How implementation of cybersecurity practices affects the architectural design of hospital information systems.

Yuan Li
University of Melbourne
yuanli2349@gmail.com

Ruohao Zhao
University of Melbourne
zrh090704@163.com

Yu Dai
University of Melbourne
bxyjdy@163.com

Mengrong Li
University of Melbourne
ginali4303@outlook.com

Xiaoxuan Yan
University of Melbourne
xiaoxuanyan604@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

The globalization of healthcare services and the growing digital infrastructure, with rapid technological advancements, have made hospital information systems (HIS) very vulnerable to cyber threats. However, the exposure to cyber-terrorism becomes more probable as healthcare becomes an integral component of any nation's infrastructure. Our work establishes the significant role of cybersecurity measures in the evolution of infrastructural security in the backdrop of increasing threats. Initially, we provide the basic knowledge of the information architecture in healthcare facilities and determine the responsibility of each lay level. It then examines the cybersecurity challenges that might disrupt the HIS architecture and classifies the cybersecurity upgrades that are often used. In addition, the study reviews several cyber security incidents that have occurred in healthcare systems in recent years and measures the effect of network problems on architecture design, especially changes in communication, domain and application layers. The paper also examines broader strategies incorporating systematic update processes, role-based access control, and encrypting sensitive data aimed at reinforcing the overall cyber-resilience of hospital information systems. In conclusion, this paper presents a holistic plan for the future improvement of the HIS network security architecture which should be able to handle the rapidly growing cyber threats. The framework includes strong defence mechanisms to defend sensitive health data and patients' safety in the digital world, which is becoming more popular.

Keywords: Hospital Information Systems, Cyber Security, Enterprise Architecture

1. Introduction

In recent years, cybersecurity has become increasingly important and critical as more and more organizations have realized that information is the key asset of the company. With the rapid advancement of Information and Communication Technology (ICT) and the growing reliance on IT infrastructure, information security breaches become more tangible and create tremendous impacts on business operations (Cherdantseva & Hilton, 2015). Although cybersecurity measures adopted within organizations, including firewalls, anti-virus protection and regular backups of data, anti-spam software and compliance with cyber security policies, etc, can largely mitigate and minimize the impact of cyber security breaches (Hughes & Stanton, 2006), organizations should be more proactive in ensuring the cyber security. In other words, organizations should take cyber security into the consideration when building their enterprise architecture.

In this research report, to ensure practical relevance and enhance specificity, Hospital Information Systems (HIS) architectures have been selected as the primary domain of the study. The main objective of this research is to identify how the implementations of cybersecurity practices affect the architectural design of Hospital Information Systems. Layers of HIS architecture and the main cyber security issues that existed within the organizations will be introduced respectively. Then, the case analysis will be illustrated in detail, followed by relative recommendations.

2. Hospital Information Systems (HIS) Architecture

The Hospital Information System (HIS) is an integrated system that captures, stores, processes and communicates data and information within healthcare institutions (Pinciroli et al., 2000). This system aims to improve operational efficiency, clinical outcomes and patient care. With the development of information technology applications in the healthcare industry, the functions of HIS have evolved. It transitioned the emphasis from solely administrative tasks to a dual focus on both hospital management and healthcare management (Reichertz, 2006). The comprehensive functions of current HIS allow institutions to make better decision, streamline operational processes and access real-time data.

In order to create value, HIS has a comprehensive architecture that can be categorized into three layers – communication layer, domain layer and technology & application layer.

2.1. Communication Layer

The communication layer plays a critical role in the architecture of HIS. It not only enables data exchange and integration across different departments, but it also allows departments to maintain their autonomy and local data models (Pinciroli et al., 2000). The multi-layered architecture of HIS requires a robust communication layer to support diverse communication needs across different systems. Accordingly, three modes of communication were identified by Reichertz (2006).

