Ransomware Attacks on Healthcare Systems: Legal Responsibilities and Risk Management

Ramashish Murugan
Independent Research Scholar, Verginia, United States
Email ID: paulissacres2005@gmail.com

Cybersecurity Law and Policy Review
Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

Ransomware attacks against healthcare organisations have emerged as one of the most acute and consequential cybersecurity threats of the contemporary era, combining devastating operational disruption with the exposure of uniquely sensitive personal health information and, in documented cases, the direct causation of patient harm and death. The healthcare sector's structural vulnerabilities — a vast and heterogeneous attack surface, pervasive legacy technology, under-resourced security functions, and the life-critical nature of operations that makes ransom payment an institutionally tempting response — have made it the single most targeted sector for ransomware globally. This article examines the legal responsibilities of healthcare organisations, technology vendors, and state actors arising from ransomware attacks, analysing the duty of care under data protection law, healthcare regulation, and general negligence principles; the contractual and tortious liability frameworks applicable to healthcare ransomware incidents; the regulatory enforcement landscape across key jurisdictions; the specific legal obligations triggered by ransomware-induced data breaches; and the risk management and governance frameworks that law requires and that best practice recommends.

Keywords: *ransomware; healthcare cybersecurity; HIPAA; NHS; data breach; duty of care; patient safety; ransomware payment; risk management; critical infrastructure; vendor liability; cyber insurance*

1. INTRODUCTION

On 12 May 2017, the WannaCry ransomware attack swept across the global internet, encrypting the files of an estimated 200,000 computers across 150 countries within the space of a single day. For most affected organisations, the attack was a costly but ultimately recoverable disruption. For the United Kingdom's National Health Service, it was a humanitarian emergency. Approximately 80 of 236 NHS Trusts in England were affected, with 34 Trusts having data encrypted and a further 46 Trusts whose systems were blocked as a precautionary measure. An estimated 19,000 appointments were cancelled, ambulances were diverted, and clinical records became inaccessible at a critical moment of patient care. The NHS attack cost an estimated £92 million in disrupted services and IT remediation — and it was caused not by sophisticated new malware but by a vulnerability

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

in Windows operating systems for which a patch had been available for two months, deployed against an NHS estate that had conspicuously failed to apply it.

WannaCry was a watershed, but not because it was unprecedented. Ransomware attacks had been targeting healthcare organisations for years before 2017, and they have continued to do so with increasing frequency, sophistication, and severity in the years since. In 2020, a ransomware attack on Düsseldorf University Hospital in Germany caused the diversion of a critically ill patient to another facility; the patient died in transit, and German prosecutors opened — though ultimately did not pursue — what would have been the world's first criminal homicide investigation arising from a cyberattack. In 2021, an attack on Ireland's Health Service Executive (HSE) paralysed the national health system of an entire country for weeks, with full system restoration taking months and costing an estimated €100 million. In 2024, an attack on Ascension Health, one of the largest private healthcare systems in the United States with 140 hospitals across 19 states, disrupted clinical operations for weeks and exposed the personal health data of millions of patients. These are not isolated incidents; they are representative episodes in a sustained, industrialised campaign against one of the world's most critical sectors.

This article examines the legal responsibilities of healthcare organisations arising from ransomware incidents and the risk management frameworks — both legally mandated and best-practice recommended — through which those responsibilities should be discharged. Part Two analyses the ransomware threat to healthcare in depth: the attack vectors exploited, the operational consequences of attacks, and the criminal ecosystems that perpetrate them. Part Three examines the regulatory framework governing healthcare cybersecurity across key jurisdictions. Part Four analyses the duty of care, contractual, and tortious liability frameworks applicable to healthcare ransomware incidents. Part Five addresses the specific legal obligations triggered by ransomware-induced data breaches. Part Six examines the ransomware payment decision and its legal dimensions. Part Seven addresses vendor liability and supply chain responsibility. Part Eight advances a normative framework for risk management. Part Nine concludes.

2. THE RANSOMWARE THREAT TO HEALTHCARE: SCOPE, VECTORS, AND CONSEQUENCES

2.1 The Scale and Trajectory of the Threat

Healthcare has consistently ranked as the most targeted sector for ransomware attacks globally since at least 2016, a distinction attributable to a combination of factors that make healthcare organisations both attractive targets and reliable payers. The attractiveness of healthcare as a ransomware target derives from the extreme sensitivity of health data — which commands premium prices on criminal marketplaces and generates maximum leverage for double-extortion strategies that combine system encryption with the threat of data publication — combined with the operational imperative that makes prolonged system outages intolerable in ways that make the ransom payment calculation more favourable for attackers than in most other sectors.

