):1-3,
2. Chandramohan A, Krothapalli V, Augustin A, Kandagaddala M, Thomas HM, Sudarsanam TD, et al. Teleradiology and technology innovations in radiology: status in India and its role in increasing access to primary health care. *The Lancet Regional Health - Southeast Asia*. Apr 2023 https://doi.org/10.1016/j.lansea.2023.100195,
3. Burute N, Jankharia B. Teleradiology: The Indian perspective. *Indian J Radiol Imaging*. 2009; 19(1):16–8.
4. Markets and Markets. Teleradiology Market by Product and service (Services, Hardware, Software (PACS, RIS)), Imaging Technique (MRI, CT, X-ray, Ultrasound, Mammograpy, Nuclear Imaging), End User (Hospitals, Diagnostic Centers & Laboratories) & Region- Global Forecast to 2026. Available at https://www.marketsandmarkets.com/Market-Reports/teleradiology-market-8937290.html Accessed 24 December 2024.
5. Medical Buyer. Available at https://www.medicalbuyer.co.in/india-teleradiology-market-to-hit-usd-2-43-billion/ Accessed 24 December 2024.
6. Nguyen XV, Petscavage-Thomas JM, Straus CM, Ikuta I. Cybersecurity in radiology: Cautionary Tales, Proactive Prevention, and What to do When You Get Hacked. Current Problems in Diagnostic Radiology. Jul 2024, https://doi.org/10.1067/j.cpradiol.2024.07.010
7. Ackcent Cybersecurity. Why the Healthcare Industry Is a Prime Target for Cyberattacks Ackcent Cybersecurity May 15, 2023 https://ackcent.com/why-the-healthcare-industry-is-a-prime-target-for-cyberattacks/
8. Cybersecurity Healthcare. Enhancing Security with Healthcare Data Encryption Solutions. February 8, 2024 https://www.cit-net.com/enhancing-security-with-healthcare-data-encryption-solutions /.
9. Kelley, K: What is Cybersecurity and Why It is Important? Nov 17, 2024 https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security#:~:text=Cybersecurity%20is%20the%20protection%20to,data%20breaches%2C%20and%20financial%20losses
10. Ang A: 1.9 million cyberattacks against Indian healthcare recorded in 2022, Healthcare IT News, December 05, 2022 https://www.healthcareitnews.com/news/asia/19-million-cyberattacks-against-indian-healthcare-recorded-2022
11. Indian healthcare sector faces 6,953 cyberattacks weekly, outpacing global rates: Check Point threat intelligence report, Express Computer. Jun 28, 2024. https://www.expresscomputer.in/news/indian-healthcare-sector-faces-6953-cyberattacks-weekly-outpacing-global-rates-check-point-threat-intelligence-report/113528/
12. Seon. Available at https://seon.io/resources/global-cybercrime-report/ Accessed 24 December 2024.
13. Gandhi P, Pahwa S. All India Institute of Medical Sciences (AIIMS), Delhi: Cyberattack Puts Digitalisation Under Scanner. JIM [Internet]. Apr 2024. Available from: https://jim.imibh.edu.in/pages/table-of-contents/fulltext/?id=72&title=All+India+Institute+of+Medical+Sciences+(AIIMS),+Delhi:+Cyberattack+Puts+Digitalisation+Under+Scanner
14. Lessing, M. Case Study: WannaCry Ransomware Available from: https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-wannacry-ransomware/ Accessed 24 December 2024.
15. Chen, P.-H., Bodak, R., Gandhi, N.S. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *J Digit Imaging*, 2021; 34: 731–740. https://doi.org/10.1007/s10278-021-00466-x
16. Namoca E: Ransomware Attack on the University of Vermont Health Network March 4, 2021 https://westoahu.hawaii.edu/cyber/ics-cybersecurity/ics-weekly-summaries/ransomware-attack-on-the-university-of-vermont-health-network/
17. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity in PACS and Medical Imaging: an Overview. *J Digit Imaging*, 2020 Dec; 33(6):1527–42.
