Science of Law, 2026, No. 3, pp. 1-6
DOI: 10.55284/5hm75m04

# Cyber Security in Hospitals: Legal Responsibilities

Nicki James Shepherd[1*], Stephanie Ness[2], Amjad Ali[3], Javeria Umber[3]

[1]The University of Law, Manchester, United Kingdom.
[2]Diplomatische Akademie, Austria.
[3]Department of Bioinformatics & Biotechnology, Government College University Faisalabad (GCUF), Pakistan.

**Keywords:**
Breach notification,
Critical infrastructure protection,
Cyber governance,
Cybersecurity,
Enterprise risk Management,
GDPR,
Health information privacy,
Healthcare data protection,
HIPAA,
Hospitals,
Legal liability,
Medical device security,
NIS2 directive,
Patient safety,
Ransomware.

**Abstract.** As a result of the increased use of interconnected technologies in healthcare systems, there has been a rapid transformation of healthcare organizations and an increase in reliance on these technologies, thus changing how hospitals operate. Hospitals now utilize many technologies that are interconnected through a number of electronic health record (EHR) systems, Internet of Medical Things (IoMT) devices, telehealth platforms, and cloud-based systems. While technology allows hospitals to provide better care and operate more efficiently, it has resulted in increased exposure to various types of cyber threats. Cyber threats directed at healthcare organizations include ransomware, phishing attacks, insider threats, and the exploitation of medical devices, and there are numerous case studies linking cyber incidents and the operational disruption they cause to the risks associated with the safety of patients. This article reviews the current state of cybersecurity in health care organizations with an emphasis on the legal obligations created by major regulatory frameworks—including HIPAA, HITECH, the GDPR, the NIS2 Directive, and cybersecurity guidance for medical devices—because of the increased reliance on these technologies. This article also discusses the intersection of various legal frameworks including data protection laws, the regulation of critical infrastructure, tort liability, and corporate governance; evaluates civil liability risk created through the use of technology, exposure to civil penalties for violations of regulations, notification of affected parties when a breach occurs, and third-party liability for cloud and vendor environments; and discusses ethical issues related to confidentiality, professional duties, and the effects of decisions made in response to ransomware attacks. The findings demonstrate that cybersecurity in hospitals has evolved from a technical IT function into a comprehensive legal and governance responsibility requiring board-level oversight, structured risk management frameworks, continuous compliance documentation, and workforce training. Strengthening institutional resilience requires integrating cybersecurity into enterprise risk management and aligning regulatory compliance with patient safety imperatives.

## 1. INTRODUCTION

As healthcare systems undergo fast-paced digital transformation, the landscape of providing patient services and associated outcomes is changing. Healthcare providers are relying on, and utilizing, many different types of technology most notably electronic healthcare record (EHR) systems, telehealth platforms, cloud computing, and various other medical devices that create a sophisticated digital ecosystem. While these technologies provide opportunities for improving care delivery, they also create an expanded attack surface for cybercriminals. Healthcare is one of the most "attacked" of all critical infrastructure sectors across the globe because of the high monetary value of medical data and the urgency of the services these organizations provide [1, 2]. Over the last ten years, there has been a dramatic increase in cyberattacks against hospitals, with the emergence of ransomware as one of the most troubled forms of attack. In fact, ransomware attacks have been documented to disrupt clinical workflow, delay treatment, and ultimately lead to an increase in the number of patients who die in a hospital [3] . A comprehensive analysis of ransomware attacks on US healthcare delivery organizations reported significant operational disruptions to their delivery process, including: ambulance diversion to an alternate location, downtime for electronic systems, etc. These disruptions reflect that failures in cybersecurity in hospitals are not simply technical issues, but concerns for patient safety [4].

Unlike regular confidential documents, health data is subject to increased levels of sensitivity. Health records include personal identifiers, financial information, insurance details, and a full medical history[5]. Because of this, health records are typically worth more than credit card information on the black market since they can be used for identity theft, insurance fraud, and other illegal activities [5]. For these reasons, hospitals need to treat cybersecurity as an obligation regarding the protection of information and as a legal obligation based on the principles of confidentiality with patients.