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

The statistics are stark. According to the cybersecurity firm Sophos's annual State of Ransomware in Healthcare report for 2024, 67 percent of healthcare organisations surveyed globally reported being hit by ransomware in the prior year, compared to a cross-sector average of 59 percent. The average ransom demanded from healthcare organisations reached approximately $4.4 million in 2023, with average total recovery costs — including system restoration, business interruption, regulatory response, legal costs, and reputational damage — approaching $10 million per incident. In the United States, the Department of Health and Human Services' Office for Civil Rights (OCR) received 725 reports of healthcare data breaches affecting 500 or more individuals in 2023 alone, collectively exposing the health records of over 133 million Americans — a figure that represents more than one in three of the US population.

2.2 Attack Vectors and Healthcare-Specific Vulnerabilities

Healthcare organisations present an unusually broad and heterogeneous attack surface that creates multiple entry points for ransomware operators. The primary attack vectors — phishing emails, exploitation of unpatched vulnerabilities in internet-facing systems, compromise of remote desktop protocol (RDP) connections, and supply chain compromise through healthcare IT vendors and managed service providers — are common across sectors. What distinguishes the healthcare context is the combination of a vast legacy technology estate, chronic under-investment in cybersecurity, and operational constraints that limit the ability to apply security controls that would be standard in other sectors.

Legacy technology is a particularly acute vulnerability in healthcare. Clinical equipment — from imaging systems to patient monitoring devices to infusion pumps — frequently runs on operating systems that have reached end-of-life and can no longer receive security patches, yet cannot be replaced or isolated without disrupting patient care. The NHS estate attacked by WannaCry contained a substantial proportion of computers running Windows XP, an operating system that Microsoft had ceased to support in 2014. The integration of medical devices with hospital networks — driven by genuine clinical benefits including remote monitoring, electronic prescribing, and automated data transfer — extends the attack surface into the clinical environment in ways that have profound implications for both cybersecurity and patient safety.

2.3 Operational Consequences and Patient Harm

The operational consequences of ransomware attacks on healthcare organisations extend far beyond the financial costs of ransom payments and system restoration to encompass direct impacts on patient care whose severity is unique to the healthcare context. When clinical systems are encrypted and rendered unavailable, the consequences cascade through every aspect of healthcare delivery: electronic health records become inaccessible, forcing staff to revert to paper-based processes with which many have little experience; laboratory results cannot be delivered electronically; medication administration systems are disrupted; imaging systems go offline; scheduling systems fail; and the communication infrastructure that coordinates clinical teams is compromised.

The empirical evidence of patient harm from healthcare ransomware attacks has grown substantially over recent years, though the causal links between cyberattacks and adverse patient outcomes are often difficult to establish definitively and healthcare organisations

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

and their legal advisors have incentives to resist such characterisation. A landmark 2023 study published in JAMA Network Open, examining mortality data at hospitals affected by ransomware attacks, found a statistically significant association between ransomware attacks and increased in-hospital mortality, particularly among time-sensitive conditions including stroke, sepsis, and cardiac events where delays in diagnosis and treatment measured in minutes can determine outcomes. A systematic review published in Health Affairs the same year identified documented instances of treatment delays, medication errors, diverted ambulances, cancelled surgeries, and complications in labour and delivery attributable to ransomware-induced system outages.

The 2020 Düsseldorf University Hospital incident, though ultimately not prosecuted as a homicide, crystallised the connection between ransomware attacks and patient mortality in a way that has significantly influenced subsequent regulatory and legal discourse. German prosecutors' initial characterisation of the patient death as potentially constituting negligent homicide attributable to the ransomware operators — a characterisation ultimately abandoned when it was established that the patient's condition was likely fatal regardless of the diversion — illustrated both the legal theory and its evidentiary challenges. Subsequent analysis by legal scholars and regulators has focused not only on the liability of the criminal attackers (whose location and identity present obvious enforcement challenges) but on the liability of the healthcare organisation whose inadequate security allowed the attack to succeed.

3. THE REGULATORY FRAMEWORK GOVERNING HEALTHCARE CYBERSECURITY

3.1 United States: HIPAA, HHS Enforcement, and Emerging Mandates

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations — principally the Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the Security Rule (45 CFR Parts 160 and 164, Subparts A and C) — establish the foundational regulatory framework for the protection of health information in the United States. The HIPAA Security Rule requires covered entities (healthcare providers, health plans, and healthcare clearinghouses) and their business associates to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI). Its required and addressable implementation specifications encompass risk analysis and risk management, workforce training, access controls, audit controls, transmission security, contingency planning, and a range of other security measures.