- Intra-structural (Ants mode) for communication within a single system.
- Inter-structural (Tarzan mode) for communication across different systems.
- Inter-system (Galactic mode) for communication between entirely different systems.

These allow better data integration, improve the flexibility of information flow and localize the complexity of protocols.

The infrastructure that supports communication within HIS is based on network technologies. The network infrastructure ensures that data is transmitted securely and efficiently, adhering to healthcare compliance and security standards (Pinciroli et al., 2000). It also provides real-time data transmission which improves decision-making.

Moreover, the communication layer standardizes the format for data exchange which maintains data integrity and consistency across different systems (El Azami et al., 2012). It adopts standard protocols, such as Knowledge Query and Manipulation Language (KQML) and XML, for information exchange.

2.2. Domain Layer

The domain layer is described as a hospital functions model for storing or processing various data (Pinciroli et al., 2000 & Winter et al., 2010). This model provides a storage library of hospital information data and allows standardized HIS terminology. It is distributed into different entities, each consisting of object types and tasks (Winter et al., 2001). The main entities will depend on the hospital, and the fundamental structure of basic entities is presented at Figure 1.0

Each of these will have an identifier and description based on attributes, allowing enterprises to create or use entity information (Hübner-Bloder et al., 2005). The integration of the data can provide a comprehensive medical history of each patient. The design of the model helps to better operate and coordinate data within the HIS (Pinciroli et al., 2000).

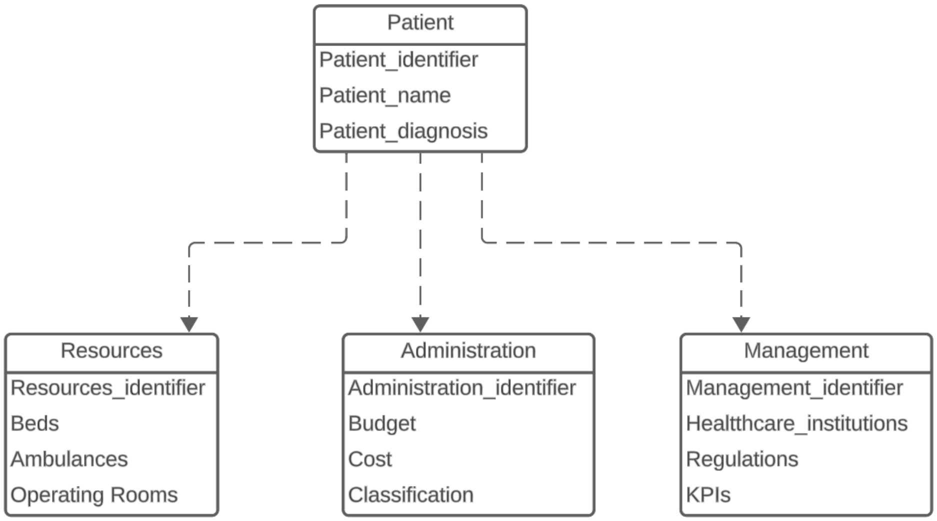

Figure 1.0 Fundamental Structure of Basic Entities

2.3. Technology & Application Layer

The technology and application layer within hospital information systems (HIS) facilitates interaction between institutions and patients (Winter et al., 2010; El et al., 2012). HIS comprises various sub-systems, including the patient administration system (PAS) and Prescription and Drug Management System (PDMS), to support dynamic enterprise functions and maintain data consistency. Each patient is assigned a unique patient identification number (PIN) or master patient index (MPI), along with a case identification number (CIS), enabling better management of patient information and care. These identifiers not only facilitate access to patient information within the HIS but also enable trans institutional HIS to access patient data (Winter et al., 2010). This interoperability allows for the seamless sharing of information across different systems (El et al., 2012). Such systems provide hospitals with efficient and convenient work environments, ultimately enhancing the quality and efficiency of medical services.