From a compliance standpoint, hospitals operate within strictly regulated environments that impose specific obligations regarding cybersecurity. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities to have administrative, technical, and physical safeguards to protect electronic protected health information (EHLPH) [6]. The General Data Protection Regulation (GDPR) in the European Union also requires “appropriate technical and organizational measures to protect personal data” and imposes significant penalties for non-compliance [7]. These rules demonstrate a global shift toward recognizing cybersecurity as part of legal compliance requirements in the health care field.

In addition to mandated laws, hospitals could be held liable for negligence and/or malpractice in cases where failure to implement reasonable cyber security measures has led to foreseeable injury or damage. According to researchers [7], "cyber security governance is more closely related to the accountability of institutions and to the risk management responsibilities of boards and the executive level" than ever before. As a result, hospitals' cyber security risks extend beyond the information technology (IT) department as they pertain to legal governance and organizational leadership. With the merging of patient safety, data protection laws, and institution liability laws, it is timely and necessary to analyze the legal obligations of hospitals regarding cyber security. This paper provides an overview of the changing cyber security environment in the health care sector, assesses

*Corresponding author.

the applicable legal environments, discusses liability issues, and recommends governance safeguards to improve compliance and resilience.

## 1.1. Cybersecurity Landscape in Hospitals

Due to rapid digital evolution, the rise in connected health technology and the increased reliance on real-time sharing of data between systems, the health care cyber environment has also evolved into a multi-layered and high risk landscape. Today, modern hospitals are viewed as Cyber-Physical Systems (CPS); the clinical care process, the business of running a hospital and the use of life support medical devices (e.g., patient monitors and MRI machines) are digitally integrated. This convergence creates a much larger attack surface, hence, health care as one of the most vulnerable sectors in terms of Critical Infrastructure globally. Cybercriminals frequently rank health care among the top three most targeted sectors for cyberattacks because the disruption of services can provide immediate financial leverage to the cybercriminal and potentially cause serious bodily harm to patients [8]. Cyber threats targeting hospitals are no longer limited to data theft; they increasingly aim to disrupt operations. Ransomware remains the dominant threat vector, capable of encrypting hospital systems, halting clinical services, and disabling diagnostic equipment. A comprehensive analysis of healthcare cybersecurity incidents highlights that ransomware attacks often exploit unpatched systems and phishing vulnerabilities, leading to prolonged downtime and financial losses. Unlike traditional cybercrime, hospital ransomware attacks carry profound ethical and legal implications because service interruptions can delay surgeries, diagnostic testing, and emergency responses [9]. Phishing and social engineering are still the main attack vectors to break into a healthcare organization, in addition to ransomware. Because of the high-pressure environments in healthcare, employees are highly vulnerable to falling for trick email messages or credential theft schemes. Research shows that human factors contribute significantly to breaches in cybersecurity in healthcare; therefore, there is an urgent need for structured training and organization protections. Insider threats, whether intentional or unintentional, pose a significant threat to a large healthcare network and large hospitals with many distribution points of access [10].

### 1.1.1. Vulnerable Systems in Hospital Environments

### 1.1.1.1. Electronic Health Records (EHRs)

The foundation of contemporary healthcare technology is made up of electronic health records. EHRs provide an effective way to coordinate care and provide greater access to information; however, the centralization of highly sensitive data in an EHR also makes it an attractive target for attack. According to studies, healthcare databases have been affected by breaches more often than any other sector, primarily due to the lack of protection for legacy systems and fragmented security governance. The combination of EHRs with other systems such as labs, billing systems, and outside providers only increases susceptibility due to dependences across multiple systems [11].

