Cyber Resilience in Healthcare: Securing Lifesaving Infrastructure in Digital Age, Advancing AI Technology and Protection for Data Privacy and Medical Device

Neha N. Buddhadev[1] and Dr. Trupesh M. Pethani[2]

[1,2] Department of Pharmaceutical Sciences, Saurashtra University, Rajkot, Gujarat, India. (360005)

Abstract:

Digital healthcare is transforming modern medicine by integrating technologies that enable personalized, efficient, and data-driven patient care. In India, the Digital Information Security in Healthcare Act (DISHA) provides a framework for managing digital health data, though definitions for areas like digital therapeutics are still developing. Innovations such as wearable sensors and connected medical devices enhance real-time monitoring, particularly for chronic disease management and specialized patient groups. However, connecting medical devices to IT networks introduces serious cybersecurity risks, including data breaches, service disruptions, and cyberattacks. These challenges threaten patient privacy and system reliability. Artificial intelligence (AI) is increasingly used to strengthen healthcare cybersecurity by detecting anomalies, predicting threats, and automating responses in real time. This article explores the intersection of digital health, cybersecurity, and AI, highlighting the need for strong regulatory frameworks and intelligent security solutions. Robust protections are essential to safeguard patient safety, maintain data integrity, and build trust in a rapidly digitizing healthcare ecosystem.

Key words: AI, Cybersecurity Data Privacy, Digital Health, Medical Device

Introduction

Digital healthcare is a multidisciplinary field at the intersection of medicine and digital technology, transforming healthcare delivery through integrated platforms, tools and services. It enhances efficiency and enables more personalised patient care, aligning with the broader concept of "digital health".

The rapid evolution of digital technologies-particularly in data gathering and communication has transformed how health information is collected, exchanged and analysed. Advances in data collection and communication have transformed how health data is gathered, shared and analysed, supporting better clinical decisions [2]. Key objectives include minimizing patient harm, enhancing safety, and delivering high-quality, timely, and equitable healthcare. Wearable sensors monitor heart rate and physical activity, aiding chronic patients, soldiers, and athletes, while secure communication and key management safeguard connected device [3].

Over the past few years, there has been increasing confusion over the definition of what constitutes a medical device, arising from the CDSCO ruling that medical device rule 2017 includes:

"Medical device" means:

Any instruments, apparatus, appliance, material or other article, whether used alone or in combination, including software, intended for use in human or animal for diagnosis, prevention, treatment or alleviation of any disease, injury or disability and also used to support and sustain life.

Or substances used for in vitro diagnosis and surgical dressings, surgical bandages, surgical staples, surgical sutures, ligatures, blood and blood component collection bag with or without anticoagulant

Or The CDSCO Medical Device Rule 2017 defines medical devices broadly, covering instruments, materials, software, and substances for diagnosis, prevention, treatment, and in vitro diagnosis, including surgical supplies and contraceptives [4].

Or New interconnectivity between medical devices and clinical systems offers better patient outcomes but introduces cybersecurity risks. Cybersecurity protects networks and data from unauthorized access and damage, ensuring system safety and integrity [5].

Regulatory framework for Medical Device in India

Table 1: Overview of Medical Device regulations in India

Sr. no.	Title of regulation	Description
1	The Drugs and Cosmetics Act ("D&C Act") 1940	Regulates import, manufacture, distribution & sale of drugs and cosmetics in India to ensure safety, efficacy, and quality. Contains provisions on misbranding, adulteration, licensing of manufacturing/import, and empowers drug inspectors. [1]
2	Information Technology Act and Rules (IT Act) 2000	Provides legal recognition for electronic records and signatures, and defines cybercrimes such as hacking, data theft, and malware. Establishes certifying authorities and cyber appellate tribunals. (Detailed descriptions in IT Act and IT Rules documents.) [6]
3	The Indian medical council (professional, conduct, etiquette, and ethics) regulation 2002	Defines professional standards, ethics, and disciplinary procedures for physicians registered with the Medical Council of India, promoting responsible practice. [7]
4	The Clinical Establishments (Registration and Regulation) Act 2010	Mandates minimum standards, registration, and regulation of public and private health care facilities, including reporting and record maintenance. Enhances quality of care. [8]
5	The Information Technology Reasonable security practices and procedures and sensitive personal data or information Rules ("Data	Specifies security safeguards and procedures to be adopted by entities handling SPDI; includes consent requirements, data breach reporting, and standards for notified bodies. [9]