18. Özmen MN, Dicle O, Şenol U, Aydıngöz Ü. TSR guidelines for the practice of teleradiology: 2021 update. *Diagn Interv Radiol.*, Jul 2021; 27(4):504–10.
19. Ruotsalainen P. Privacy and security in teleradiology. *European Journal of Radiology*, Jan 2010; 73(1):31–5.
20. Kalyanpur A, Nair HTS, Mathur N. Teleradiology Service is Indispensable in the Indian Healthcare Sector. *International Journal of Health Technology and Innovation*, 2023; 2(2):1-3.
21. Liu D. and Zhang J. Y. Case Study of Security in Teleradiology Reporting System for Management of Data from Multiple Enterprises, 2011; 2(4).
22. Databrackets, Available from: https://databrackets.com/cybersecurity-and-compliance-best-practices-for-radiology/ Accessed 24 December 2024.
23. Enhancing Security with Healthcare Data Encryption Solutions Cybersecurity, Healthcare February 8, 2024 Available from: https://www.cit-net.com/enhancing-security-with-healthcare-data-encryption-solutions/ Accessed 24 December 2024.
24. Zafar S. R. Data Security in Teleradiology: The Power of Homomorphic Encryption 2023. https://www.linkedin.com/pulse/unlocking-data-security-teleradiology-power-encryption-zafar/
25. Frontegg, Available from: https://frontegg.com/guides/rbac Accessed 24 December 2024.
26. Hady AA, Ghubaish A, Salman T, Unal D, Jain R: Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study. *IEEE Access*, 2020; 8:106576–84.
27. Akram F, Liu D, Zhao P, Kryvinska N, Abbas S, Rizwan M. Trustworthy Intrusion Detection in E-Healthcare Systems. *Front Public Health*, 2021; 9:788347
28. BasuMallick C: Top 10 Endpoint Detection and Response Tools in 2022, 2022.

https://www.spiceworks.com/it-security/endpoint-security/articles/best-edr-tools/
29. Medtrainer, Available from: https://medtrainer.com/blog/healthcare-incident-response-plan/ Accessed 24 December 2024.
30. Check point, Available from: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-incident-response/the-6-phases-of-an-incident-response-plan/#:~:text=An%20incident%20response%20plan%20is,security%20incidents%20within%20an%20organization, Accessed 24 December 2024.
31. DrKumo, Available from: https://drkumo.com/tips-for-cybersecurity-for-healthcare-providers/, Accessed 24 December 2024.
32. RSI Security, Cybersecurity Best Practices for Telemedicine, 2020. https://blog.rsisecurity.com/cybersecurity-best-practices-for-telemedicine/,
33. Alder S: What is ISO/IEC 27001 in Healthcare? Feb 6, 2024. https://www.hipaajournal.com/iso-iec-27001-in-healthcare/#:~:text=ISO%2FIEC%2027001%20in%20healthcare%20is%20a%20standard%20for%20managing,an%20information%20security%20management%20system,
34. Singh M. and Musyuni P: Digital Health Laws and Regulations India 2024. 2024. https://iclg.com/practice-areas/digital-health-laws-and-regulations/india,
35. Crowdstrike, Available from: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-audit/ Accessed 24 December 2024.
36. Kelly BS, Quinn C, Belton N, Lawlor A, Killeen RP, Burrell J: Cybersecurity considerations for radiology departments involved with artificial intelligence. *Eur Radiol*, Dec 2023; 33(12):8833–41,
37. Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S.: Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks* 2, 130–139, 2021; https://doi.org/10.1016/j.ijin.2021.09.005
38. Kshetri, N: Blockchain and Electronic Healthcare Records [Cybertrust]. *Computer 51*, 2018; 59–63, https://doi.org/10.1109/MC.2018.2880021
39. Kaspersky, What is Cloud Security? Available from: https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security, Accessed 24 December 2024.