### 1.1.1.2. Internet of Medical Things (IoMT):

The proliferation of Internet of Medical Things (IoMT) devices—including infusion pumps, cardiac monitors, imaging systems, and wearable sensors—introduces significant cybersecurity risks. Many devices operate on outdated operating systems or lack robust encryption mechanisms. A systematic review on IoMT security identifies device heterogeneity, insufficient patch management, and weak authentication protocols as key systemic weaknesses .Compromised medical devices not only threaten data confidentiality but also raise concerns regarding device manipulation and patient safety [12].

### 1.1.1.3. Telehealth and Cloud-Based Systems:

In recent years, telemedicine has become increasingly prevalent, especially since the onset of COVID-19. The need for telemedicine has pushed the boundaries of hospital cyber security well beyond their physical locations. Hospitals can use technology to provide patient care through the use of telehealth platforms, which have been built on cloud infrastructures, remote access systems and third party service providers. While cloud technologies create opportunities for scalability and redundancy, the jurisdictional and compliance issues associated with utilizing these services for cross-border data transfers and shared responsibility models add a layer of complexity to the risk management process. Studies have shown that inadequate access controls and misconfigured cloud storage are two of the most significant reasons for the exposure of healthcare data [13]. In addition to using cloud technologies, hospitals are increasingly adopting a hybrid IT environment to support both on-premises and cloud-based services. The resulting architectural complexity makes it difficult for hospitals to effectively manage their cybersecurity risks. To achieve effective cybersecurity in hospitals, technical measures alone do not suffice; governance must also incorporate legal compliance, risk assessment and incident response preparedness components [13].

### 1.1.2. Systemic Challenges

Hospitals have special challenges when it comes to cybersecurity compared to other industries. For instance, when updating software and applying system patches, hospitals have strict criteria placed on them with respect to the amount of allowable time for these updates (limited). Due to budgetary constraints, money is usually spent on purchases and upgrading medical equipment before spending any money on enhancing cybersecurity. Lastly, regulations that define interoperability require that data be easily exchanged between and within organizations creating "weak" perimeter security structures for protecting sensitive data from being accessed by unauthorized individuals and/or organizations. According to research, healthcare organizations are lagging behind many other critical industries when it comes to cybersecurity maturity due to fragmented IT governance and/or poorly funded security organizations. In addition to the many challenges hospitals face with cybersecurity, the amount of overlapping regulatory compliance requirements further complicates an already complicated situation. Hospitals must comply with multiple sets of overlapping laws, standards for accreditation and industry standards. As well, if the hospital does not include cybersecurity as part of its risk management system, it will incur significant operational liabilities, reputational liabilities and/or legal liabilities. More importantly, the perception of cybersecurity has evolved so as to not be viewed as just an issue for the IT department, but rather as a governance issue that requires input from and oversight by senior executives [14].

Hospital Cybersecurity Vulnerabilities
Ransomware
Phishing & Social Engineering
Medical Device Hacking

Figure 1. Major cybersecurity vulnerabilities in hospital environments, including ransomware attacks, phishing and social engineering schemes, and medical device hacking targeting interconnected clinical systems.

## 1.2. Legal Frameworks Governing Hospital Cybersecurity

Regulations surrounding hospitals are multi-layered, regulated and encompass a variety of safety, privacy and critical infrastructure regulations which indicates that cybersecurity practices must be included as a legal requirement within the overall context of patient safety and the operation of critical infrastructure. The healthcare sector, as opposed to other sectors, is governed by specific privacy laws, general data protection laws, cybersecurity regulations, medical device regulations and contractual obligations. These regulations create increasing numbers of affirmative obligations for hospitals including risk assessment, protection implementation, documentation of compliance, notification of breaches to regulatory authorities and patients. Failure to comply with a hospital's regulatory obligations can result in significant administrative fines, civil liability, and damage to reputation and in some cases, criminal prosecution.

Understanding the legal framework surrounding the healthcare industry is accomplished through three intersecting domains: (1) data protection and privacy legislation, (2) cybersecurity and critical infrastructure regulations, and (3) medical device and health technology regulations.

