Enhancing Cyber Resilience of Smart hospitals against Ransomware attacks

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Chukwuka Onyekwelu

Supervisors:
Dr. Seppo Virtanen (University of Turku)
Jolly Trivedi (University of Turku)

May 2026

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Chukwuka Onyekwelu
Title: Enhancing Cyber Resilience of Smart hospitals against Ransomware attacks
Supervisor(s): Seppo Virtanen, Jolly Trivedi
Date: 26.05.2026

The increased addition of Internet of Things (IoT) devices in connected medical technologies and electronic medical record systems into today's healthcare has created smart hospitals where clinical work and digital connections are closely linked. This connection between traditional healthcare and technology has greatly improved health services and care in this century. However, it also brings big security risks and a larger, more often targeted attack surface area. Ransomware has become one of the most harmful cyber threats to healthcare, with cases showing it can disrupt clinical services, endanger patient safety, and in worst cases cause death and large financial and legal problems.

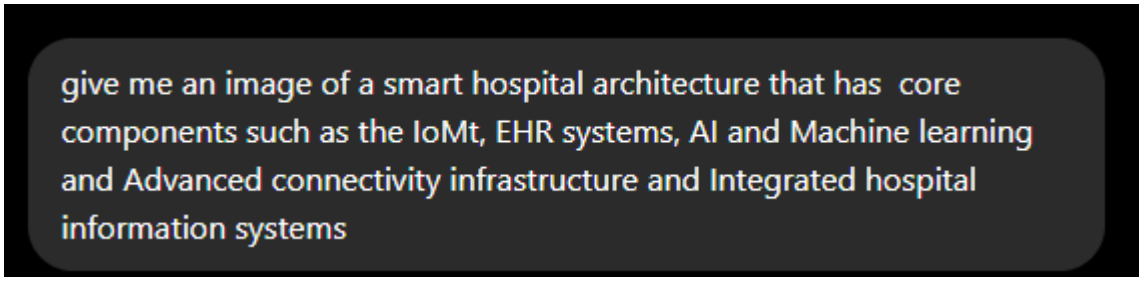
This thesis provides a thorough review of ransomware threats in smart healthcare systems by combining existing research, cybersecurity guidelines, and real incident data to create a clear and evidence-based analysis. It focuses on the different ransomware threats affecting hospitals, evaluates how well current cybersecurity standards and defences work against these threats, and compares healthcare security with other critical infrastructure sectors. Through detailed gap analysis, the thesis points out ongoing weaknesses in both research and practical work, shown by the lack of a unified cyber resilience model that considers the special links between clinical workflows and digital systems in healthcare.

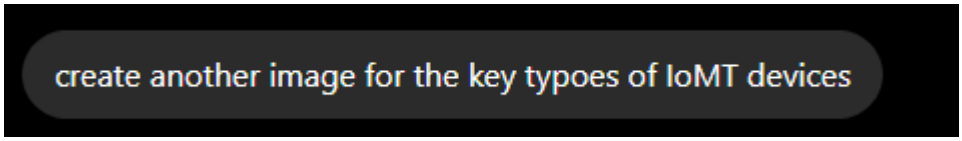
Based on these findings, the thesis offers its main contribution which is a set of specific policy recommendations designed for different groups in the healthcare sector including healthcare providers and managers, policymakers and regulators, technology developers and sellers, and the public. Rather than providing generic guidance, the recommendations address the distinct responsibilities, capabilities, and vulnerabilities of each stakeholder group to help them know the right steps to take when facing ransomware incidents in hospitals. In broader terms, this work adds value by gathering scattered literature, highlighting key research gaps, and turning academic knowledge into practical policy advice, providing a timely and organized resource for those working to protect smart hospitals from growing ransomware threats.