HIPAA enforcement is vested primarily in the Department of Health and Human Services' Office for Civil Rights (OCR), which investigates complaints and conducts compliance reviews, and the Department of Justice, which may prosecute wilful HIPAA violations criminally. OCR's civil monetary penalty authority — up to $1.9 million per violation category per year, with no cap on total penalties in cases of wilful neglect — provides a substantial enforcement mechanism that OCR has deployed with increasing aggressiveness in the ransomware context. OCR's resolution agreements with ransomware-affected covered entities — including Doctors' Management Services ($100,000 resolution

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

agreement in 2023 following a GandCrab ransomware attack), Lafourche Medical Group ($480,000 resolution agreement in 2022), and numerous other settlements — have established a clear regulatory expectation that ransomware attacks will trigger HIPAA compliance reviews and that inadequate security risk analysis and risk management programmes will result in enforcement action.

The adequacy of HIPAA as a cybersecurity framework for the contemporary ransomware threat has been the subject of sustained criticism from cybersecurity professionals and policy analysts. The Security Rule's 'addressable' implementation specification structure — which permits covered entities to assess whether a given specification is reasonable and appropriate in their environment and to implement an alternative measure or document why the specification is not applicable — has been interpreted by many covered entities as providing greater flexibility than OCR intends, resulting in security programmes that satisfy HIPAA's letter without achieving meaningful security against contemporary ransomware threats. HHS's December 2023 Cybersecurity Performance Goals for the healthcare sector, developed in coordination with CISA, represent a significant step toward articulating more specific and contemporary security expectations, and proposed legislation to update HIPAA's security requirements and increase civil penalties for violations has been introduced in Congress, though not yet enacted as of this writing.

3.2 United Kingdom and European Union

In the United Kingdom, the regulatory framework for healthcare cybersecurity is fragmented across multiple bodies and instruments. NHS organisations are subject to the Data Security and Protection Toolkit (DSPT), an annual self-assessment mechanism that requires NHS bodies to demonstrate compliance with the National Data Guardian's ten data security standards. The DSPT's security requirements were substantially strengthened following the WannaCry attack and the subsequent Securing Cyber Resilience in Health and Care report published by the Department of Health and Social Care. NHS organisations are also subject to the UK GDPR and Data Protection Act 2018 as data controllers, with enforcement by the Information Commissioner's Office (ICO); the ICO has issued enforcement notices and monetary penalty notices against NHS organisations for data security failures, though penalties in the healthcare context have generally been modest relative to the sector's data processing scale.

The NHS's cybersecurity governance has been subject to sustained critical scrutiny since WannaCry. The National Audit Office's 2017 report on the WannaCry attack found that the NHS lacked a coordinated cybersecurity strategy, that basic security hygiene measures (patch management, backed-up data, tested business continuity plans) were not consistently implemented, and that the Department of Health had not acted on specific warnings about NHS cybersecurity vulnerabilities issued by NHS Digital in the months before the attack. Subsequent investment in the NHS Cyber Operations Centre and NHS-CERT has improved the sector's detection and response capabilities, though the persistent underfunding of NHS IT infrastructure — of which cybersecurity investment is a subset — continues to limit the sector's resilience against sophisticated ransomware campaigns.

3.3 Australia, Canada, and Comparative Perspectives

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

Australia's regulatory framework for healthcare cybersecurity has been significantly strengthened in recent years. The My Health Records Act 2012 governs the security of Australia's national digital health record system, imposing specific security obligations on system operators and healthcare providers who register with the system. The Privacy Act 1988 and the Australian Privacy Principles impose data security obligations on healthcare providers that handle health information, with the Office of the Australian Information Commissioner empowered to investigate and impose civil penalties for serious or repeated privacy interferences. The Security of Critical Infrastructure Act 2018, as amended to encompass the health sector, imposes risk management programme obligations and incident reporting requirements on defined critical healthcare infrastructure assets.

Canada's healthcare cybersecurity framework operates across federal and provincial jurisdictions, reflecting the division of healthcare regulatory authority under the Canadian Constitution. At the federal level, PIPEDA (the Personal Information Protection and Electronic Documents Act) imposes security safeguard obligations on federally regulated private sector organisations handling personal health information. Provincial health privacy legislation — including Ontario's Personal Health Information Protection Act (PHIPA), British Columbia's E-Health (Personal Health Information Access and Protection of Privacy) Act, and Alberta's Health Information Act — imposes more specific obligations on healthcare providers and custodians. The Canadian Centre for Cyber Security has published sector-specific guidance for healthcare organisations, and the increasing frequency of ransomware attacks against Canadian hospital systems — including the 2023 attack on five southwestern Ontario hospitals — has generated legislative attention to the adequacy of the existing framework.