	Protection Rules") 2011	
6	The Information Technology (Intermediaries Guidelines) Rules ("Intermediary Guidelines") 2011	Requires intermediaries (e.g. platforms) to implement grievance redressal, appoint compliance officers, and follow due diligence to regulate online content. [10]
7	Regulation and description of ("MDR") by CDSCO 2017	Enforces risk-based classification (A to D), import/manufacture licenses, quality benchmarks, testing protocols, and reporting of adverse events under the D&C Act and CDSCO. [11]
8	Digital Personal Data Protection Bill (DPDP Bill) 2022	Establishes framework for processing digital personal data, appointing data fiduciaries, handling consent, data localization, and rights like correction and erasure. [12]
9	e-Health India 2015	(Not a formal law) A strategy outlining India's digital health initiatives like electronic medical records, telehealth integration, standards adoption, and interoperability. [13]
10	Telemedicine Practice Guideline 2020	Clarifies standards for remote clinical consultations, prescription protocols (via video/phone/chat), professional responsibilities, and record-keeping requirements. [14]
11	National Cyber Security Policy 2013	Advises a strategic framework to protect cyberspace—covers critical infrastructure, awareness, R&D, incident response, and public-private cybersecurity partnerships. [15]
12	Digital Health Law and Regulation 2025	Clarify about the digital health, their market size, regulation and requirement. [16]

13	Bureau of Indian standard (BIS) Medical Devices standard (National Medical Device Policy 2023)	Compliance with these standard is already mandatory under the Medical Devices Rule 2017 and failure to adhere may render a device not of standard quality and subject to liability. [17]

Digital technologies in healthcare sector

In today's digital society, national borders have become irrelevant due to cyberspace, enabling businesses across industries to innovate their models by incorporating digital technologies. In healthcare, the primary goal of digital innovation is to optimize medical professionals' work, enhance software systems, improve patient outcomes, lower costs, and minimize human errors [19].

Digital technologies classification

IoT (Internet of Things):

In today's era, Internet has become inevitable in our daily life. Proper and smart use of internet makes our life simple, fast and easy. Amongst the many uses of the internet, one of the important technologies is "IoT (Internet of Things)". So, basically it is to connect the smart "things" or objects to the internet in the easiest and transparent way.

Some of the examples of the IoT are as follows:

1. **Remote Patient Monitoring (RPM):** Wearable devices track vital signs (heart rate, temperature, blood pressure) and send data to doctors, allowing remote observation and fast intervention. *Example:* A 65-year-old heart patient's smartwatch alerts her doctor if her pulse drops suddenly.
2. **Glucose Monitoring:** Automated sensors track blood sugar levels and send alerts when too high or low. *Example:* A teenager with Type 1 diabetes wears a glucose sensor that updates her mom's phone, preventing diabetic episodes.
3. **Heart Rate Monitoring:** Wearable fitness bands and patches continuously track heart activity. *Example:* An athlete recovering from heart condition wears a chest strap that records heart rate and flags irregular rhythms.

4. **Hand Hygiene Monitoring:** Sensors at hospital entrances remind staff and visitors to sanitize hands, reducing infections. *Example:* In a children's hospital, sensors decrease infection rates by prompting proper hygiene.
5. **Mood and Mental Health Monitoring:** Devices estimate mood from physical signs and suggest exercises. *Example:* A smartwatch detects anxiety signs in a college student and suggests breathing exercises.
6. **Parkinson's Disease Monitoring:** Sensors track tremors and movement in real time to guide treatment. *Example:* A senior wears a patch that monitors tremors, allowing doctors to adjust care remotely.
7. **Connected Inhalers:** Smart inhalers remind use, record data, and identify environmental triggers. *Example:* A man with asthma gets alerts for missed inhaler use and pollution-related triggers.
8. **Ingestible Sensors:** Tiny pill-like sensors pass through the digestive tract to collect data painlessly. *Example:* A woman swallows a sensor that sends stomach pH data, aiding ulcer diagnosis without invasive tests.
9. **Smart Contact Lenses:** Track glucose levels in tears or eye pressure and may interface with digital content. *Example:* A diabetic patient's contact lenses alert her via smartphone when glucose spikes [18,19,20].