3. Cyber Security Issues

As organizations increasingly rely on digital technologies to automate and streamline business processes, analyse and visualize massive amounts of data, drive innovations for further competitive advantages, and better engage with customers, safeguarding sensitive information and digital assets within organizational information systems becomes a critical imperative. The Committee on National Security Systems (CNSS) emphasizes the importance of information security and outlines information security as the safeguarding of data and its crucial components, encompassing the systems and hardware using, storing and transmitting the information (Whitman & Mattord, 2022). This definition is further developed by the computer security industry, C.I.A. triad, which prioritized the protection of the confidentiality, integrity and availability of information assets in storage, processing and transmission (Cherdantseva & Hilton, 2015). In this research report, cyber security is used interchangeably with information security but primarily focuses on data and system aspects under the organizational context, excluding considerations related to hardware protection.

In the digital landscape, cybersecurity issues become increasingly prevalent, posing significant challenges to organizations across various sectors. Whitman and Mattord (2022) classify cybersecurity threats into twelve categories. This research report will focus on the following four categories related to the data and system of an organization.

Espionage or trespass

Espionage and trespass encompass a range of electronic and human activities aimed at breaching the confidentiality of information. A typical example is hackers, who usually use fictional accounts to manipulate networks, systems and data to gain protected information.

Information extortion

Information extortion, or cyber extortion, refers to the actions of gaining unauthorized access to sensitive data. Different from espionage and trespass, information extortion aims at payment or other compromise. For example, ransomware, targeting the host system, denies access to the users, but provides a key for users. Users have to pay to get the key and regain access to the system and data. This is a typical type of information extortion.

Sabotage or vandalism

Sabotage or vandalism describes intentional actions aimed at damaging information systems and businesses and destroying the assets and reputation of organizations. The scale of sabotage and vandalism can vary from localized and minor acts to organized attacks against the organization or even terrorist attacks assaulting civilians or the government.

Software attacks

Software attacks are intentional actions undertaken by individuals or groups who create and implement specialized software with the aim of targeting and compromising computer systems. These attacks often involve the deployment of deceptive software designed to either disrupt the functionality of online systems or covertly infiltrate protected systems for malicious purposes. Examples include malware, viruses and worms.

Other categories of cybersecurity threats include compromises to intellectual property, deviations in the quality of services, forces of nature, human error or failure, technical hardware failures or errors, technical software failures or errors, technological obsolescence, and theft.

4. Case Analysis

4.1. Increasing Cyberattacks on Hospital Information Systems: A Rising Threat

The frequency and scale of cyberattacks, that aim at Hospital Information Systems in the healthcare industry over the course of the previous decade, have become more significant. Attackers usually break through the system from the Communication layer, destroy the process and network of each branch system in the technology and application layer, and steal data information in the domain layer. In particular, ransomware, which compromises hospitals' digital systems. A ransomware cyberattack against an Indiana hospital system in 2018 caused $55,000 in damage (Kumar et al., 2021). Cyberattacks have occurred during a period when ransomware attacks are on the rise, increasing three times from 2015 to 2016 alone (Millard, 2017).

If a cyber assault is launched against the technology and application layer, hospital operations may be disrupted through the shutdown of many services. From surgery to drug delivery, targets are advanced equipment that includes blood product refrigerators, imaging equipment, and electronic health records. Critical systems that support the operation of the hospital such as heating, ventilation and air conditioning (HVAC) are also targets (Argaw et al., 2020). In the context of extreme or conflict situations, hospitals are particularly vulnerable, because malware that penetrates systems covertly could still be around even after a long time, potentially being activated when treatment is needed most (for example, after natural or man-made accidents). The WannaCry international attack in 2017 was unprecedented in scale. National Health System hospitals in the UK were hit by the WannaCry ransomware attack, which forced them to delay treatment plans and even reroute ambulances due to a lack of access to Hospital Information Systems (Millard, 2017). In Portugal's national health system, WannaCry's cyberattack mainly affected medical assistance services at Garcia da Horta Hospital (HGO). It is estimated that a single attack can cost a hospital up to $7 million, which can lead to long-term harmful losses in reputation, activities, and revenue for hospitals and health institutions (Portela et al., 2023). In addition, on May 14, 2021, hackers launched a malicious cyberattack against Ireland's public healthcare system, the Health Service Executive. The cyberattack swept over the Irish National Orthopaedic Registry (INOR) causing a thorough shutdown of all national healthcare computer systems including INOR, and disruption to most of the hospital activities (Russell et al., 2023).