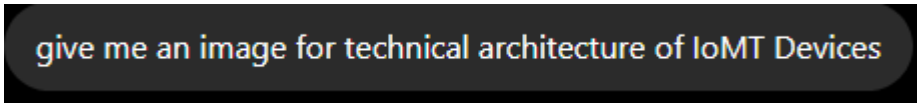
Key words: smart hospitals, ransomware, Internet of things, cyber threats, IoMT, EHR, Cyber resilience, cyber security, healthcare cybersecurity, patient safety, compliance, OEMs (Original equipment manufacturers)

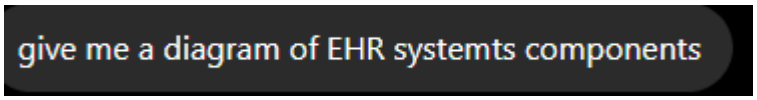
Declaration of the use of AI

Artificial Intelligence (AI) tools were used for proofreading and figure generation. ChatGPT was used to generate Figures 1–5. The prompts used to generate these figures are listed below.









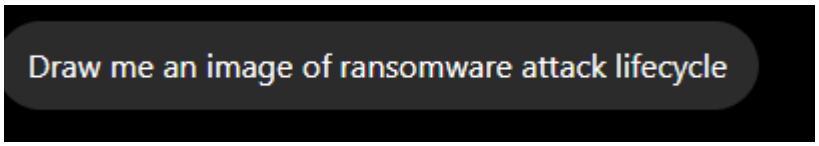


Table of contents

1 Introduction

The expansion of the global population, coupled with heightened expectations for effective treatments and an overall improved quality of life, is exerting mounting pressure on healthcare systems. Consequently, healthcare remains one of the foremost social and economic challenges on a global scale, demanding innovative and advanced solutions from the fields of science and technology [1]. Due to these demands since the early 1990s, Information and Communication Technologies (ICTs) have significantly enhanced access, efficiency, and the quality of nearly every healthcare process. Consequently, the term eHealth, referring to the use of Information and Communication Technologies (ICTs) in the healthcare sector, has gained widespread acceptance [2]. In fact, eHealth has attracted significant interest from both the public and private sectors, leading to unparalleled levels of investment in research and financial support.

1.1 Background and Motivation

The healthcare Industry is going through a major digital shift, with smart hospitals leading the way. These hospitals use technologies like IoT devices, artificial intelligence, electronic health records, connected medical devices, and automated systems to improve patient care, increase efficiency, and help with data-driven decisions [1]. This shift has fundamentally changed healthcare delivery by allowing for real-time patient monitoring, remote diagnostics, predictive analytics, and smooth information exchange across separated healthcare networks [3].

The increased connectivity and digitization used in smart hospitals have helped to create an increased attack surface area for cyber threats, making healthcare institutions particularly exposed to advanced cyberattacks. From these threats, ransomware has surfaced as one of the deadliest types of cyberattack that affects healthcare organizations. According to H. T. Neprash et al. [4], there are reports that show that ransomware attacks disrupt the delivery of care by making computers and electronic health records unusable or encrypted.

There are some statistics to back up this claim as seen in a journal by Thomas Slayton which states that the number of healthcare organizations that were affected by ransomware increased from 34% in 2021 to 67% in 2024 [5]. 2024 was also the year that healthcare organizations faced their most expensive data breaches when compared from 2019 to date, with the average cost of a data breach amounting to $7.42 million per incident, while total losses across the industry because of ransomware-related incidents downtime exceeded $21.9 billion [6]. This

statistic proves that ransomware incidents in the healthcare Industry can lead to serious financial risks if not addressed.

The escalating cybersecurity risks faced by smart hospitals are among the primary motivations for this thesis. The risks arising from ransomware-related incidents have been on the increase on a yearly basis and more needs to be done to fully mitigate against these risks. In the first nine months of 2025, two hundred and ninety-three (293) documented ransomware incidents affecting hospitals and care providers were identified along with one hundred and thirty (130) attacks targeting healthcare organizations [7].

These incidents do not only cause financial damage to the hospitals but can also lead to postponed treatments, rerouted emergency services, cancelled surgical operations, and in some instances, negative effect in the life of patients [8]. The ransomware attack on Change Healthcare in February 2024, which had a financial impact of $2.9billion exposed the health information of 100 million individuals and resulted in significant losses for UnitedHealth Group [9].The billing cycles for healthcare providers were impacted as a result of the ransomware attack and this shows the impact that a single incident can have in an increasing globally interconnected healthcare infrastructure.