IoMT (Internet of Medical Things)

The **Internet of Medical Things (IoMT)** has enhanced patient care by connecting medical devices, applications, and healthcare systems to the internet, enabling secure data transfer and reducing unnecessary hospital visits. However, IoMT also increases vulnerabilities in data management, raising concerns over privacy and data security.

Examples of Digital Technologies in Healthcare:

- **Wearable Devices:** Devices like smartwatches, fitness trackers, and smart clothing monitor heart rate, blood pressure, sleep patterns, and physical activity in real time. Example: A wearable device alerts healthcare providers if a patient's blood pressure exceeds normal limits.
- **Smart Medical Devices:** Purpose-built devices monitor vital signs such as glucose, oxygen levels, and body temperature, and communicate directly with healthcare professionals. Example: A smart insulin pump adjusts insulin delivery based on glucose readings, preventing hypo- or hyperglycemia.

- **Telemedicine Devices:** These include video conferencing tools, remote monitoring systems, and mobile health apps, allowing patients to consult doctors remotely, improving healthcare access in rural areas. Example: Patients use video calls to consult physicians without traveling to clinics.
- **Smart Home Devices:** Integrated into homes to enhance comfort and security, they also monitor patient health and notify providers about abnormalities. Example: A smart bed tracks sleep patterns and sends alerts if deviations suggest potential health problems [19,21]. (Figure 1)

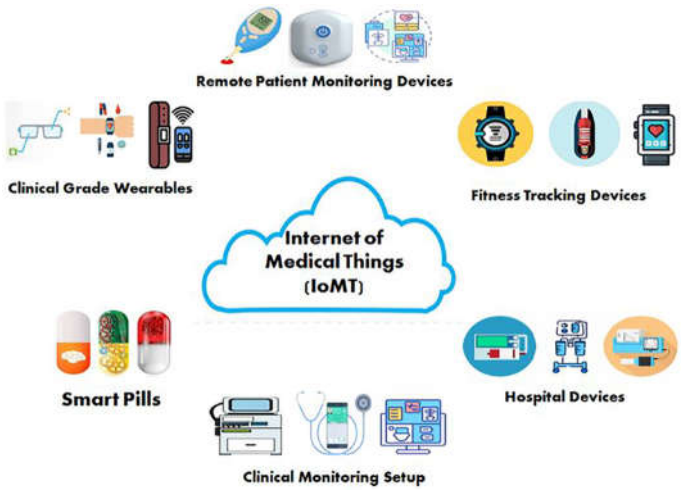

Figure 1: example of IoMT Medical Device [22]

From Scans to Scams: Mapping the Cybersecurity Landscape of Medical Device in India

In India, the vast scale and complexity of the healthcare ecosystem—combined with fragmented and legacy IT infrastructures—pose significant challenges to implementing effective cybersecurity measures. The success of digital transformation hinges not only on technological adoption but also on healthcare professionals' willingness to acknowledge and address cybersecurity risks.

Patients expect both quality care and data protection. Enforcing basic security measures and proactive strategies at institutional and individual levels is essential to mitigate threats [23].

Types of Cyberattacks in Healthcare

Healthcare organizations commonly face three main cyberattacks:

1. **Infrastructure Exploitation Attacks:** Exploit system vulnerabilities (misconfigured networks, software bugs) using DoS, DDoS, MITM, eavesdropping, SQL exploits, privilege escalation, and cryptographic attacks.
2. **Ransomware Attacks:** Attackers encrypt critical data and demand ransom, exploiting the sensitivity of healthcare data.
3. **Human Exploitation Attacks:** Manipulating individuals through phishing and social engineering to gain unauthorized access [24,25].

