
RANSOMWARE ATTACKS ON HOSPITALS: A COMPARATIVE ANALYSIS OF GLOBAL CYBERSECURITY LAWS

Evania Irene K, LLM (Cyber Law), The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

Ransomware attacks have emerged as one of the most significant cybersecurity threats to the global healthcare sector, disrupting essential medical services, compromising sensitive patient data, and endangering patient safety. Hospitals have become prime targets due to their reliance on digital health systems, electronic health records, interconnected medical devices, and the urgent nature of healthcare delivery, making them more susceptible to extortion. High profile incidents such as the WannaCry attack on the United Kingdom's National Health Service, the cyberattack on Ireland's Health Service Executive, and ransomware attacks on healthcare institutions in several countries demonstrate the far reaching legal, operational, and public health consequences of such attacks. Despite the increasing frequency and sophistication of ransomware, legal and regulatory responses remain fragmented across jurisdictions, creating challenges in cybercrime investigation, cross border cooperation, data protection, liability, and critical infrastructure security. This paper undertakes a comparative analysis of global cybersecurity laws governing ransomware attacks on hospitals by examining international legal instruments and selected national regulatory frameworks. It evaluates the effectiveness of existing legal measures in preventing, responding to, and mitigating ransomware attacks while identifying common regulatory gaps and enforcement challenges. The paper argues that protecting hospitals from ransomware requires more than technical cybersecurity measures; it demands a comprehensive legal framework that strengthens cybersecurity governance, mandates incident reporting, safeguards patient data, promotes international cooperation, and clearly allocates institutional accountability. It concludes that a harmonised and resilient legal approach is essential to protect healthcare infrastructure, ensure continuity of medical services, and strengthen public trust in an increasingly digital healthcare environment.

Keywords: Ransomware, Hospitals, Critical Infrastructure, Cyber Crime, Healthcare Cybersecurity

Introduction

The rapid digitalisation of healthcare has transformed the delivery of medical services through electronic health records, telemedicine, cloud computing, connected medical devices, and Artificial Intelligence (AI). The efficiency and accessibility of healthcare have been greatly enhanced by these technological developments, but they have also made the industry more susceptible to cyberthreats, especially ransomware attacks. Malicious software known as ransomware encrypts an organisation's data and requests money to decrypt it. Such attacks have the potential to seriously jeopardise patient safety, interfere with vital medical services, postpone emergency care, and compromise private patient data.

Due to their reliance on digital infrastructure and inability to afford extended system outages, hospitals have emerged as one of the most attractive targets for ransomware attackers. The serious operational, financial, and legal consequences of such attacks can be seen by high-profile incidents like the WannaCry attack on the National Health Service (NHS) in the United Kingdom, the cyberattack on the Health Service Executive (HSE) in Ireland, and the ransomware attack on the All India Institute of Medical Sciences (AIIMS), New Delhi. These cases have demonstrated that ransomware is now a serious legal and public policy matter that affects vital healthcare infrastructure, rather than just a cybersecurity issue.

Although several countries have strengthened their cybersecurity and data protection laws, the legal response to ransomware remains fragmented. Challenges relating to jurisdiction, cross-border cybercrime, attribution of attacks, liability, mandatory breach reporting, and protection of patient data continue to hinder effective enforcement and international cooperation. In light of this, this study compares international cybersecurity regulations pertaining to hospital ransomware attacks. It looks at current domestic and international legal frameworks, highlights important regulatory issues, and assesses best practices used in various jurisdictions. The paper makes the case that a coordinated legal and regulatory framework that promotes cybersecurity resilience, protects patient data, fortifies institutional accountability, and strengthens international cooperation against evolving cyber threats is necessary to protect healthcare institutions from ransomware.

Understanding Ransomware in Healthcare

A type of malicious software known as ransomware encrypts a victim's data or prevents access

to computer systems until a ransom is paid. Double extortion is a common tactic used in modern ransomware attacks, in which the attackers encrypt data, take confidential information, then threaten to disclose it until payment is received. Because hospitals rely so significantly on continuous access to digital systems for patient care, ransomware is a major danger in the healthcare industry¹.