4. DUTY OF CARE, NEGLIGENCE, AND TORTIOUS LIABILITY

4.1 The Healthcare Organisation's Duty of Care in Cybersecurity

The duty of care that healthcare organisations owe their patients is one of the most clearly established and demanding duties in tort law, grounded in the special relationship between healthcare provider and patient and the particular vulnerability that patients bring to that relationship. The traditional scope of this duty — encompassing the obligation to exercise reasonable skill and care in the provision of treatment — has historically been analysed in terms of clinical decisions and physical interventions. The pervasive integration of digital systems into healthcare delivery requires that this duty be understood as extending to the cybersecurity of the systems and infrastructure upon which treatment depends, as a natural and necessary evolution of the duty's application to the contemporary healthcare environment.

Under this analysis, a healthcare organisation that fails to implement reasonable cybersecurity measures — and that suffers a ransomware attack that disrupts patient care as a result — may bear tortious liability for patient harm that flows from that disruption. The standard of care in negligence — what a reasonable healthcare organisation in the defendant's position would have done — would be informed by regulatory requirements (including HIPAA Security Rule specifications, NIS2 obligations, and equivalent national frameworks), industry security standards (including the NIST Cybersecurity Framework

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

and sector-specific security benchmarks), publicly available information about known ransomware attack vectors, and the specific vulnerabilities present in the defendant organisation's environment.

The causal link between cybersecurity negligence and patient harm presents significant evidentiary challenges but is not insurmountable. Where a ransomware attack can be demonstrated to have caused the delay, cancellation, or degradation of treatment, and where that delay or degradation can be linked to adverse patient outcomes through evidence establishing that earlier or uninterrupted treatment would have produced a better outcome, the chain of causation from cybersecurity negligence to patient injury is established in principle. The empirical literature on ransomware-attributable patient harm — including the JAMA Network Open and Health Affairs studies cited in Part Two — provides expert evidence support for such claims that did not exist a decade ago.

4.2 Class Actions and Collective Redress

The mass exposure of patient health data in ransomware-induced breaches — affecting tens or hundreds of thousands of patients in major incidents — has generated significant class action litigation in the United States, where the class action mechanism provides a vehicle for aggregating individually modest privacy injury claims into litigation that achieves both compensation and deterrence at scale. US federal courts have seen a substantial proliferation of healthcare data breach class actions following ransomware incidents, with plaintiffs alleging violations of HIPAA (which does not provide a private right of action but is used to establish the standard of care in negligence claims), state consumer protection statutes, common law negligence, and state medical privacy laws.

The threshold question in healthcare ransomware class actions — whether data breach victims have suffered cognisable legal injury sufficient to establish Article III standing — has been the subject of extensive litigation, with the US Supreme Court's 2021 decision in TransUnion LLC v. Ramirez significantly affecting the analysis. Courts have been more willing to find standing where plaintiffs can demonstrate actual misuse of their exposed health data, documented identity theft or fraud, or out-of-pocket expenditures on credit monitoring and identity theft protection.

Settlement values in healthcare ransomware class actions have been substantial. The settlement of class litigation arising from the Anthem health insurance data breach (2015) reached $115 million; the settlement of litigation arising from the Community Health Systems breach reached $162 million; and numerous hospital system ransomware breach class actions have settled for tens of millions of dollars. These settlements — though often structured to provide relatively modest per-plaintiff compensation — impose significant aggregate costs on healthcare organisations and their insurers, and the combination of settlement pressure and reputational risk drives cybersecurity investment more effectively than regulatory penalties in some institutional contexts.

4.3 Contractual Liability and Business Associate Agreements

HIPAA's Business Associate Agreement (BAA) framework imposes contractual cybersecurity obligations on the extensive ecosystem of technology vendors, cloud service providers, managed service providers, billing companies, and other business associates that handle ePHI on behalf of covered entities. A BAA must require the business associate to

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

implement appropriate safeguards to protect the security of ePHI, report security incidents to the covered entity, and comply with the applicable requirements of the HIPAA Security Rule. Business associates that fail to comply with these contractual and regulatory obligations bear direct regulatory liability to OCR and may also face contractual liability to the covered entity for breach of the BAA.

5. RANSOMWARE-INDUCED DATA BREACHES: LEGAL NOTIFICATION AND RESPONSE OBLIGATIONS

5.1 HIPAA Breach Notification

The HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D) requires covered entities to notify affected individuals, the Secretary of HHS, and in cases of breaches affecting 500 or more residents of a state, prominent media outlets, following the discovery of a breach of unsecured protected health information. The notification must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. For breaches affecting 500 or more individuals at the national level, HHS must be notified contemporaneously with individual notification; for smaller breaches, HHS notification may be deferred to an annual summary report.