Various mode of attacks in healthcare

1. **Vulnerable Software:** Outdated systems like RDP and SMB are malware targets, with over 1,500 unique payloads infiltrating Indian networks [24].
2. **Social Engineering Attacks:** Exploiting personal data shared on social media to target healthcare professionals [25,26].
3. **Phishing Attacks:** Deceptive emails or messages impersonate trusted sources to steal credentials or install malware [26,27].
4. **Ransomware Attacks:** Hospital data is encrypted until ransom is paid, disrupting operations and patient care [27].
5. **SQL Injection (SQLi):** Attackers inject malicious queries to access and manipulate sensitive records [25].

Notable Cybersecurity Incidents in Indian Healthcare

Cybersecurity is the practice of safeguarding the computer systems, its network and data from cyberattacks, theft and damage. The healthcare sector is increasingly targeted by cybercriminals, with 60% of organizations globally experiencing attacks in 2022 to 2025. [28]

I. **AIIMS Delhi Ransomware Attack – November 2022:** A phishing email encrypted 1.3 TB of data, affecting over 3–4 crore patient records. Critical services went offline for two weeks, with hackers demanding ₹200 crore. Authorities responded by deploying antivirus solutions, network isolation, and strengthening backups [29].

II. **KD Hospital Ransomware – Ahmedabad, May 2023:** Ransomware rendered hospital data inaccessible, demanding $70,000 in Bitcoin. Core medical services continued offline. The malware was present since March 2023 , showing monitoring gaps [30].

III. **Apollo Hospitals Phishing Attack – October 2024:** KillSec group used a malware-laced document to threaten data leaks. Experts recommended email filtering, employee training, and AI-based threat detection [31].

IV. **Star Health Insurance Breach – Sept–Oct 2024:** Records of over 31 million policyholders were exposed and offered for sale. Legal actions followed. The breach highlighted the need for stronger access controls and timely disclosure [32].

V. **Sant Parmanand & NKS Hospital Hack – June 2025:** Targeted attack disrupted systems, forcing manual operations. FIR was filed under the IT Act, and cybersecurity experts began investigation [33].

Medical Device Security Mechanisms

Healthcare devices are implanted and connected to patients' bodies to collect sensitive health data, which is sent to experts and labs for analysis. Manufacturers prioritize low-cost, low-power designs, often avoiding additional safety mechanisms that could increase complexity and production costs [25]. The security mechanism is shown in the figure 2. For example, when making on-site medical devices such as X-ray, MRI, and Ultrasound, etc., keeping the device secure and protecting it from hackers is not the priority of the developers.

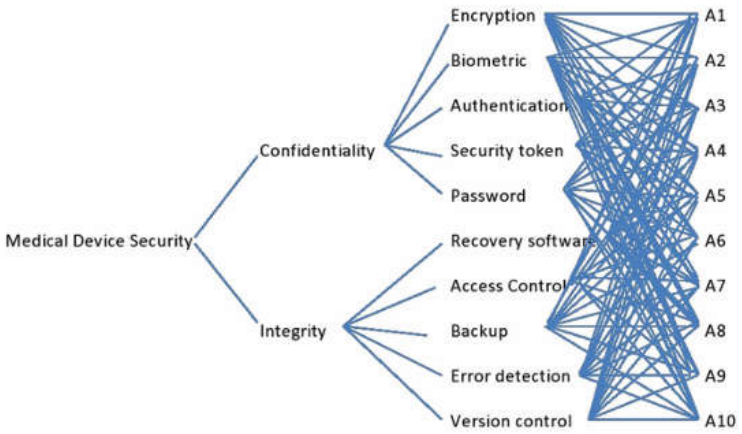

Figure 2: Medical device security method [34]

i. **Encryption:** Encryption converts plain characters into coded form using algorithms, ensuring message secrecy. It protects data from unauthorized access during transmission.

ii. **Biometrics:** Biometrics uses physical or behavioral traits (fingerprints, facial recognition) to identify individuals digitally. It enables secure access to devices and systems.

iii. **Authentication:** Authentication verifies the identity of a person or system, typically using a username and password. Correct credentials grant access to the system.

iv. **Recovery:** Data recovery software restores lost data after accidental deletion, formatting errors, or system crashes. It helps maintain data integrity.

v. **Access Control:** Access control ensures that individuals are who they claim to be. It restricts access to personal and sensitive information.

vi. **Backup:** Backup is a stored copy of data used to recover originals during data loss events. It safeguards important information from accidental loss.

vii. **Error Detection:** Error detection identifies errors in data transmitted between devices using redundancy codes. It ensures the accuracy of transmitted information [34].