In addition, when it is customer or patient data in the domain layer that is stolen by criminals, the decision to pay the ransom is confusing for healthcare organizations. Law enforcement and security professionals maintain that the most appropriate action is not to pay ransom (Minnaar & Herbig, 2021). They argue that payments will stimulate cybercriminals to launch more ransomware malware attacks (Minnaar & Herbig, 2021). However, medical institutions that do not pay the ransom are at risk of having their customer and patient data information compromised, and they may be fined by regulators. The US healthcare system imposes very high standards for privacy, and any patient data breach can be heavily fined (Minnaar & Herbig, 2021). Hence, small and medium-sized healthcare organizations have been reluctant to disclose the news of data breaches for the sake of avoiding fines, which is money they prefer to spend on data redemption. The survey found that more than half of victims who were targeted by ransomware attacks paid a ransom to restore access to stolen data. However, of those who did pay, 17% did not receive any data (Kaspersky, 2021).

4.2. Inherent Vulnerabilities in Hospital Information Systems: Risks and Implications

On the other hand, the rapid development and deployment of Hospital Information Systems worldwide have indeed brought about significant benefits in terms of operational efficiency and patient care. However, due to the immaturity of the development of HIS, the system complexity, and the sensitive nature of the data it handles, its defence system is not complete and is vulnerable to various threats which will compromise its integrity, availability, and confidentiality (Smith & Eloff, 1999). They can negatively impact organizational operations, information assets, individuals, organizations, and even national interests.

Hospital Information Systems are typically connected to the Internet, various medical devices, third-party service providers, and external partners. This extensive connectivity increases the attack surface the system faces, making it easier for hackers to find entry points. This happens all the time, especially in Iran. In 2014, Iran's integration of Hospital Information Systems with the national electronic health record system through the public internet increased vulnerability to cyberattacks, and exposed gaps in the protection of patient data (Zarei & Sadoughi, 2016). The absence of stringent protocols for data confidentiality led to potential privacy risks. Furthermore, due to geopolitical tensions related to Iran's nuclear program, the hospital systems faced sophisticated cyber threats like Stuxnet and Flame, impacting healthcare operations and national security. Such disruptions will have dire implications for patient care and safety.

Besides, Hospital Information Systems store vast amounts of sensitive data, including patient medical records, personally identifiable information, and financial information. This data is highly valuable to hackers and can be used to carry out identity theft, financial fraud, or extortion attacks, making Hospital Information Systems an important target for hackers. In 2008, a cyberattack targeted a hospital in Shenzhen, China, resulting in the disclosure of healthcare information of pregnant women. The attack compromised up to 40,000 items of data, including names, baby's birth dates, home addresses, and mobile numbers. This information was compiled into disks and sold to businesses for marketing purposes, such as promoting baby-related products and services. The data breach caused significant distress to the victims due to the intrusive nature of the marketing activities (He & Johnson, 2012). The victims realized that the information provided during hospital registration had been misused, leading to both the loss of confidential data and personal privacy invasion. Since Hospital Information Systems are relatively new in China, managers initially prioritized business functionalities over system security. This kind of focus resulted in inadequate attention to security measures, leading to abuses of privileges and unauthorized access to the systems.