Although IoT devices have many advantages when used in the hospital, the devices also come with many vulnerabilities [10]. In 2025, IoMT devices averaged 6.2 security flaws per device with 60% of these devices running outdated systems. For medical IoT devices, they mostly often have weak security features, run on old and unsupported operating systems, and it is very difficult in applying security updates on the devices without causing downtime in critical clinical operations.

According to Z. Amos [11], 88 % of healthcare organizations experienced at least one data breach in the last two years due to weaknesses in their connected devices. These devices, provides several entry points for attackers to access hospital networks [12]. Because of how connected a smart hospital network is, a cyber breach in one of the components can quickly spread across all other devices in the same network if not quickly mitigated [13].

The COVID-19 pandemic showed the importance of strong cybersecurity culture in the health care industry. While hospitals were adopting things like remote patient monitoring due to the

pandemic, cybercriminals took advantage of this and launched different types of attacks on an already stretched healthcare system [14]. In Verizon's 2025 data breach investigation report, Ransomware was identified as the leading cause of healthcare data breaches [15]. This time frame clearly showed that cybersecurity in healthcare is not just a technical issue, it is a crucial public health and patient safety concern that requires immediate, collaborative action from all parties involved [16].

1.2 Problem Statement

The central issue is that while the problem of smart hospitals and the threats that ransomware poses to them is recognized, the current frameworks for cybersecurity in the healthcare Industry do not meet the challenges of protecting the healthcare Industry's critical infrastructure.

While there is an increase in the number of trainings on cybersecurity threats in the health care sector, there are still significant gaps that remains in addressing and explaining the different issues that healthcare organizations face in mitigating against ransomware attacks. Current frameworks (HIPAA, ISO27001), standards and regulations do not fully provide guidance and recommendations on how to mitigate against the unique needs of a smart healthcare environment [17].

In the healthcare Industry, mitigating against cyberthreats such as ransomware is done in a reactive instead of a proactive manner whereby vulnerabilities are remediated as they arise instead of a proactive approach that provides a clear and easy path to fully address the challenges [18]. The reactive method used by healthcare organizations creates significant gaps in the defensive systems and does not fully mitigate against the threats and risks that arise from ransomware attacks.

The level of investments in security solutions and staff is not in tandem with the risk levels experienced in the healthcare Industry. They tend to focus on protection of "low level assets" while the critical infrastructures are not fully protected [19]. Communication and collaboration among different stakeholders working in the healthcare organization is also another challenge faced in the health care industry. According to G. Miller [20], in order for a hospital to have an effective cybersecurity plan, there needs to be synergy among different stakeholders in a hospital environment. Because these stakeholders often work in silos, it leads to collaboration gaps in the healthcare Industry.

While academic research has developed important theoretical information on healthcare cybersecurity, there is still a huge gap between the theoretical knowledge and the practicalities involved in the healthcare environment. It is more prevalent in healthcare environment with limited resources. Different solutions have been recommended ignoring specific operational challenges that faces a modern healthcare environment such as budget constraints and the ever-evolving regulatory landscape that health care must adhere to it e.g. HIPAA. Because of these issues and the gaps identified between theoretical and practical healthcare, the effectiveness of cybersecurity advancement is not fully complete [21].

According to H. Landi [22], Healthcare organizations are dealing with an ever evolving and dynamic ransomware environment because attackers are not only focused on just encryption, but they are also focused on data extortion. Because of this, the number of ransomware attacks that involves extortion has increased. The risk assessment methods today do not fully address the wide number of ransomware threats in smart hospitals, especially regarding their effects on patient safety, clinical outcomes, operational stability, and the organization's reputation [23].

Traditional cybersecurity risk assessments mainly concentrate on data confidentiality and financial effects, failing to sufficiently consider the availability and integrity needs that are essential for healthcare operations and patient safety [24]. Smart hospitals often operate in difficult and mixed hybrid settings that implement and integrate advanced technologies with older medical devices and information systems. It is very difficult for these older medical devices to be upgraded or patched without causing disruptions to patient care [25]. A statistics data seen in [26] further support this claim. It is also said that attackers frequently exploit these legacy devices to gain initial entry and maintain a presence in hospital networks [27].

1.3 Research Objectives

This Master's thesis provides recommendations for different stakeholders in the healthcare sector on how to be cyber resilient against ransomware attacks and it also provides a cyber-resilience model that can be used by a smart hospital in the 21st century.