Different way to protect the medical device

As healthcare facilities increase endpoint devices, the attack surface expands, giving cybercriminals more opportunities to target medical equipment like infusion pumps and cardiac monitors. Securing these devices is challenging, so alternative strategies are recommended [35].

- **Vendor's Recommendation:** Follow manufacturer guidelines to safeguard medical equipment.
- **Maintain Device Health:** Regularly update software, enable encryption, and track assets to meet HIPAA standards.
- **Segment the Network:** Isolate medical devices using VLANs or dedicated service identifiers to protect against external threats.
- **Use AI for Threat Detection:** Tools like IBM QRadar and Suricata use AI and machine learning to detect abnormal network activity early, preventing breaches.
- **Track System Faults and Notifications:** Adaptive security platforms analyze network and endpoint traffic for signs of attack [36].

Cybersecurity Regulatory Standards:

Standards like ISO/IEC 15408, ISO 14971, UL 2900, and IEC 62304 guide risk management and security protocols in medical technology. The IMDRF promotes global harmonization of

cybersecurity regulations, while IEC emphasizes IEC 62304 as essential for medical software security [37].

Artificial Intelligence in Healthcare and Cybersecurity

AI (Artificial Intelligence)-integrated medical devices are transforming healthcare but also increasing cybersecurity risks, potentially endangering patient safety. For example, a hacked AI-powered insulin pump could malfunction, causing serious harm [38].

In India, AI is advancing diagnostics, drug discovery, and patient care, with a growing number of startups and collaborations between healthcare providers, tech firms, and government initiatives. Programs like National Health Stack, Ayushman Bharat, and Pradhan Mantri Jan Arogya Yojana support AI-driven healthcare innovation [39].

Artificial intelligence:

AI enables systems to reason, learn, and operate independently, covering areas like machine learning, natural language processing, computer vision, and robotics.AI can be broadly classified into two types:

1. **Narrow AI** – Designed for specific tasks, like image recognition or playing chess.
2. **Generative AI** – Has wider capabilities, adapting to various scenarios, and performing diverse tasks like a human [40].

Trends in Medical Devices with AI

Technological progress is driving the evolution of medical devices powered by AI, primarily across three domains:

- **Chronic Disease Management:** Wearable sensors monitor vitals and dispense treatments (e.g., insulin for diabetes patients).
- **Medical Imaging:** AI enhances image quality and diagnostic accuracy while reducing radiation exposure.
- **IoT Integration:** Smart medical devices collect and share data in real time, improving communication, reducing costs, and enhancing patient care when combined with AI [41].

Application of AI in Cybersecurity

AI also plays a critical role in cybersecurity within healthcare by enhancing the following areas:

- Threat detection and prediction
- Incident response and automation

- Vulnerability management
- Network security
- Protection of electronic health records
- Remote monitoring
- Bioinformatics [39,40]

Role of AI in Healthcare

Global healthcare has improved life expectancy, but ageing populations are driving higher demand, costs, and workforce shortages. By 2050, one in four people in Europe and North America will be over 65, increasing the need for chronic care. Training more professionals is essential, but AI and automation can also optimize efficiency and allow staff to focus on patient care [42].

AI, defined by the European Parliament as systems performing tasks requiring human intelligence, enhances outcomes, operations, and workflows by reducing administrative burdens and accelerating innovations. However, ethical and regulatory issues such as data use, fairness, and accountability remain critical challenges [43].

Future AIin the Medical Device Industry

The integration of AI in medical devices is growing to enhance precision, automation, and reliability, especially for chronic disease management. While AI in medical imaging is widespread, wearable AI medical devices are still developing. By 2030, the industry aims to shift from traditional tools to intelligent AI-driven systems, supported by global regulatory standards from ISO, IEC, and IEEE to ensure ethical, safe deployment.

Key trends include integrating AI with virtual reality (VR) for real-time adaptive feedback and repurposing non-medical AI devices (e.g., biometric payment tools) for healthcare due to faster development cycles.