Moreover, software and hardware in Hospital Information Systems may have preliminary fixes that hackers can exploit to gain system access or execute malicious code. Hospital Information Systems often use a variety of different software and technologies, so vulnerability fixes and system updates can be lagging, leaving the system vulnerable to attacks. In April 2023, NationsBenefits, a provider of supplemental benefits administration services to healthcare plans in the USA, reported a significant data breach affecting over 3 million individuals. The breach was traced back to a known vulnerability in a managed file transfer solution within their system (Freestone, 2024). The compromised data included a range of sensitive information, such as names, demographic details, health insurance numbers, social security numbers, dates of service, phone numbers, and provider names, leading to an increased risk of identity theft and fraud for those affected.

Therefore, the escalation in the frequency and intensity of cyberattacks on hospital information systems over the past decade highlights a significant threat to the healthcare industry. These attacks often infiltrate systems through various layers, leading to disrupted operations and stolen data, including sensitive patient information. The repercussions of such breaches are not only immediate but can also have long-lasting effects on an institution’s reputation and financial stability. Furthermore, the inherent vulnerabilities of these systems, due to their complexity and rapid development, add another layer of risk. These vulnerabilities provide numerous opportunities for attackers, making Hospital Information Systems prime targets for cybercriminal activity and potential national security concerns.

5. Key Cybersecurity Challenges in Hospital Information Systems Architecture

The iteration of the domain layer typically has a low change rate (Rod Dilnutt, 2024, slides for Seminar 5 of ISYS90043, slide 5), necessitating regular system updates to address evolving cyber threats. However, the lack of timely updates poses significant cybersecurity risks within the HIS architecture. Attackers often exploit vulnerabilities in the communication layer to breach the system, highlighting the critical need for robust security measures. A well-designed infrastructure is essential to mitigate these vulnerabilities and ensure the integrity of the HIS.

Lack of security updates and Lack of control access

A case study by Millard (2017) underscores the impact of malware on HIS architecture, posing risks not only to patient data but also to the overall hospital system and patient outcomes. For instance, malware attacks on the technology and application layer can lead to inaccurate outcomes, hindering doctors' ability to analyse and provide accurate diagnoses. Additionally, inadequate access control within the HIS, necessitated by the diverse user groups such as patients, nursing staff, and third parties, further compromises data security and confidentiality.

Lack of sensitive data protection regulations

These cybersecurity challenges highlight a pressing need for more comprehensive sensitive data protection regulations within the HIS technology layer and domain layer from the Zarei and Sadoughi Case study (2016). Clarification is required on user access privileges and data modification capabilities, alongside robust mechanisms for system recovery from security breaches. Addressing these regulatory gaps is crucial for enhancing the protection of sensitive healthcare information and safeguarding the confidentiality, integrity, and availability of data within the HIS.

6. Strategies for Enhancing Security in Hospital Information Systems Architecture

To effectively mitigate the vulnerabilities in the current Hospital Information Systems, it is imperative to initiate a robust and systematic update process in all layers. This process should ensure that all system components, such as operating systems, applications, and network devices, are consistently updated with the latest security patches. By utilizing automated tools to continuously monitor emerging security vulnerabilities, organizations can deploy necessary patches swiftly as new threats are disclosed, thereby minimizing potential exposure windows.

Moreover, implementing a strict role-based access control (RBAC) system in the technology & application layer is crucial. This system should rigorously define and enforce user access rights based solely on individual responsibilities and the essential need-to-know basis (Xu et al., 2020). Also, to bolster security, multi-factor authentication should be mandatory for all users accessing sensitive data, adding an extra layer of security and significantly reducing the risk of unauthorized access. Additionally, in the domain layer, the encryption of sensitive data, whether in storage or transit, must adhere to the highest industry-standard encryption protocols and algorithms. For particularly sensitive information, such as medical records and personal identification data, adopting advanced encryption standards is paramount to ensure that data remains secure from interception or breaches.