### 1.2.1. Data Protection and Privacy Regulations

Data protection laws form the cornerstone of hospital cybersecurity obligations because health data is classified as highly sensitive personal information.

#### 1.2.1.1. European Union: GDPR

GDPR offers one of the most rigorous global protections for data. The GDPR recognizes health data as special category data and sets additional security protections for the data under Article 9. Article 32 requires the implementation of appropriate technical and organizational controls (for example, encryption, confidentiality, integrity and durability of processing systems). The GDPR also requires notification of breaches within 72 hours of becoming aware of the breach (Article 33). According to scholarly analysis, the GDPR has transformed Cybersecurity from a best practice approach to a legally binding compliance obligation with accountability and demonstrable risk management. Empirical research on the implementing of the GDPR found that it has strengthened governing Cybersecurity based on requiring documentation of data protection impact assessments (DPIAs) for high-risk processing situations such as hospitals [7, 15].

#### 1.2.1.2. United States: HIPAA and HITECH

The Security Rule under HIPAA (Health Insurance Portability and Accountability Act) mandates the use of administrative, physical and technical safeguards to safeguard ePHI (Electronic Protected Health Information). HITECH (Health Information Technology for Economic and Clinical Health) increased enforcement of these regulations with the introduction of mandatory breach notifications and increased penalties. Legal scholarship points out that HIPAA created a "reasonable and appropriate" security standard that requires continuing risk assessments rather than relying upon static compliance. Studies suggest that HITECH’s mandatory breach notification requirements increased transparency but also exposed hospitals to class-action lawsuits and reputational damage [16].

### 1.2.2. Cybersecurity and Critical Infrastructure Regulations:

Hospitals are increasingly recognized as part of national critical infrastructure sectors, subject to broader cybersecurity directives beyond privacy law. The NIS2 Directive imposes additional responsibilities on "essential entities", which include healthcare organizations, including hospitals. The NIS2 Directive requires organizations to have risk management processes, report incidents, secure their supply chain as well as have board-level accountability. Legal commentary has suggested that the NIS2 Directive represents a shifting of the focus away from simply notifying upon a breach to hold organizations accountable for managing risks and having proactive governance obligations. In the U.S. hospitals are identified as part of the Healthcare and

Public Health (HPH) Sector under national critical infrastructure policy which is coordinated by the Cybersecurity and Infrastructure Security Agency (CISA). The mandatory list of control measures may vary from one hospital to another however, federal guidance continues to influence regulations and establish benchmarks for the provision of patient care. Research has shown that not only will aligning with the NIST Cybersecurity Framework increase your organizations legal defensibility but will also establish a record of your organizations efforts to exercise due diligence prior, during and after a cyber incident [14].

### 1.2.3. Medical Device and Health Technology Regulation

Cybersecurity regulation increasingly extends to network-connected medical devices. In the United States, the U.S. Food and Drug Administration (FDA) has issued premarket and postmarket cybersecurity guidance for medical devices, requiring manufacturers to integrate cybersecurity risk management throughout product lifecycles. Scholars argue that cybersecurity vulnerabilities in medical devices create overlapping liability regimes involving manufacturers, hospitals, and software vendors. Research on IoMT regulation further emphasizes the need for coordinated compliance between device safety law and data protection law [12, 17].

Table 1. Comparative Overview of Key Legal Frameworks.

| Framework | Jurisdiction | Core Obligation | Breach Notification | Penalties |
|---|---|---|---|---|
| GDPR | European Union | Implement appropriate technical & organizational measures; DPIAs | 72 hours to supervisory authority | Up to 4% of global annual turnover |
| HIPAA Security Rule | United States | Administrative, physical, technical safeguards | Without unreasonable delay (≤60 days under HITECH) | Civil & criminal penalties |
| NIS2 Directive | European Union | Risk management, governance, supply chain security | 24-hour early warning + follow-up | Significant administrative fines |
| FDA Cybersecurity Guidance | United States | Secure design & lifecycle risk management for medical devices | Reporting of device vulnerabilities | Regulatory enforcement actions |