1.4 Scope and Significance

The scope of this Master's thesis is focused on ransomware threats that affects a smart hospital setting in a highly advanced healthcare system. The thesis looks into smart hospital technologies such as IoT medical devices (patient monitoring systems, infusion pumps, ventilators, and

diagnostic tools), electronic health record systems, picture archiving and communication systems (PACS), hospital information systems (HIS), laboratory information systems (LIS), pharmacy management systems, building management systems, as well as the network infrastructure, security systems, and middleware that link and integrate these elements. It creates a correlation between clinical technologies and operational technologies used in a smart hospital. It also focuses on ransomware attacks and their different forms, such as traditional file-encryption ransomware, double extortion schemes. It also looks at the ransomware life cycle from the first stage to the last stage.

The study provides an outlook to relevant stakeholders in a healthcare setting and how they are affected by cybersecurity incidents. While the focus area is on hospitals located in highly advanced and developed nations, it can also be beneficial to hospitals located in developing nations and third world countries that are still experiencing some level of digital improvements. The scope is focused on the current situation of ransomware threats from the year 2020 to present day today.

2 Related Work

2.1 Evolution of Smart Healthcare Infrastructure

The change from traditional hospitals to smart healthcare facilities is one of the biggest technological changes in modern medicine. This shift has been fuelled by improvements in computing power, wireless connectivity, sensor technology, and data analytics, which together allow for the integration of digital technologies in healthcare delivery [28].

2.1.1 Historical development of healthcare digitization

The digitization of healthcare started in the 1960s with initial efforts in electronic record-keeping. The Mayo Clinic in Rochester, Minnesota, was one of the first major health systems to adopt electronic health records during this time, although high costs initially restricted this to well-funded academic medical centres and government-supported health systems [29]. These early plans became the foundation for greater improvements in the healthcare information technology. Dr. Lawrence Weed in 1968 introduced the problem-oriented medical record (POMR), making an important discovery in systematic patient documentation [30].

The POMR provided an important way to arrange patient data around unique clinical issues, providing the building blocks that will later impact the design and creation of electronic health records. The method used focused on the thoroughness, organization, and problem-centred documentation, which continues to be important in modern EHR (Electronic Health Records) systems. The electronic health records systems was created for the first time in the 1970s.

Clement McDonald and his team at the Regenstrief Institute in Indianapolis created the Regenstrief Medical record systems in the year 1972 which addressed some of the key issues in database designs and system interoperability [31]. They understood that patients always leave incomplete medical information across different providers, leading to disintegrated records that hardly integrate due to incompatible systems. Their efforts in database design and data standardization laid the groundwork for future EHR advancements.

During this same period, a group known as the Veterans Administration created one of the earliest large-scale EHR systems that they later developed into the Veterans Health Information

System and Technology Architecture (VistA) [29]. Their system showed that extensive electronic health records can be developed and created in a large healthcare organization offering tangible knowledge and technical know-how for a national adoption in the United States of America.

2.1.2 Modern Smart Hospital Architecture

Smart hospitals in this century have an advanced architectural design as compared to the Initial electronic record system that was developed in the 1970s. For a hospital to be called a smart hospital, it makes use of different technological systems such as IoT devices, EHR, AI etc. to offer better health services to patients [28]. Figure 1 provides some different components that makes up the smart hospital architecture.