Furthermore, to protect critical systems and data storage areas from external threats, it is necessary to isolate these systems from the wider network, especially in the communication layer. Employing comprehensive firewall configurations and robust intrusion detection systems (IDS) will help safeguard network boundaries (Ozkan-Okay et al., 2021). Additionally, implementing thorough internal network monitoring systems can provide early detection of any unusual or potentially malicious activity within the network, enabling a quicker response to internal threats and abnormalities. By enhancing these protective measures, Hospital Information Systems can be secured against a wide range of cyber threats, ensuring the privacy and integrity of sensitive health data.

7. Conclusion

This research has examined the critical role of cybersecurity in protecting HIS from the growing landscape of cyber threats. The increasing digitization of healthcare services has made HIS vulnerable to a wide range of cybersecurity issues. It is found that the existing HIS architecture is very complicated, but we can propose an intermediary architecture to integrate multiple databases with different structures. Our architecture is an infrastructure that is divided into three levels: the communication layer, the domain layer, and the application layer. However, in the process of summarizing the architecture, we found that most HIS architectures have critical vulnerabilities that can lead to cyberattacks. These include the lack of timely software and system updates, inadequate access controls, and insufficient data protection regulations around sensitive healthcare data. The consequences of such breaches are severe, risking patient safety, operational disruptions, financial losses, and reputational damage to healthcare institutions. To address these cybersecurity challenges, this research recommends implementing a systematic process for security updates, enforcing role-based access controls and encryption for sensitive data, and utilizing network segmentation with monitoring at boundaries. These findings align with recommendations from prior literature emphasizing the need for integrated systems in healthcare to improve patient outcomes and operational efficiency. Additionally, our HIS architecture is scalable, implementing the system's security update process without impacting its native functionality or changing the mission of healthcare professionals. By adopting the recommended solutions, healthcare institutions can better protect their critical information systems, ultimately ensuring the safety and privacy of patient data and the resilience of healthcare services. Our intermediary architecture facilitates the full integration of different systems in the hospital, and it facilitates the integration of Healthcare Information Systems.

8. Limitations

While this research provides valuable insights into cybersecurity measures for HIS, there are three main limitations that should be acknowledged. Firstly, this research primarily focuses on the cybersecurity issues associated with data and software, neglecting the human aspect of cybersecurity vulnerabilities. Secondly, this research relies on a limited number of case studies. The narrow range of cases analysed may not capture all the cybersecurity challenges affecting HIS architectures. Lastly, since the enterprise architecture lifecycle of HIS spans several years, the proposed security framework may struggle to adapt at the same pace as the evolving cybersecurity threat landscape. Thus, the suggestions for future research are to explore more cybersecurity cases within HIS architectures and conduct a comprehensive analysis of a broader range of threats. Further, frameworks or methodologies should be developed to assess the dynamic impact of emerging threats, ensuring the long-term resilience and effectiveness of cybersecurity measures for HIS.

9. Reference

Argaw, S., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(1). https://doi.org/10.1186/s12911-020-01161-7

Azami, I. E., Malki, M. O. C., & Tahón, C. (2011). Integrating hospital information systems in healthcare institutions: A mediation architecture. *Journal of Medical Systems, 36*(5), 3123–3134. https://doi.org/10.1007/s10916-011-9797-8

Cherdantseva, Y., & Hilton, J. (2014). Information security and information assurance. In *Advances in Systems Analysis, Software Engineering, and High Performance Computing* (pp. 167–198). https://doi.org/10.4018/978-1-4666-4526-4.ch010

Dilnutt, R. (2024). Lecture notes, ISYS90043, Seminar 5, The University of Melbourne.