OCR's guidance on HIPAA breach notification in the ransomware context has evolved significantly over the decade since ransomware first became a widespread threat. OCR's 2016 ransomware guidance established the principle that, where ransomware encrypts ePHI, this presumptively constitutes a breach of unsecured PHI requiring notification unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised based on a four-factor risk assessment. The 2016 guidance's risk assessment framework — examining the nature and extent of the PHI involved, the identity of the unauthorised person who used or may have accessed the PHI, whether the PHI was actually acquired or viewed, and the extent to which risk has been mitigated — has proven difficult to apply in practice to modern double-extortion ransomware incidents, where data exfiltration frequently precedes encryption and where the volume of exfiltrated data may be enormous while the actual extent of adversary access to specific records remains uncertain.

The tension between the 60-day notification deadline and the practical timeline of ransomware incident response — in which full forensic investigation of the scope and nature of a breach may require months — generates significant legal risk for affected healthcare organisations. Organisations that provide premature notifications based on incomplete forensic findings may subsequently need to issue corrections or supplements; organisations that await complete forensic clarity before notifying may miss the 60-day deadline and face OCR enforcement for untimely notification. OCR's consistent position that the 60-day period begins upon discovery rather than upon completion of investigation places substantial pressure on healthcare organisations to accelerate forensic timelines in ways that may compromise investigation quality.

5.2 GDPR and International Notification Obligations

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

Under the General Data Protection Regulation, healthcare organisations subject to its requirements must notify the competent supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it (Article 33). Where the breach is likely to result in a high risk to the rights and freedoms of natural persons — as health data breaches almost invariably will — the controller must also communicate the breach to the affected data subjects without undue delay (Article 34). The 72-hour notification window under the GDPR is substantially more compressed than HIPAA's 60-day window, creating severe operational pressures for healthcare organisations managing the acute phase of a ransomware incident while simultaneously attempting to conduct preliminary breach assessment and initiate regulatory notification.

Healthcare data is classified as a special category of personal data under Article 9 of the GDPR, subject to enhanced protection and processing restrictions that reinforce the sensitivity of health data breaches. The combination of mandatory breach notification to supervisory authorities, mandatory communication to affected individuals, the enhanced sensitivity of health data, and the potential for significant administrative fines creates a multi-dimensional regulatory exposure for EU healthcare organisations affected by ransomware. Supervisory authority responses to healthcare ransomware breaches have varied across member states, with some authorities demonstrating greater sympathy for the circumstances of organisations that have been the victims of criminal attacks while others have pursued enforcement action primarily focused on the adequacy of pre-attack security measures.

5.3 Double Extortion and the Data Publication Threat

The evolution of ransomware tactics from pure encryption-and-ransom to double extortion — in which attackers exfiltrate data before encrypting it and threaten to publish the exfiltrated data on criminal leak sites unless ransom is paid — has substantially complicated both the legal analysis of healthcare ransomware incidents and the operational decisions facing affected organisations. Double extortion creates a second independent basis for ransom payment pressure (beyond the operational disruption of encryption) that is particularly acute in the healthcare context, where the public disclosure of patient health records can cause direct harm to patients through stigma, discrimination, and emotional distress, and where the reputational consequences for the healthcare organisation of prominent data publication can be severe.

From a legal perspective, double extortion means that a ransomware attack on a healthcare organisation almost invariably constitutes a personal data breach requiring notification under HIPAA and/or GDPR, regardless of whether encryption has prevented access to systems or whether backup systems have enabled prompt restoration. The exfiltration of patient data — even if the organisation's own systems are not persistently compromised — triggers breach notification obligations, mandatory forensic investigation of the scope of exfiltration, and the full range of regulatory and litigation risks associated with a health data breach. Organisations that pay the ransom in the hope of suppressing data publication must understand that payment provides no legal assurance against publication, no evidence that exfiltrated data has been deleted by the attacker, and no indemnification against the legal consequences of the underlying breach.

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

6. THE RANSOMWARE PAYMENT DECISION: LEGAL, ETHICAL, AND POLICY DIMENSIONS

6.1 The Legal Framework Governing Ransomware Payments

The decision whether to pay a ransomware demand is one of the most consequential and legally complex decisions that a healthcare organisation facing an attack must make, typically under conditions of extreme operational pressure, incomplete information about the attackers' identity, and acute awareness of the patient safety consequences of prolonged system outages. The legal framework governing ransomware payments is neither straightforward nor uniform across jurisdictions, and has been evolving rapidly in response to both the growth of the ransomware threat and the increasingly prominent involvement of state-sanctioned criminal organisations in ransomware operations.