Hospitals reliance on electronic health records (EHRs), interconnected medical devices, cloudbased systems, and time-sensitive healthcare services makes them appealing targets for ransomware attackers. Healthcare organisations are more likely to pay the ransom in order to promptly resume operations if these systems are disrupted, as this could cause delays in diagnostics, surgeries, emergency care, and other vital medical services. Hospitals are more appealing to cybercriminals due to the number of sensitive patient data they store².

Beyond just monetary losses, ransomware attacks have far reaching effects. They have a direct impact on patient safety and continuity of treatment by interfering with hospital operations, delaying medical procedures, and limiting access to crucial patient records. Additionally, these attacks reveal private health information, which can result in identity theft, data breaches, and privacy violations. Furthermore, the public's confidence in digital healthcare systems may be damaged, and healthcare organisations frequently have to pay high fees for cybersecurity enhancements, legal compliance, and system recovery.

Major Global Ransomware Incidents

The vulnerability of healthcare institutions around the world has been revealed by a number of ransomware attacks, underscoring the pressing need for stricter cybersecurity regulations. The 2017 WannaCry ransomware outbreak seriously damaged the National Health Service (NHS) in the United Kingdom and impacted over 150 countries. Thousands of surgeries and appointments were canceled, emergency patients were diverted, and access to electronic health records was momentarily lost as a result of the impact on over 80 NHS trusts. The event illustrated how patient safety and the continuation of vital healthcare services might be directly threatened by hackers.

¹ NIH, <https://pmc.ncbi.nlm.nih.gov/articles/PMC13141016/>, (last visited Aug 28, 2026)

² IBM, <https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities>, (last visited Sep. 01, 2026).

One of the most severe ransomware attacks against a public healthcare system occurred in 2021 against Ireland's Health Service Executive (HSE). The attack caused the nation's IT systems to shut down, interfered with laboratory and diagnostic services, postponed doctor's appointments, and had a major impact on patient care nationwide. The HSE suffered significant financial losses during system recovery and repair while refusing to pay the ransom.

In 2022, a significant ransomware attack occurred at the All India Institute of Medical Sciences (AIIMS) in New Delhi, India, causing many days of disruption to hospital operations. Staff were forced to rely on manual procedures since access to electronic patient information, appointment scheduling, laboratory testing, and invoicing functions was compromised. The attack exposed India's digital healthcare infrastructure's cybersecurity flaws and emphasised the need for more robust institutional, legal, and regulatory safeguards to shield hospitals from emerging cyberthreats³.

In June 2026, a major private hospital in Ernakulam, Kerala, suffered one of India's most significant healthcare cyber incidents when the ransomware group "The Gentlemen" allegedly stole nearly 800 GB of sensitive hospital data. The compromised information reportedly included patient medical records, admission and treatment details, administrative documents, financial records, and internal committee meeting minutes. The attackers later listed the stolen data for sale on the dark web, raising serious concerns regarding patient privacy and healthcare cybersecurity.

According to reports, the attack began through a ransomware email, after which the attackers infiltrated the hospital's network and exfiltrated large volumes of confidential information. Initially, the hospital believed that no critical data had been compromised and therefore focused on restoring its systems with the assistance of an external cybersecurity firm. However, subsequent forensic log analysis confirmed the theft of approximately 800 GB of data. Despite the scale of the breach, the hospital reportedly did not immediately file a police complaint, drawing criticism from cybersecurity experts and highlighting the importance of timely incident reporting and compliance with cybersecurity regulations⁴.

³ HEALTHVOICE, <https://healthvoice.in/the-rise-of-ransomware-in-healthcare-critical-lessons-for-hospital-leaders-inindia>, (last visited Sep 30, 2026)

⁴ Shan A.S, *Hackers target Ernakulam hospital, steal 800GB data*, THE NEW INDIAN EXPRESS, (June 10, 2026, 08:53 AM) *Hackers target Ernakulam hospital, steal 800GB data*

This incident demonstrates that ransomware attacks on healthcare institutions have evolved beyond encrypting systems to double extortion attacks, where cybercriminals steal sensitive data before demanding ransom. Even if hospitals restore their operations from backups, the exposure of confidential patient information can result in long-term privacy violations, reputational damage, regulatory consequences, and loss of public trust. The Ernakulam hospital attack underscores the urgent need for stronger cybersecurity governance, continuous network monitoring, employee awareness against phishing attacks, and effective incident response mechanisms within the healthcare sector.