Freestone, T. (2024). Managing private content exposure risk in 2024. *Network Security, 2024*(2). https://doi.org/10.12968/s1353-4858(24)70005-1

He, Y., & Johnson, C. W. (2012). Generic security cases for information system security in healthcare systems. *7th IET International Conference on System Safety, Incorporating the Cyber Security Conference 2012*. https://doi.org/10.1049/cp.2012.1507

Hübner-Bloder, G., Ammenwerth, E., Brigl, B., & Winter, A. (2005). Specification of a reference model for the domain layer of a hospital information system. *International Journal of Medical Informatics, 116*, 497–502. https://pubmed.ncbi.nlm.nih.gov/16160306

Hughes, M., & Stanton, R. (2006). Winning security policy acceptance. *Computer Fraud & Security, 2006*(5), 17–19. https://doi.org/10.1016/s1361-3723(06)70358-x

Kaspersky. (2021). Consumer appetite versus action: The state of data privacy amid growing digital dependency. *Kaspersky Consumer IT Security Risks Report 2021*. Retrieved May 4, 2024, from https://media.kasperskydaily.com/wp-content/uploads/sites/92/2021/03/16090300/consumer-appetite-versus-action-report.pdf

Kumar, P., Gupta, G. P., & Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Computer Communications, 166*, 110–124. https://doi.org/10.1016/j.comcom.2020.12.003

Millard, W. B. (2017). Where bits and bytes meet flesh and blood. *Annals of Emergency Medicine, 70*(3), A17–A21. https://doi.org/10.1016/j.annemergmed.2017.07.008

Minnaar, A., & Herbig, F. J. W. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology, 34*(3), 155–185. https://doi.org/10.10520/ejc-crim_v34_n3_a1

Ozkan-Okay, M., Samet, R., Aslan, Ö., & Gupta, D. (2021). A comprehensive systematic literature review on intrusion detection systems. *IEEE Access*, *9*, 157727–157760. https://doi.org/10.1109/access.2021.3129336

Pinciroli, F., Marchente, M., Combi, C., Fava, D., Brambillaschi, G., & Pedrazzi, A. (2000). TEODOLINDA: A communication architecture for hospital information systems. *Computer Methods and Programs in Biomedicine*, *62*(1), 59–68. https://doi.org/10.1016/s0169-2607(99)00052-8

Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic impact of a hospital cyberattack in a national health system: Descriptive case study. *JMIR Formative Research*, *7*, e41738. https://doi.org/10.2196/41738

Reichertz, P. L. (2006). Hospital information systems—Past, present, future. *International Journal of Medical Informatics*, *75*(3–4), 282–299. https://doi.org/10.1016/j.ijmedinf.2005.10.001

Russell, S. P., Fahey, E., Curtin, M. S., Rowley, S., Kenny, P., & Cashman, J. (2023). The Irish National Orthopaedic Register under cyberattack: What happened, and what were the consequences? *Clinical Orthopaedics and Related Research*, *481*(9), 1763–1768. https://doi.org/10.1097/corr.0000000000002643

Smith, E., & Eloff, J. H. P. (1999). Security in healthcare information systems—Current trends. *International Journal of Medical Informatics*, *54*(1), 39–54. https://doi.org/10.1016/s1386-5056(98)00168-3

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (6th ed.). Cengage Learning.

Winter, A., Brigl, B., & Wendt, T. (2001). A UML-based ontology for describing hospital information system architectures. *PubMed*, *84*(Pt 1), 778–782. https://pubmed.ncbi.nlm.nih.gov/11604843

Winter, A., Haux, R., Ammenwerth, E., Brigl, B., Hellrung, N., & Jahn, F. (2010). Architecture of hospital information systems. In *Health Information Systems* (pp. 75–183). Springer. https://doi.org/10.1007/978-1-84996-441-8_6

Xu, J., Yu, Y., Meng, Q., Wu, Q., & Zhou, F. (2020). Role-based access control model for cloud storage using identity-based cryptosystem. *Journal on Special Topics in Mobile Networks and Applications/Mobile Networks and Applications*, *26*(4), 1475–1492. https://doi.org/10.1007/s11036-019-01484-4

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy*, *75*. https://doi.org/10.2147/rmhp.s99908