## 1.3. Legal Responsibilities and Liability in Hospital Cybersecurity

Hospitals’ cybersecurity obligations extend beyond technical safeguards; they are grounded in statutory duties, fiduciary responsibilities, professional standards, and tort principles. Increasingly, regulators and courts treat cybersecurity failures as foreseeable risks that may trigger civil, administrative, or even criminal liability. The legal responsibility of hospitals is therefore twofold: (1) proactive compliance and risk mitigation, and (2) reactive accountability in the event of harm.

### 1.3.1. Duty to Protect Patient Data:

Legal obligations to ensure the confidentiality, integrity and availability of employee health records are required by healthcare facilities. HIPAA recognizes this as a requirement for covered entities to implement safeguards (technical; administrative; and/or physical) to protect electronic protected health information (ePHI). The Guardian Data Protection Regulation (GDPR) provides similar types of requirements, namely technical and organizational security measures (32) with respect to ePHI. Moreover, legal scholars have concluded that these requirements also establish an ongoing duty of risk management rather than a one-time compliance activity. Appari & Johnson (2010) have indicated lack of regular risk assessments as being a major deficiency identified by enforcement actions related to non-compliance. The principle of accountability set forth in GDPR requires lawful documentation of compliance, thereby shifting the responsibility of compliance from regulatory response to pre-emptive governance [16].

Risk analysis is an important requirement from a legal standpoint throughout all jurisdictions. The Health Insurance Portability and Accountability Act (HIPAA) mandates regular risk assessments. Health care organizations need to develop structured risk management frameworks, incident detection systems, and controls over the security of their supply chains as required by the General Data Protection Regulation (GDPR) and the NIS2 Directive. The adoption of structured cybersecurity governance models has been shown to positively impact compliance and decrease breach risk. As well, hospitals' cybersecurity maturity is linked to their executive oversight and integration of cybersecurity into their enterprise risk management structures [9]. Breach notification requirements show the legal recognition that cybersecurity failures can have an adverse effect on patients' rights. GDPR requires notification to supervisory authorities within 72 hours. Under HITECH, covered entities must notify affected individuals; within 60 days. Studies assessing health care organization breach disclosures indicate that mandatory reporting laws have increased transparency; however, they have also resulted in increased exposure to litigation and enforcement scrutin. Delayed notification has been considered a sign of inadequate governance by regulatory bodies. Increasingly, hospitals are using cloud service providers and medical device manufacturers. Under HIPAA, Business Associate Agreements (BAAs) define the security responsibilities of each party through contract. Under the GDPR, processors have direct obligations and both parties share liability risk [14].

### 1.3.2. Civil Liability and Negligence

If a plaintiff proves it was negligent by failing to implement appropriate cybersecurity protections, hospitals are liable for their digital breaches under negligence law. A wide range of legal scholarship has pointed to increasing integration of cybersecurity readiness into the overall duty of care of healthcare entities (Martin et al. 2017).

Ransomware attacks that occur on a large scale are being linked to operational disruptions, which will also enhance the viability of claims for foreseeable harm against the various entities. Furthermore, as mandatory notice jurisdictions have been introduced, class action lawsuits resulting from a data breach have greatly expanded in those jurisdictions[14].

Table 2. Administrative and Regulatory Penalties.

| Framework | Enforcement Authority | Penalty Structure |
|---|---|---|
| GDPR | National Data Protection Authorities | Up to €20M or 4% global annual turnover |
| HIPAA | U.S. Office for Civil Rights (HHS) | Tiered civil monetary penalties |
| NIS2 | National cybersecurity regulators | Significant administrative fines |