In the United States, the Office of Foreign Assets Control (OFAC) of the Department of the Treasury administers sanctions programmes that may render ransomware payments to certain threat actors illegal. OFAC's 2020 Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, updated in 2021, warns that organisations that make ransomware payments to threat actors on OFAC's Specially Designated Nationals (SDN) list — or that facilitate such payments through cyber insurance, digital forensic incident response firms, or financial institutions — may be liable for sanctions violations carrying civil penalties up to approximately $16 million per violation, regardless of whether the organisation knew it was dealing with a sanctioned entity. In the healthcare context, ransomware groups including Evil Corp (sanctioned in 2019), a subsidiary of which deployed the BitPaymer ransomware against multiple healthcare targets, and groups with alleged Russian government affiliations, have been subject to SDN designations that nominally render payments to them prohibited.

The practical application of OFAC's sanctions framework to healthcare ransomware payments is complicated by the significant uncertainty that typically exists at the time of payment about the true identity of the ransomware operators. Criminal ransomware groups routinely use pseudonyms, change group names after high-profile incidents or law enforcement pressure, and share code and infrastructure in ways that make definitive attribution extremely difficult within the timelines relevant to the payment decision. OFAC's expectation that organisations conduct due diligence on the identity of potential ransomware payees — and the significant practical barriers to conducting such due diligence under operational emergency conditions — creates a legal risk that healthcare organisations cannot fully mitigate through reasonable efforts.

6.2 Payment Transparency, Mandatory Reporting, and Policy Debates

The opacity of the ransomware payment landscape — arising from the absence of mandatory reporting requirements for ransomware payments in most jurisdictions — has significantly hampered both law enforcement intelligence gathering and policy-maker understanding of the scale and character of the ransomware economy. Healthcare organisations that pay ransoms have historically done so discreetly, frequently with the assistance of specialist incident response firms and cyber insurers who facilitate the negotiation and payment process, with minimal public disclosure and no mandatory regulatory reporting specifically focused on the payment decision. This opacity serves the

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

interests of ransomware operators by sustaining their revenue model and preventing the development of intelligence that could support law enforcement disruption.

7. VENDOR LIABILITY AND SUPPLY CHAIN RESPONSIBILITY IN HEALTHCARE RANSOMWARE

7.1 The Healthcare IT Vendor's Security Obligations

The healthcare IT vendor ecosystem — encompassing electronic health record providers, medical device manufacturers, cloud service providers, managed security service providers, telehealth platforms, and the full range of technology suppliers that support healthcare operations — occupies a position of extraordinary security significance. Ransomware operators have demonstrated a clear strategic preference for targeting healthcare IT vendors whose products are widely deployed across multiple healthcare organisations, enabling a single successful intrusion to cascade rapidly across a large population of victims. The 2024 Change Healthcare attack, the 2021 Kaseya VSA attack (which affected multiple managed service providers serving healthcare clients), and the 2020 SolarWinds compromise (which affected healthcare organisations among its estimated 18,000 victims) illustrate the devastating amplification effect of attacks on widely deployed healthcare IT infrastructure.

Notwithstanding the breadth of these contractual and regulatory obligations, the practical reality is that the liability exposure of healthcare IT vendors for security failures that enable ransomware attacks on their healthcare clients has historically been substantially limited by contractual limitation of liability clauses, software warranty disclaimers, and the challenges of establishing causation between vendor security failures and downstream patient harm. The reform of vendor liability — to ensure that the vendors who supply insecure technology to healthcare organisations bear an appropriate share of the costs when that insecurity enables ransomware attacks — represents one of the most important and underattended dimensions of healthcare cybersecurity law reform.

7.2 Medical Device Security and the Regulatory Gap

Medical devices present a cybersecurity challenge that is unique to the healthcare context and that has until recently received inadequate regulatory attention. Networked medical devices — including infusion pumps, insulin pumps, pacemakers, patient monitoring systems, ventilators, imaging equipment, and a vast range of other clinical technologies — are attractive ransomware targets because their compromise can directly threaten patient safety, creating maximum leverage for ransomware operators. At the same time, the long operational lifecycles of medical devices, the rigorous and time-consuming regulatory approval processes required for device modifications, and the manufacturers' historical reluctance to develop and distribute security updates have created a population of deployed medical devices with significant known vulnerabilities for which no patches are available or installable.

The FDA's 2016 postmarket cybersecurity guidance for medical devices and its 2023 premarket guidance — supported by the Omnibus Consolidated Appropriations Act of 2023, which gave FDA explicit authority to require cybersecurity provisions as a condition

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

of medical device marketing authorisation — represent a significant step toward addressing the medical device security gap. The requirement that device manufacturers provide a software bill of materials, maintain a vulnerability disclosure programme, and develop plans for post-market security updates marks a fundamental shift from the historical assumption that medical device software was static and self-contained. However, the gap between the new regulatory requirements (applicable to new devices seeking authorisation) and the existing deployed base of vulnerable legacy devices remains substantial and will not be resolved by premarket requirements alone.