Comparative Analysis of Global Cybersecurity Laws

Countries and international organisations have strengthened their cybersecurity and data protection regimes in response to the growing frequency and sophistication of ransomware attacks on hospitals. While different countries use different strategies, most aim to strengthen resilience against cyber threats, preserve vital healthcare infrastructure, and protect patient data. In order to find common practices, regulatory variations, and lessons for enhancing healthcare cybersecurity, this part looks at the major international legal instruments and contrasts the cybersecurity legislation of a few chosen jurisdictions⁵.

International Legal Framework

Countries and international organisations have developed legislative and regulatory frameworks to boost cybersecurity and safeguard vital healthcare infrastructure in response to the growing frequency and sophistication of ransomware attacks on healthcare facilities. Although the scope and execution of these frameworks vary, they all share a common goal of preventing cyber attacks, protecting sensitive health data, guaranteeing prompt incident reporting, and fostering international cooperation. The main worldwide legal frameworks controlling healthcare cybersecurity are examined in the part that follows, along with how they handle ransomware assaults.

Budapest Convention

The first international agreement to exclusively address cybercrime is the Budapest Convention

⁵ Nasar Mohammed, Abdul Faisal Mohammed, Sruthi Balammagary, *Ransomware in Healthcare: Reducing Threats to Patient Care*, 1, JCCCI, 27, 31 - 32, (2025)

on Cybercrime (2001). It aims to improve international cooperation among law enforcement agencies, preserve electronic evidence, expedite cross-border investigations, and harmonise national cybercrime legislation. Although it does not specifically regulate ransomware attacks on hospitals, its provisions on illegal access, data interference, and system interference provide the legal basis for prosecuting ransomware offences. The Convention has become the global benchmark for international cooperation in combating cybercrime.

World Health Organisation

Cybersecurity is acknowledged by the World Health Organisation (WHO) as a crucial element of digital health. WHO encourages member nations to improve cybersecurity governance, safeguard health information, advance secure digital health systems, and increase resilience against cyber attacks through its Global Strategy on Digital Health 2020–2025. Additionally, WHO emphasises how important cybersecurity is to preserving patient safety and upholding confidence in digital healthcare.

European Union

One of the most extensive legal frameworks for cybersecurity in healthcare has been adopted by the European Union. Healthcare is categorised as an essential industry under the NIS2 Directive, which also mandates that hospitals and healthcare providers establish business continuity plans, report severe cyber events, and apply risk management strategies. By implementing stringent requirements for data processing, security, breach reporting, and accountability, the General Data Protection Regulation (GDPR) significantly protects patients' personal and health data. When taken as a whole, these regulations provide a proactive framework that guarantees robust data protection while preventing cyberattacks.

United States

The United States follows a sector-specific approach to healthcare cybersecurity. The Health Insurance Portability and Accountability Act (HIPAA)⁶ establishes national standards for protecting electronic health information and requires healthcare organisations to implement administrative, technical, and physical safeguards. The HITECH Act⁷ strengthens these

⁶ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

⁷ Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, tit. XIII, 123 Stat. 226 (2009).

obligations by promoting electronic health records and introducing mandatory breach notification requirements. In addition, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCI⁸) requires critical infrastructure entities to report significant cyber incidents, thereby improving national cyber resilience.

Additionally, the US has taken a proactive stance against ransomware by discouraging ransom payments and strengthening cyber incident reporting. Policymakers have actively discussed the adoption of a nationwide payment ban to reduce the financial incentives for cybercriminals, even though there isn't already a federal legislation that forbids victims from paying ransomware demands. While acknowledging that an immediate prohibition would discourage victims from reporting attacks and force payments underground, the Biden Administration has investigated the prospect of limiting ransom payments through the International Counter Ransomware Initiative (CRI). As a result, rather than criminalising victims, the present approach concentrates on enhancing cyber resilience⁹.