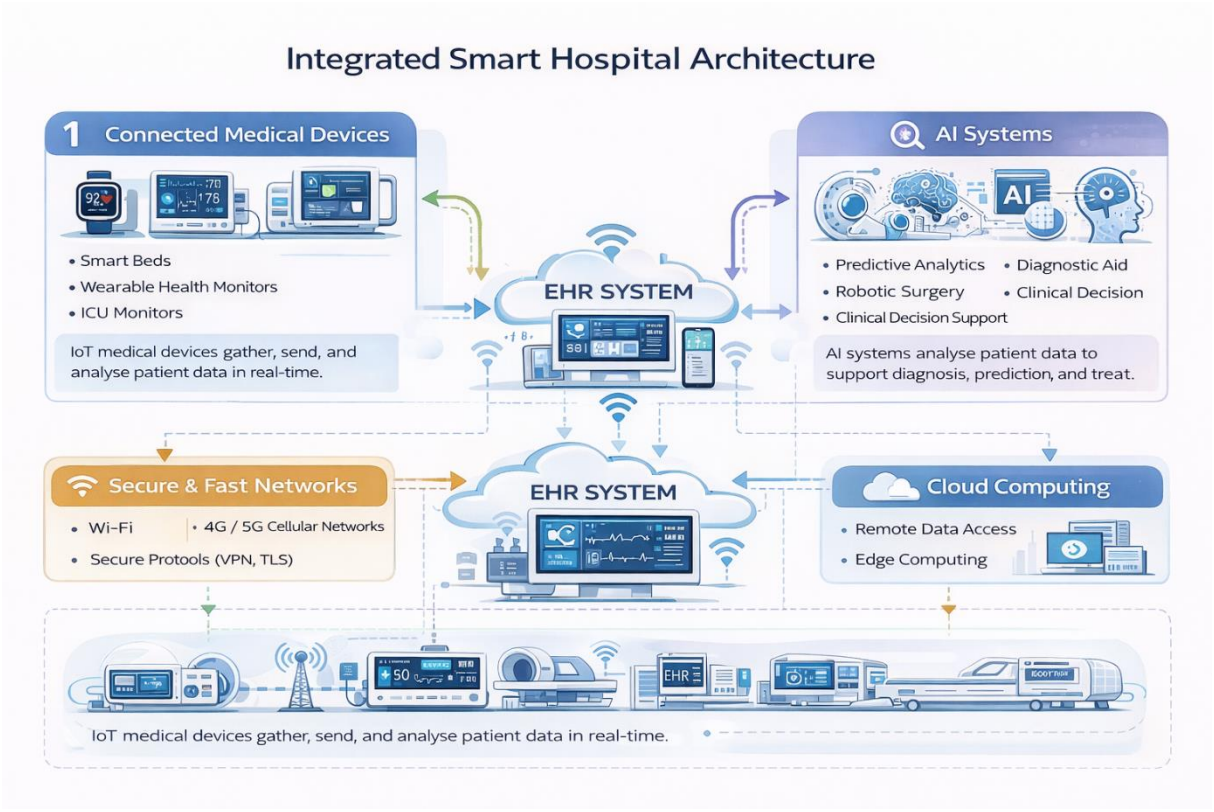


Figure 1 A simple smart hospital architecture source: Figure generated with LLM (ChatGPT 5.5)

In the architecture, Smart hospitals use large networks of connected medical devices that gather, send, and analyse patient data in real-time [32]. Some of these devices are smart beds, wearable health monitors, etc. These devices help doctors and nurses to better administer care and

monitor patients remotely [33]. Every smart hospital must have an EHR (Electronic Health Records) systems which helps to ensure that every detail about a patient is available in an electronic format and readily available online [34]. The change from paper records to electronic ones gained traction after the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, which offered financial incentives for the meaningful use of certified EHR technology [35]. The smart hospital environment also makes use of AI systems for better management of patient data.

AI systems process large amounts of patient data to gain useful insights, enhance diagnostic precision, and support tailored treatment plans [36]. In smart hospitals, AI applications feature predictive analytics for monitoring patient decline, automated image evaluation for radiology and pathology, natural language processing for clinical records, and reinforcement learning for robotic surgery assistance [37]. Sophisticated AI systems enhance resource use by examining real-time data from connected devices, reducing congestion, and facilitating patient movement within the hospital [38].

For smart hospitals to share health data real-time across devices, systems and within different healthcare providers, they must use fast network systems like Wi-Fi and 4G and 5G cellular networks [39]. The increased usage of 5G technology will help with advanced features like remote surgeries and edge computing for local data handling [36]. With Cloud computing, patient and hospital information can be accessed from anywhere which will help with care co-ordination among different health networks and hospitals [40]. Smart hospitals integrate different components as seen in figure 1 that allows for less mundane and operational tasks such as decrease in manual data entry, reduction of transcription errors, etc. [41].