## 1.4. Ethical and Professional Obligations

Cyberspace has a long history of ethical obligations to keep patients' data confidential and avoid immersing them in harm and maintaining a high degree of professionalism. Due to the digitisation of patient records, healthcare organisations have many more obligations to keep patients safe from harm through proper integration of cybersecurity as part of their clinical ethical frameworks. In addition, many have stated that protecting against cyber incidents, such as data breaches or cyber-attacks, represents the extension of the traditional Hippocratic duty to "do no harm" to patients. This is especially true because cyber incidents can disrupt the ability of healthcare institutions to provide care to their patients safely and effectively. Furthermore, ethical analyses also show that failing to implement cybersecurity measures diminishes patients' trust in hospitals, which is critical to the success of the entire healthcare system. With the advent of ransomware, there continues to be much debate as to the morality of paying attackers to restore clinical access to hospitals; however, the research suggests that such payments perpetuate systemic harm while only providing temporary relief to patients. As a result, hospital governance for cybersecurity should not be considered simply achieving regulatory compliance but should also be seen as a professional and moral obligation inherent in medical ethics and organisational accountability [18].

Effective governance and compliance strategies play a vital role in reducing both legal and operational risks associated with cybersecurity threats to hospitals. Recent research has shown that the compliance of an organization regarding its cybersecurity program is likely to increase as its executives provide oversight and leadership for cybersecurity and the organization embraces cybersecurity as ongoing concern. Establishing structured frameworks (i.e., risk-based governance models and continuous monitoring systems) has been shown to enhance institutional resilience and decrease cybersecurity breach likelihood. Furthermore, organizational culture and staff training related to cybersecurity have a significant impact on compliance outcomes; as human error is found to be one of the largest vulnerabilities in healthcare systems. The combined findings of this research support the assertion that there are no single technical security interventions that will establish sustainable cyber security compliance for hospitals, but rather a collective reliance on board of director accountability, cross-department collaboration, and ongoing assessment of risks to achieve this outcome [19, 20].

## 2. CONCLUSIONS

The nature of hospital cybersecurity has changed dramatically from being purely a technical support role to being a key part of the overall legal, ethical and governance responsibilities of an organization. Hospital's reliance on their digital environments to support their services, e.g., electronic health records, cloud computing, telemedicine platforms and medical devices connected with networks, has resulted in a much larger attack surface. Hospital's cyber-physical systems have become much more complex, and therefore the effect of disruption to the digital environment has much greater potential to adversely affect clinical workflow and patient outcomes. The rapid growth in occurrences and severity of ransomware attacks and large-scale data breaches highlight the fact that failures in cybersecurity are not merely technology-based issues, but rather are direct risks to the safety of patients. Based on this review, hospitals operate in an environment of dense regulatory requirements that are a result of data privacy legislation, cybersecurity regulations, critical infrastructure regulations and medical device oversight legislation. Examples of legal instruments, such as HIPAA, HITECH, GDPR, and NIS2 Directive, place affirmative obligations on healthcare organizations through the requirements for: continuous assessment of risk, implementation of safeguards, documentation of compliance with those safeguards, notification of breaches and oversight of the supply chain. Thus, today’s regulatory framework places greater emphasis on accountability and governance compared to traditional regulatory frameworks that were focused on technical compliance. As an example, organizations must now demonstrate that they use appropriate technical and organizational measures to manage risk on an ongoing basis and build resilience proactively into their organization. Hospitals are subject to considerable financial liability in addition to meeting statutory requirements. Increasingly, courts are interpreting cybersecurity readiness as being part of the duty of care that hospitals owe to their patients. Any foreseeable harm caused by a cyber incident - including delayed care, compromised medical devices and/or identity theft - will potentially enable a patient (or a third-party to the patient) to file suit for negligence. The rise of mandatory breach notice laws has increased transparency but at the same time has raised reputational exposure for hospitals and the risk of litigation. Furthermore, when government regulators consider violations of law, they will assess not only technical security measures but also the governance structure, executive oversight, and documented risk management practices of hospitals in determining potential penalties. Ethics reinforces the legal framework on all aspects of protecting health information of individuals through the use of electronic technology. The duty of confidentiality and a duty of non-maleficence is an extension of the historical ethical commitments within the practice of medicine. Therefore, cybersecurity governance must be consistent with the ethical principles within the standards of the profession and the trust that our patients have placed in us. The decision on whether to pay a ransom to unlock data from a ransomware attack is illustrative of the complex intersections of ethical judgment, legal compliance, and the continuity of hospital operations.