In addition, the United States has strengthened its regulatory framework through the Cyber Incident Reporting for Critical Infrastructure Act (CIRCI⁸), which requires critical infrastructure entities to report significant cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA) within prescribed timelines. The Office of Foreign Assets Control (OFAC) further discourages ransom payments by warning that payments made to sanctioned individuals or organisations may violate U.S. sanctions laws and attract civil penalties. At the state level, jurisdictions such as North Carolina and Florida have enacted legislation prohibiting state agencies from paying ransomware demands. To effectively tackle ransomware attacks, the United States continues to prioritise required reporting, cybersecurity readiness, public-private partnership, and international cooperation rather than depending only on payment prohibitions¹⁰.

United Kingdom

The Computer Misuse Act 1990¹¹, which makes unauthorised access to computer systems

⁸ Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, div. Y, tit. II, 136 Stat. 1038 (2022).

⁹ International Counter Ransomware Initiative (CRI), *Joint Statement of the Counter Ransomware Initiative* (2023), <https://www.state.gov/counter-ransomware-initiative/> (last visited Sept. 11, 2026).

¹⁰ Fabian Teichmann, *International legal responses to ransomware: toward a ban on payments?*, ICLR, 32, 44 - 46, (2026)

¹¹ Computer Misuse Act 1990, c. 18 (U.K.).

illegal, and the Network and Information Systems (NIS) Regulations 2018, which mandate that operators of essential services, including healthcare providers, put in place suitable cybersecurity measures and report major cyber incidents, are two ways that the United Kingdom regulates healthcare cybersecurity. The Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), which offer strong protections for personal and health data, supplement these legislation. The National Cyber Security Center (NCSC) provides cybersecurity advice, threat information, and incident response support to the National Health Service (NHS).

The UK greatly improved its cybersecurity strategy for the healthcare industry after the 2017 WannaCry ransomware attack by treating cyber risk as a national security and patient safety concern rather than just an information technology problem. The Cyber Strategy for Health and Social Care 2023–2030 was unveiled by the Department of Health and Social Care. It focuses on enhancing cyber resilience through improved incident response capabilities, stronger governance, secure digital transformation, and increased collaboration throughout the healthcare system. In order to reduce the impact of ransomware attacks on vital healthcare services, recent policy recommendations have further emphasised that cybersecurity should be treated as an organisational business resilience risk, supported by stronger board-level accountability, consistent implementation of cybersecurity standards, centralised oversight, and improved governance across NHS Trusts¹².

Singapore

The Cybersecurity Act 2018¹³, which governs Critical Information Infrastructure (CII), including healthcare facilities, has given Singapore a strong cybersecurity framework. Critical system operators are required to conduct audits, put cybersecurity measures in place, and notify the Cyber Security Agency of Singapore (CSA) of any cyber events. In order to avoid unauthorised access and data breaches, the Personal Data Protection Act (PDPA)¹⁴ mandates that organisations use adequate security measures.

¹² Monica Kello, Steve Hill, Zofia Hill, Tim Stevens, *Building NHS Resilience to Ransomware: Central Oversight and Shared Capability*, CSRG, 1, 9 - 17, (2026) <https://www.kcl.ac.uk/warstudies/assets/building-nhs-resilience-to-ransomware.pdf>

¹³ Cybersecurity Act 2018 (No. 9 of 2018) (Sing.).

¹⁴ Personal Data Protection Act 2012 (No. 26 of 2012) (Sing.).

By providing comprehensive incident response guidelines via the CSA, Singapore has also taken a proactive stance in responding to ransomware. Organisations are encouraged to isolate affected systems right away, get rid of malware, restore operations using safe backups, and keep an eye out for suspicious activity on networks. Although paying a ransom is not legally forbidden, the government strongly advises against doing so since it does not ensure data recovery and could incite other attacks. Organisations must notify the police, the Singapore Computer Emergency Response Team (SingCERT) under the CSA, and the Personal Data Protection Commission (PDPC) in the event of a ransomware attack if there has been a notifiable breach of personal data¹⁵.