2.1.3 Benefits and Operational Impact

The usage of smart hospital components has led to new developments in the different areas of healthcare. One of such areas is in real-time remote monitoring which helps in identifying health issues as they occur and proactive medical responses [33]. Tasks that were manually done before are now automated and this helps reduce the chance of human errors and helps to improve and manage human resources effectively [42].

Smart hospitals components have helped with things like telemedicine and remote monitoring services. This service makes healthcare more accessible beyond the hospital environment, and

this helps in the management of severe conditions and increases health outcome for patients [39]. One of such benefits of Smart hospital technologies is the ability to create personalized treatment plans based on the patient traits and reactions [38]. Sheba Medical Centre in Israel has been accepted globally as an example of a healthcare centre that has implemented smart hospital infrastructure. The hospital uses AI for patient triage and IoT for remote monitoring. These implementations have led to less hospital admission and quick and fast interventions in critical care situations [38]. The Mount Sinai health system is also another example. They hospital used AI and IoT monitoring system in their critical care units and this resulted in a 35% decrease in cardiac arrest incidents, which shows the importance of smart technologies in an healthcare environment.

2.2 IoT Devices and Connected Medical Technologies

The increase of the usage of Internet of Medical Things (IoMT) devices has many benefits to the health sector. While the benefits of this are enormous, it also leads to more vulnerabilities in the healthcare environment. In this section, the landscape of IoMT technologies, their clinical applications, and the security challenges they introduce are discussed.

2.2.1 Categories and Applications of IoMT Devices

Medical IoT devices varies across different categories with each serving a unique function within the smart hospital environment. The categories can be seen in figure 2