Sustainable hospital cybersecurity requires more than technical controls to be effective through: governance that holds boards accountable; inclusion of cyber security within the enterprise risk management framework; continuous work force training; oversight of supply chain and vendor risks; alignment with recognized cybersecurity standards; and embedding cybersecurity as part of the organizational strategy (rather than only delegating to the IT department). Cybersecurity is now integral to patient safety, institutional integrity, and regulatory compliance in today’s modern health care environment. The evolving digital health technologies will create increasing legal expectations and more effective enforcement. Therefore, hospitals must proactively implement a governance approach that incorporates legal compliance, ethical responsibility, and technical resilience to protect both patients’ interests and the continued viability of their organization.

## REFERENCES

Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. *Cureus, 17*(5), e83614. https://doi.org/10.7759/cureus.83614

Broeders, D. (2016). The secret in the information society. *Philosophy & Technology, 29*(3), 293–305. https://doi.org/10.1007/s13347-015-0203-3

Drolet, B. C., et al. (2017). Electronic communication of protected health information: Privacy, security, and HIPAA compliance. *Journal of Hand Surgery (American Volume), 42*(6), 411–416. https://doi.org/10.1016/j.jhsa.2017.03.004

Grover, P., Kar, A. K., & Davies, G. (2018). “Technology enabled health” – Insights from Twitter analytics with a socio-technical perspective. *International Journal of Information Management, 43*, 85–97. https://doi.org/10.1016/j.ijinfomgt.2018.07.003

Khatoon, Z., et al. (2018). Bacterial biofilm formation on implantable devices and approaches to its treatment and prevention. *Heliyon, 4*(12), e01067. https://doi.org/10.1016/j.heliyon.2018.e01067

Kruse, C. S., et al. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1–10. https://doi.org/10.3233/THC-161263

Martin, G., et al. (2017). Cybersecurity and healthcare: How safe are we? *BMJ, 358*, j3179. https://doi.org/10.1136/bmj.j3179

McCoy, T. H., Jr., & Perlis, R. H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA, 320*(12), 1282–1284. https://doi.org/10.1001/jama.2018.9221

Neprash, H. T., et al. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum, 3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Pinto-Llorente, A. M., et al. (2017). Students’ perceptions and attitudes towards asynchronous technological tools in blended-learning training to improve grammatical competence in English as a second language. *Computers in Human Behavior, 72*, 632–643. https://doi.org/10.1016/j.chb.2017.03.002

Seh, A. H., et al. (2020). Healthcare data breaches: Insights and implications. *Healthcare, 8*(2), 133. https://doi.org/10.3390/healthcare8020133

Tahir, A., et al. (2020). A systematic review on cloud storage mechanisms concerning e-healthcare systems. *Sensors, 20*(18), 5280. https://doi.org/10.3390/s20185280

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Webb, T., & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review, 33*(4), 559–563. https://doi.org/10.1016/j.clsr.2017.03.006

Winarno, I., et al. (2016). Increasing the diversity of resilient server using multiple virtualization engines. *Procedia Computer Science, 96*, 1701–1709. https://doi.org/10.1016/j.procs.2016.08.213

Xiao, B., & Benbasat, I. (2015). Designing warning messages for detecting biased online product recommendations: An empirical investigation. *Information Systems Research, 26*(4), 793–811. https://doi.org/10.1287/isre.2015.0600

Zhao, Y., et al. (2020). Incentive mechanisms for mobile data offloading through operator-owned WiFi access points. *Computer Networks, 174*, 107226. https://doi.org/10.1016/j.comnet.2020.107226