India

The Information Technology Act of 2000¹⁶, the Digital Personal Data Protection Act of 2023¹⁷, and the CERT-In Directions of 2022 make up the majority of India's healthcare cybersecurity architecture. These regulations mandate that organisations secure personal data, put adequate security measures in place, and report specific cyber events within the allotted time frames¹⁸. While the Digital Personal Data Protection Act strengthens the protection of personal data by requiring data fiduciaries to ensure the security of digital personal information, the Information Technology Act also criminalises offences like unauthorised access, data theft, and damage to computer systems.

In addition to the statutory framework, CERT - In has issued mandatory directions requiring entities to report cybersecurity incidents, maintain system logs, and coordinate with the national incident response agency to facilitate timely investigation and mitigation. However, unlike several other jurisdictions, India does not have a dedicated legal framework or sector specific cybersecurity standards exclusively addressing ransomware attacks on hospitals and healthcare institutions. Although ransomware attacks may attract liability under various provisions of the Information Technology Act and the Bharatiya Nyaya Sanhita, 2023, the absence of healthcare specific cybersecurity legislation creates significant regulatory gaps in protecting critical health infrastructure. As India's healthcare sector continues to undergo rapid digital transformation,

¹⁵ Chia Boon Teck, Khor Zhen Yan, *Don't be Held at Ransom by Ransomware*, LAW GAZETTE, (Sep 2022) <https://lawgazette.com.sg/practice/practice-matters/dont-be-held-at-ransom-by-ransomware/>

¹⁶ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

¹⁷ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁸ Niharika Raizada, Pranjali Srivastava, *Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India*, 11, KLR, 453, 468, (2024)

there is an increasing need for comprehensive legislation that strengthens cybersecurity governance, enhances incident response mechanisms, safeguards critical healthcare infrastructure, and improves resilience against ransomware attacks¹⁹.

Similarities and Differences in Legal Approaches

Healthcare is becoming more widely acknowledged as a key infrastructure that needs robust cybersecurity protection across all jurisdictions. The majority of legal frameworks place a strong emphasis on cybersecurity duties, risk management, patient data protection, and incident reporting. However, the United States depends on privacy laws related to the healthcare industry, whereas the European Union, the United Kingdom, and Singapore use more broad and proactive regulatory regimes with sector-specific duties. India does not yet have a specific regulatory framework for ransomware attacks on healthcare facilities and instead relies heavily on general cybersecurity and data protection legislation²⁰. These variations show that in order to successfully combat the expanding worldwide danger of ransomware, there is a need for more international collaboration and harmonised legal norms.

Legal and Regulatory Challenges

Attribution and Jurisdiction

One of the greatest challenges in combating ransomware attacks is identifying the perpetrators and determining the appropriate jurisdiction for prosecution. Cybercriminals tend to operate internationally, hiding their identities with cryptocurrencies and anonymous networks. This makes it challenging to conduct investigations, gather evidence, and extradite people, especially in situations where nations lack mutual legal aid agreements or have disparate cybercrime laws.

Protection of Health Data and Patient Privacy

Sensitive health information, such as electronic health records, diagnostic reports, and personal identity information, is regularly compromised by ransomware attacks. Identity theft, financial fraud, and grave patient privacy violations may arise from the theft and publication of such

¹⁹ ARENESS, <https://arenesslaw.com/ransomware-the-most-dangerous-cyber-threat/> (last visited Oct 05, 2026)

²⁰ Nidhi Kamath, Pratik Amit Oke, *Ransomware Threats In India's Healthcare Sector: Assessing The Need For Dedicated Legislation*, 3, LLJ, 44, 49 - 56, (2024)

information. As healthcare organisations continue to digitise their services, guaranteeing the security of health data continues to be a major concern, despite the fact that many jurisdictions have passed data protection regulations.

Liability of Hospitals and Third - Party Vendors

After a ransomware attack, determining liability is frequently difficult. In order to safeguard patient information and guaranty the continuation of medical services, hospitals are required to put in place appropriate cybersecurity safeguards. To manage digital infrastructure, however, a lot of healthcare organisations rely on third-party vendors, cloud service providers, and software developers. It is difficult to assign legal liability between hospitals and service providers when a cyberattack is caused by flaws in third-party systems, especially when there are unclear contractual and regulatory duties.