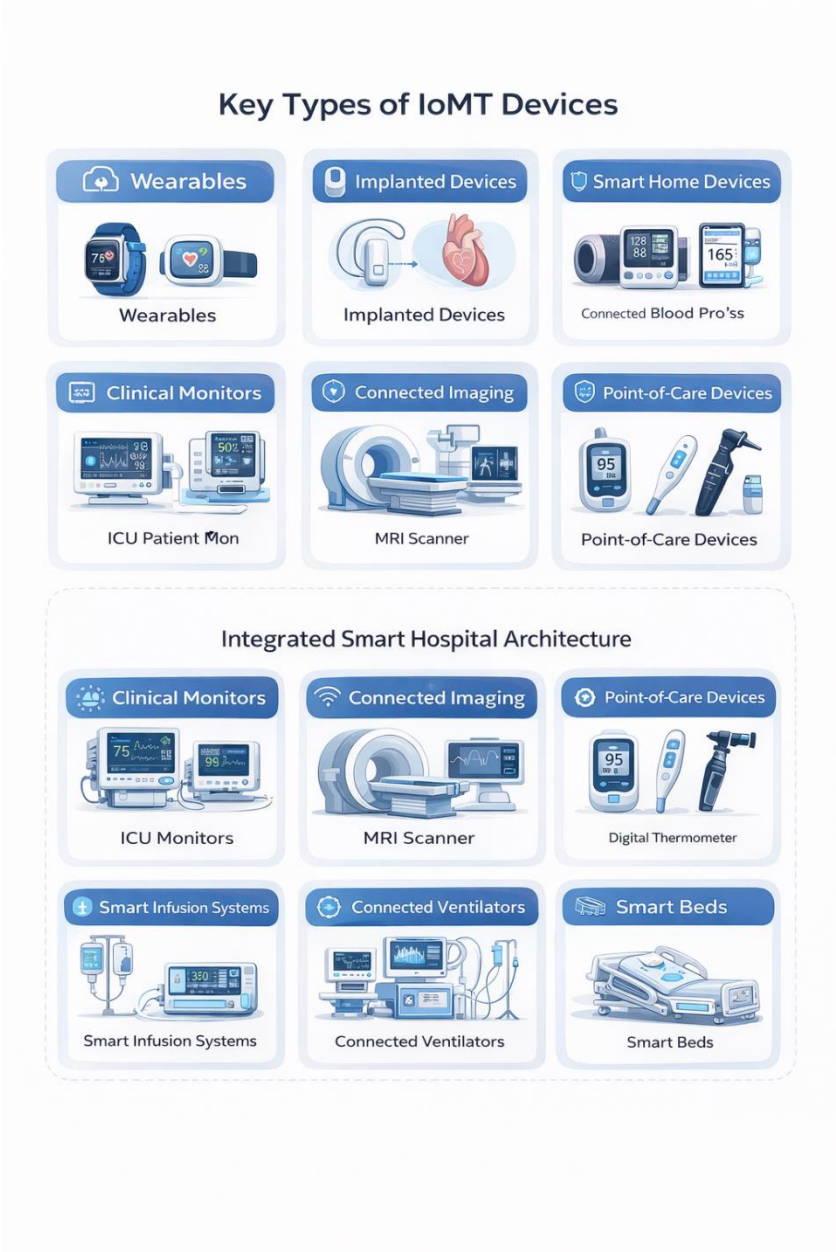


Figure 2 Types of IoMT Devices *Figure generated with LLM (ChatGPT 5.5)*

In the smart hospital environment, wearable devices such as smartwatches which can be seen in figure 2 helps for constant monitoring of a patient's vital signs such as heartbeat rate, glucose and sugar rates, etc. [42].These devices send real-time health data to healthcare providers so that they are fully updated on a patient's condition all the time and can also quicky attend to a patient as the need arises. Interconnected devices on-site, such as smart beds, infusion systems, ventilators, ICU monitors, help with regular patient monitoring and this is based on the real time data that they monitor [43].

2.2.2 Technical Architecture of IoMT Systems

IoMT consists of different layers that help to achieve the smart hospital functions. Some of the layers are device layer, network layer, data processing layer, application layer and security layer. Figure 3 contains a pictorial representation of this.

Wearable devices, sensors, and monitoring systems used in smart hospitals fall into the data layer. These devices make use of WI-FI, cellular connections for communications. The job of these devices in this layer is to constantly collect real-time patient data. In the network layer, the communication network that supports the WI-FI and cellular connections are present here. Some of the examples as seen in figure 3 are IoT gateways, communication protocols like MQTT, HL7 and FHIR. The aim of this layer is to transmit data from devices to back-end systems and to also ensure interoperability between different devices [42] .

The data processing layer seen in figure 3 can be defined as the brain of the system. This layer is responsible for the storage of patient data and the layer that is responsible for analysing and processing data for insights. This is the layer where AI models run and different patterns can be built from the data gathered and analysed.

The application layer is the layer responsible for user interface. In this layer, raw data is presented in a format that is understandable and able to draw conclusions from. The aim of this layer is to present ready-made processed data to doctors and other medical professionals. It helps medical practitioners in diagnosis and decision making.