To ensure safety and performance, close cooperation between regulators, clinicians, and manufacturers is critical. Companies like BioT lead by offering compliant, secure cloud solutions that facilitate AI-powered device development, focusing on data protection, user-friendly platforms, and flexible designs to meet global regulatory requirements [44].

REFERENCES:

1. Basic introduction about Digitalized medical care iclg.com/practice-areas/digital-health-laws-and-regulations/india
2. Rishabh Kumar Rana, Neelesh Kapoor, Dewesh Kumar, Madhur Verma, Gunjan Taneja, "Digital Health Revolution in India: Transforming Health and Medicine." *Indian Journal of Community Medicine.* **2024,** 49(8), 205-209.
3. Priya Vij, Patil Manisha Prashant, "Cybersecurity and Compliance in Healthcare: A Study on Key Management and Other Regulatory Requirements." *South Eastern European Journal of Public Health (SEEJPH),* **2024,** 23,76-80.
4. Central Drugs Standard Control Organization (CDSCO), Ministry of Health and Family Welfare, Govt. of India, 2017.
5. Patricia AH williams Andrew J woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem." *Medical Devices: Evidence and Research,* **2015,** 8, 305-316.
6. Cybersecurity Law and Policy - Present Scenario and the Way Forward, Nishith Desai Associates, 2023. DMS Code: 21821.1.
7. Dipika Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges." *Healthcare,* **2023,** 11, 911.
8. Recent regulation of the medical device in India lexorbis.com/digital-health-laws-and-regulations-india-2025/?utm_source=chatgpt.com
9. Regulation and description of Data Protection Rules 2011 indiacode.nic.in/handle/123456789/1362/simple.search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules
10. Regulation and description of intermediate guidelines dispur.nic.in/itact/it-intermediaries-guidelines-rules-2011.pdf
11. Regulation and description of the medical device rule by CDSCO 2017 cdsco.gov.in/opencms/resources/UploadCDSCOWeb/2022/m_device/Medical%20Devices%20Rules,%202017.pdf
12. Regulation and description of the digital personal data protection bill prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022
13. Regulation and description relate to e-Health mohfw.gov.in/?q=en/Organisation/departments-health-and-family-welfare/e-Health-Telemedicine
14. Regulation and description relate to telemedicine esanjeevani.mohfw.gov.in/assets/guidelines/Telemedicine_Practice_Guidelines.pdf
15. Regulation and description of national cyber security policy meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf
16. Regulation and description relate digital health law and regulation policy iclg.com/practice-areas/digital-health-laws-and-regulations/india/amp

17. Regulation and description Bureau of Indian standard (BIS) Medical Devices standard pharma.dept.gov.in/sites/default/files/Strategy%20Document%20on%20NMDP%202023_0.pdf
18. Various IoT different technologies used in the healthcare sector ordr.net/article/iot-healthcare-examples
19. Metty Paula, Leandros Maglaras, Mohamed Amine Ferragd, Iman Almomanic, "Digitization of health care sector: A study on privacy and security concerns." *ICT,* **2023,** 9, 571-588.
20. Akshay Parihara, Jigna B. Prajapatib, Bhupendra G. Prajapatic, Binti Trambadiyad, Arti Thakkare, Pinalkumar Engineerf, "Role of IOT in healthcare: Applications, security & privacy concerns." *Intelligent Pharmacy,* **2024,** 2, 707-714.
21. Study Paper on "Security and Privacy in the Internet of Things (IoMT)", Smart Network Division, TEC, Department of Telecommunication, Government of India. From ISO 9001:2015.
22. Attiya Khan, Muhummad Rizwan, Ovidiu Bagdasar, Abdulatif Alabdulatif, Sulaiman Alamro, Abdullah Alnajim, "Deep learning – driven anomaly detective for IoMT based smart healthcare system." *Computer Modelling in Enginnering & Science,* **2024,** 141(3), 2121-2141.
23. Dr. Parvathi Balaji, Dr. Divya Raghunathan, Dr. Aravinth. V, Dr.Shyam Sivasamy, Swetha.V, Dr. Preetha Elizabeth chaly, "Cyber Attack - Envenom in Indian Healthcare - A Review." *International Journal of Research Publication and Reviews,* **2023,** 4(6), 1262-1266.
24. Faddis A., "The Digital Transformation of Healthcare Technology Management." *Biomedical Instrumentation & Technology,* **2018,** 52(2), 34–38.
25. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic." *Computers & Security,* **2021,** 105(1), 1–20.
26. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S., "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review." *Sensors,* **2021,** 21(15), 5119.
27. Niki, O., Saira, G., Arvind, S., & Mike, D. 2022. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. DIGITAL HEALTH, 8, 205520762211046.
28. Dr. Anjali Dixit, Mrs. V. B. Malleswari, V Sai Medha, "A Critical Study on Enhancing Cybersecurity in India's Healthcare Sector." *Library Progress International,* **2024,** 44(4), 193-208.
29. AIIMS Delhi Ransomware Attack – November 2022 thehindu.com/news/national/13-tb-data-encrypted-in-ransomware-attack-on-aiims-by-unknown-threat-actors-centre/article66271226.ece
30. KD Hospital Ransomware – Ahmedabad, may 2023 indianexpress.com/article/cities/ahmedabad/hospital-falls-prey-to-ransomware-attack-hackers-demand-70000-8613410/