8. A LEGAL AND OPERATIONAL RISK MANAGEMENT FRAMEWORK FOR HEALTHCARE RANSOMWARE

8.1 Governance and Accountability

Effective risk management for ransomware in healthcare begins with governance — the establishment of clear accountability structures and oversight mechanisms that ensure cybersecurity receives appropriate attention and resources at the board and executive level. Healthcare organisations' governing bodies — hospital boards, NHS Trust boards, and equivalent governance structures — bear legal accountability for the adequacy of their organisations' security posture, and are expected under applicable regulatory frameworks and corporate governance standards to exercise informed oversight of cybersecurity risk. The US Department of Health and Human Services' 2023 Healthcare and Public Health Sector Cybersecurity Performance Goals explicitly address governance, including board-level cybersecurity oversight as a foundational element of healthcare cybersecurity best practice.

8.2 Technical Security Measures and Resilience

The technical security measures required to reduce healthcare organisations' ransomware risk are well-established in regulatory guidance, industry frameworks, and the published analysis of post-incident reviews. They include: comprehensive and up-to-date patch management across all networked systems, including the expedited patching of actively exploited vulnerabilities; network segmentation that limits ransomware's ability to spread laterally from an initial point of compromise to clinical systems; multi-factor authentication for all remote access and privileged account access; email security controls including advanced threat protection and user awareness training that reduces the effectiveness of phishing as an initial access vector; immutable, offline backup systems that enable restoration of clinical operations without payment; endpoint detection and response (EDR) tools capable of detecting and interrupting ransomware encryption processes; and tested incident response and business continuity plans specifically addressing ransomware scenarios.

The implementation of these measures across the full complexity of a large healthcare organisation — with its mix of modern IT systems, legacy clinical technology, medical devices, and third-party vendor-managed systems — is a substantial technical and organisational undertaking that requires sustained investment over time. Healthcare organisations must prioritise security investment through formal risk assessment processes

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

that identify and remediate the highest-risk vulnerabilities and that align security spending with the patient safety and regulatory consequences of different categories of failure. Regulatory frameworks that prescribe specific technical controls without engaging with the risk-based prioritisation challenges of healthcare security programmes risk producing compliance activity that addresses low-risk items while leaving critical vulnerabilities unaddressed.

8.3 Incident Response Planning and Legal Preparedness

Comprehensive, tested, and legally informed incident response planning is a legal obligation under HIPAA, GDPR, NIS2, and virtually every applicable cybersecurity regulatory framework. Yet the practical quality of healthcare incident response plans for ransomware — assessed against the criteria of operational workability under actual attack conditions, legal completeness with respect to notification obligations, and integration of the clinical and IT dimensions of the response — varies enormously across the sector. Incident response plans that sit unread on regulatory compliance shelves, that have not been tested through tabletop exercises simulating realistic ransomware scenarios, or that fail to address the complex notification obligations triggered by health data breaches, expose organisations to both operational and regulatory risk.

8.4 Cyber Insurance: Coverage, Gaps, and Legal Considerations

Cyber insurance has become an important component of healthcare organisations' financial risk management for ransomware, providing coverage for elements including ransom payments, forensic investigation costs, notification and credit monitoring costs, business interruption losses, and third-party liability claims. The healthcare cyber insurance market has, however, experienced significant contraction in recent years as the frequency and severity of healthcare ransomware claims have driven insurers to increase premiums substantially, reduce coverage limits, impose more stringent pre-underwriting security requirements, and introduce exclusions for specific attack categories, ransomware payment scenarios, and war and nation-state exclusions whose scope and applicability are the subject of substantial commercial litigation.

9. NORMATIVE RECOMMENDATIONS

The analysis presented in this article supports the following normative recommendations for the reform and strengthening of the legal framework governing ransomware attacks on healthcare systems.

First, regulatory frameworks governing healthcare cybersecurity — including HIPAA in the United States and equivalent national frameworks — should be updated to impose more specific and contemporary mandatory security requirements, aligned with current threat intelligence and security best practice, rather than relying on broadly stated principles whose implementation is inconsistently interpreted and enforced. The HHS Healthcare Cybersecurity Performance Goals should be translated into mandatory regulatory requirements for covered entities above defined size thresholds, with phase-in timelines and implementation support for smaller providers.

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

Second, vendor liability reform should address the systematic limitation of liability that allows healthcare IT vendors to supply insecure products and services to the healthcare sector without bearing appropriate responsibility for the downstream consequences. Software product liability frameworks — drawing on the EU Cyber Resilience Act model and the US National Cybersecurity Strategy's commitment to shifting liability to technology manufacturers — should be extended to healthcare IT products, with specific requirements for secure-by-design development, vulnerability disclosure programmes, timely patch provision, and software bills of materials for products deployed in clinical environments.