Mandatory Cyber Incident Reporting

Limiting damage, coordinating incident response, and stopping additional attacks all depend on prompt reporting of ransomware attacks. Healthcare and other critical infrastructure sectors are now required by law to disclose cyber incidents in a number of jurisdictions. However, reporting requirements vary greatly between nations, which causes inconsistent procedures and information sharing delays²¹. National and multinational cybersecurity responses would be strengthened by the establishment of consistent reporting standards.

Challenges in Cross Border Cybercrime Investigations

Attackers, victims, servers, and digital evidence are often spread across international borders in ransomware assaults. Investigations and prosecutions are frequently delayed by variations in national laws, jurisdictional disputes, limitations on data exchange, and procedural requirements. To counteract cross-border ransomware attacks that target healthcare institutions, effective international cooperation through information sharing, reciprocal legal aid, and harmonised cybercrime laws is crucial.

²¹ Arunkumar Palanichamy, Sivakumar Dhandapani, *Data Security Challenges In Hospitals: A Survey on Cyber Security Issues In HealthCare Sector and Their Applications*, RESEARCH SQUARE, 1, 5, (2025)

Strengthening Cybersecurity in Healthcare

Mandatory Cybersecurity standards

Hospitals should be subject to mandatory cybersecurity regulations set by governments, which should include minimal security standards for medical equipment, electronic health data, and healthcare systems. Frequent enforcement and monitoring of compliance can improve cyber resilience and lower the likelihood of ransomware attacks.

Risk Assessment and Incident Response Planning

Periodic cybersecurity risk assessments should be carried out by healthcare organisations in order to find weaknesses and put in place efficient mitigation strategies. To guaranty the continuation of vital healthcare services during cyberattacks, every hospital should keep an extensive incident response and disaster recovery strategy.

Data Protection and Regular Security Audits

To protect sensitive patient data, hospitals must use strong data security features like encryption, multi-factor authentication, secure backups, and access limits. To reduce security threats, regular cybersecurity audits, vulnerability assessments, and employee awareness training ought to be required.

International Cooperation and Information Sharing

Effective international cooperation is crucial since ransomware is a transnational cybercrime. To better the identification, prevention, and punishment of ransomware attacks, governments should increase information sharing, mutual legal aid, intelligence sharing, and cooperative investigations through international organisations.

Recommendations for India based on Global Best Practices

India should adopt a comprehensive healthcare cybersecurity framework by introducing sector specific cybersecurity standards for hospitals, strengthening mandatory cyber incident reporting, enhancing CERT-In's coordination with healthcare institutions, and establishing clear cybersecurity obligations for healthcare providers and third-party vendors. Drawing from global best practices, India should also promote regular security audits, cyber resilience

planning, capacity building, and international cooperation to better protect its rapidly expanding digital healthcare ecosystem from ransomware attacks²².

Conclusion

Ransomware attacks have become one of the most serious cybersecurity threats to the healthcare sector, disrupting essential medical services, compromising sensitive patient data, and endangering patient safety. Even while cybersecurity and data protection laws have been strengthened in many nations, there are still major issues with attribution, jurisdiction, responsibility, and cross-border enforcement. The comparative analysis shows that in addition to strong cybersecurity measures, comprehensive legislative and regulatory frameworks backed by international cooperation are also necessary for effective hospital protection. By implementing industry-specific laws, boosting cyber resilience, and utilising international best practices, India, in particular, can fortify its healthcare cybersecurity regime. In an increasingly digital world, protecting vital healthcare infrastructure, defending patient rights, and guaranteeing the safe provision of healthcare services all depend on a coordinated legal strategy.

²² Ranjan Pal and Bodhibrata Nag, *5 ways Indian medical administrations can boost hospital cyber-security*, FORBES INDIA, (April 14, 2023) <https://www.forbesindia.com/article/iim-calcutta/5-ways-indian-medical-administrations-canboost-hospital-cybersecurity/84397/1>