31. Apollo Hospital Phishing attack – October 2024 newindianexpress.com/magazine/2025/Feb/16/hacked-and-helpless
32. Star health insurance breach- September 2024 reddit.com/r/india/comments/1ggylmh/iffs_cybersecurity_report_for_the_third_quarter/
33. Sant Parmanand & NKS Hospital Hack – June 2025 timesofindia.indiatimes.com/city/delhi/servers-of-two-city-hospitals-hacked-police-register-fir/articleshow/121836219.cms
34. Masood Ahmad, Jehad F. Al-Amri, Ahmad F. Subahi, Sabita Khatri, Adil Hussain Seh1, Mohd Nadeem1 and Alka Agrawal, "Healthcare Device Security Assessment through Computational Methodology." *Computer Systems Science & Engineering,* **2022,** 41(2) 811-828.
35. K. Venkateswara Raju, Ayesha Siddiki, Lakshmi Prasanthi Nori, "Cyber awareness of connected medical devices and article their regulatory aspects." *Pharma Times,* **2023,** 55(8), 13-23.
36. 5 ways to properly secure medical devices; 2019. techtarget.com/searchhealthit/tip/5-ways-to-properly-secure-medical-device
37. Cybellum; Intro to Medical Device Standards and Regulations; August 4, 2022. Intro to Medical Device Standards and Regulations | Cybellum
38. Barry Solaiman & I. Glenn Cohen, Research Handbook on Health, AI and the Law, "Title: Cybersecurity of AI medical devices: risks, legislation, and challenges." 2023.
39. Artificial Intelligence in Healthcare - Navigating Regulatory Frontiers in India, Nishith Desai Associates, 2025. DMS Code: 119795.2.
40. Prof. S. B. Bele, Sanskruti R. Gourkhede, Purva V. Bonde, Prajkta P. Papalkar, "The Role of Artificial Intelligence in Cyber Security." *International Research Journal of Innovations in Engineering and Technology (IRJIET),* **2024,** 8(10), 221-224.
41. Trends in Medical Devices with Artificial Intelligence vantagemedtech.com/the-use-of-artificial-intelligence-in-medical-devices/ [last assessed on 1 August 2025.]
42. Google find this Shakeel, T.; Habib, S.; Boulila, W.; Koubaa, A.; Javed, A.R.; Rizwan, M.; Gadekallu, T.R.; Sufiyan, M., "A survey on COVID-19 impact in the healthcare domain: Worldwide market implementation, applications, security and privacy issues, challenges and future prospects." *Complex Intell Syst,* **2022,** 9, 1027–1058.
43. Dr. E. Nafeza, Ms. M.R. Iswarya, "Role of AI in Healthcare. A Conceptual Study on Its Cyber Safety and Security in India." *International Journal of Innovative Research in Technology,* **2024,** 10(10), 257-261.
44. Future of Artificial intelligence in the medical device industry biot-med.com/resources/the-role-of-artificial-intelligence-in-modern-medical-devices