Third, mandatory ransomware payment reporting — as envisaged by CIRCIA in the United States and proposed in the United Kingdom and Australia — should be implemented across all major jurisdictions and operationalised in a manner that enables law enforcement intelligence gathering without imposing unrealistic disclosure timelines on healthcare organisations in the acute phase of incident response. Payment reporting should be accompanied by legal protections ensuring that disclosed payment information cannot be used as primary evidence in enforcement proceedings against the disclosing organisation.

Fourth, international law enforcement cooperation against ransomware-as-a-service ecosystems — including the takedown of ransomware infrastructure, the prosecution of ransomware developers and affiliates, and the recovery of ransomware proceeds — should be prioritised and resourced at levels commensurate with the scale of the threat. The healthcare sector's unique patient safety dimension should be recognised in law enforcement prioritisation frameworks, with attacks on healthcare systems treated as aggravated offences attracting enhanced penalties.

10. CONCLUSION

Ransomware attacks on healthcare systems are not an abstract cybersecurity problem — they are a direct threat to patient safety, a profound violation of medical privacy, and a fundamental challenge to the healthcare sector's ability to fulfil its core mission of care. The legal frameworks governing healthcare cybersecurity — developed for a threat environment that could not have anticipated the industrialisation of ransomware as a criminal business model or its systematic targeting of the healthcare sector's structural vulnerabilities — are inadequate to the challenge in multiple dimensions: their substantive security requirements are insufficiently specific and contemporary; their enforcement is under-resourced and inconsistently applied; their vendor liability provisions fail to hold the suppliers of insecure healthcare technology appropriately accountable; and their international dimensions are inadequate to disrupt the transnational criminal ecosystems that perpetrate the attacks.

The reforming agenda advanced in this article — mandatory contemporary security standards, vendor liability reform, ransomware payment transparency, enhanced international law enforcement cooperation, and enforceable patient rights — does not represent a comprehensive solution to the ransomware threat. Ransomware is a criminal phenomenon that ultimately requires criminal justice responses: the identification, prosecution, and incarceration of the developers and operators of ransomware-as-a-service platforms, and the disruption of the cryptocurrency infrastructure through which their proceeds are laundered.

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index

REFERENCES

Agrafiotis, I. et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate' (2018) 27 Journal of Cybersecurity 1.

Ascension Health, 'Cybersecurity Incident Update' (Ascension Health Press Release, 2024).

Australian Department of Home Affairs, 'Ransomware Action Plan' (Australian Government, 2021).

Binder, C. and Reinhold, T., 'Cyber Incidents: The Dilemma Between Immediate Notification and Meaningful Notification' (2022) 16(2) European Journal of Risk Regulation 312.

Cartwright, A. et al., 'To Pay or Not to Pay? Examining the Ransomware Dilemma' (2020) Proceedings of the 7th International Conference on Information Systems Security and Privacy, 130.

Change Healthcare, 'Notice of Data Breach' (UnitedHealth Group Inc., 2024).

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103, 136 Stat. 49.

Department of Health and Social Care, 'Securing Cyber Resilience in Health and Care: Progress Update October 2018' (DHSC, 2018).

Ge, M. et al., 'A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions' (2022) 56(1) ACM Computing Surveys 1.

General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

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

Health and Human Services (HHS), 'Healthcare and Public Health Sector Cybersecurity Performance Goals' (HHS, 2023).

HHS Office for Civil Rights, 'Ransomware and HIPAA' (HHS, 2016).

HHS Office for Civil Rights, 'Resolution Agreement with Doctors' Management Services' (HHS OCR, 2023).

Jalali, M.S. et al., 'Ransomware and Hospital Operations: A Review of the Evidence' (2023) 8(1) JAMA Network Open e2230705.

Klonoff, D.C., 'Cybersecurity for Connected Diabetes Devices' (2015) 17(8) Journal of Diabetes Science and Technology 1143.

Levi-Faur, D., 'The Global Diffusion of Regulatory Capitalism' (2005) 598 The Annals of the American Academy of Political and Social Science 12.

National Audit Office, 'Investigation: WannaCry Cyber Attack and the NHS' (NAO, 2017).

Network and Information Security 2 Directive (NIS2), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

OFAC Advisory, 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (US Department of the Treasury, September 2021).

Richardson, R. and North, M., 'Ransomware: Evolution, Mitigation and Prevention' (2017) 13(1) International Management Review 10.

Sophos, 'The State of Ransomware in Healthcare 2024' (Sophos, 2024).

TransUnion LLC v. Ramirez, 594 U.S. 413 (2021).

Watson, T. et al., 'The Impact of Ransomware on Patient Outcomes: A Systematic Review' (2023) 102(4) Health Affairs 634.

© 2026 Cybersecurity Law and Policy Review | https://clprj.com/journal/index