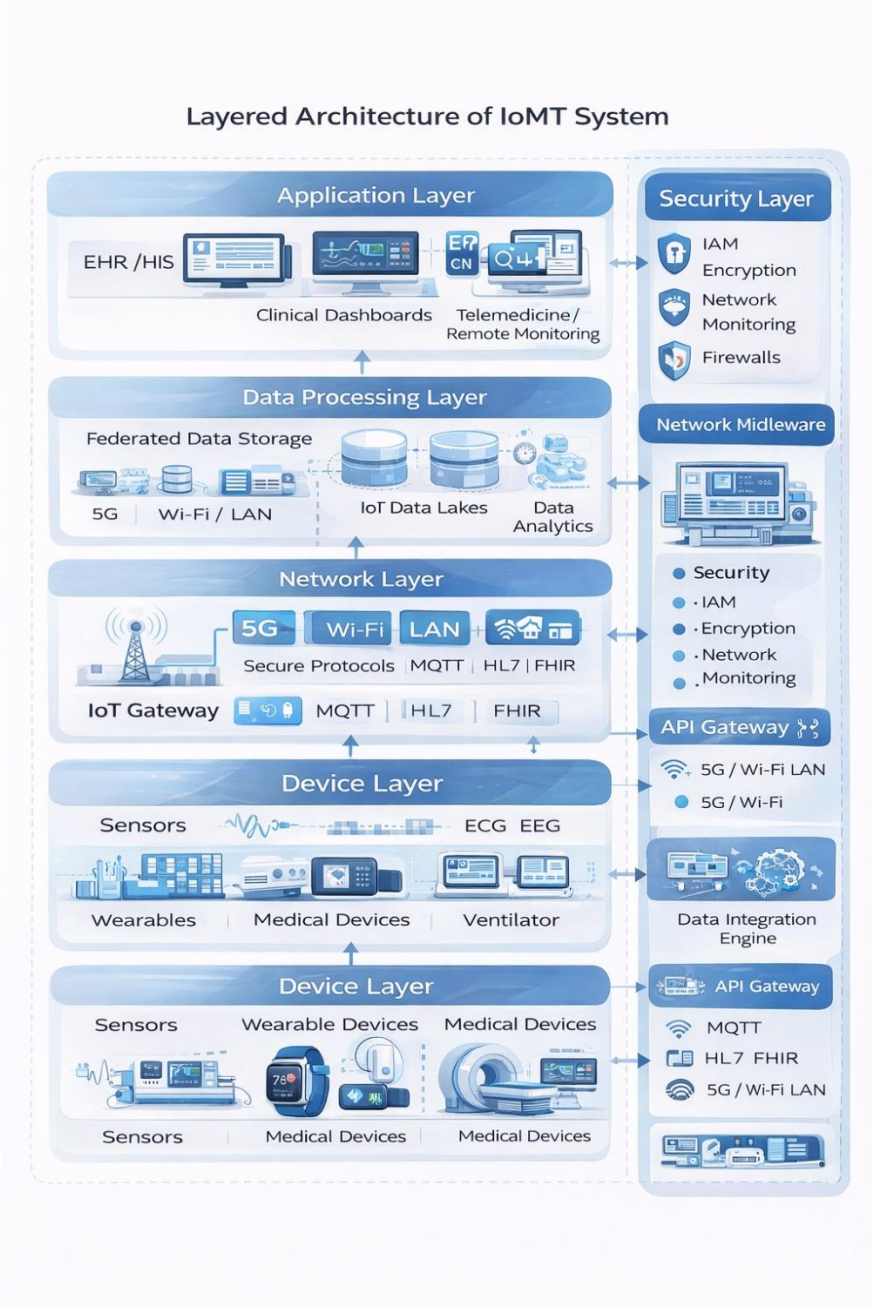


Figure 3 IoMT Architecture Figure generated with LLM (ChatGPT 5.5)

The security layer offers end-to-end encryption, authentication methods, access controls, and audit logging safeguard data during collection, transmission, storage, and analysis [40].

2.2.3 Vulnerabilities in IoMT Infrastructure

Despite their clinical advantages, IoMT devices pose serious security risks that weaken smart hospitals' defences against cyberattacks. In 2025, vulnerabilities in IoMT devices reached record highs, averaging 6.2 security flaws per device, with 60% of devices running outdated systems that no longer receive security updates [10].

Several factors contribute to IoMT security issues. One of such issues is legacy systems that cannot be patched or updated. According to an article by IoT in Healthcare, about one in five connected healthcare devices runs on unsupported, vulnerable systems that cannot be updated or patched without affecting patient care or voiding warranties. These outdated systems create ongoing vulnerabilities that attackers often exploit to gain initial access to hospital networks [26].

Smart Medical devices are built by OEMs (original equipment manufacturers) with security considered as an afterthought and this is further supported in [44]. Because of the bottlenecks involved in medical devices software updates, most vulnerabilities are not fixed, and devices are used in the default mode that they come in which poses a significant risk. Because of the demands of the healthcare environment, time required for upgrading and maintaining essential medical devices might be hard to come by [25].

Smart medical devices are required to send various health information to different hospital systems, and this can lead to a weak security posture either from the device sending the information or the device receiving it [20]. Outdated communication systems and interfaces often lack modern security features, and this is another challenge faced by IoMT devices.

2.3 Electronic Medical Records and Data Management Systems

Smart hospitals make use of electronic health record systems for gathering data on their patients and this leads to a better care. While EHR(s) have many advantages, it is a major target for attackers because if they can gain unauthorized access, they will have a plethora of PIIs (Personally Identifiable Information (PII)).

2.3.1 EHR System Components and Functionality

The various parts that are integrated into an EHR system can be seen in figure 4. This architecture shows a layered approach to better management of healthcare data and clinical workflows. Data is gotten from the different data sources as seen in figure 4. After that, the data sources then send information to the EHR core components which consists of patient registration, clinical documentation, order entry, etc.

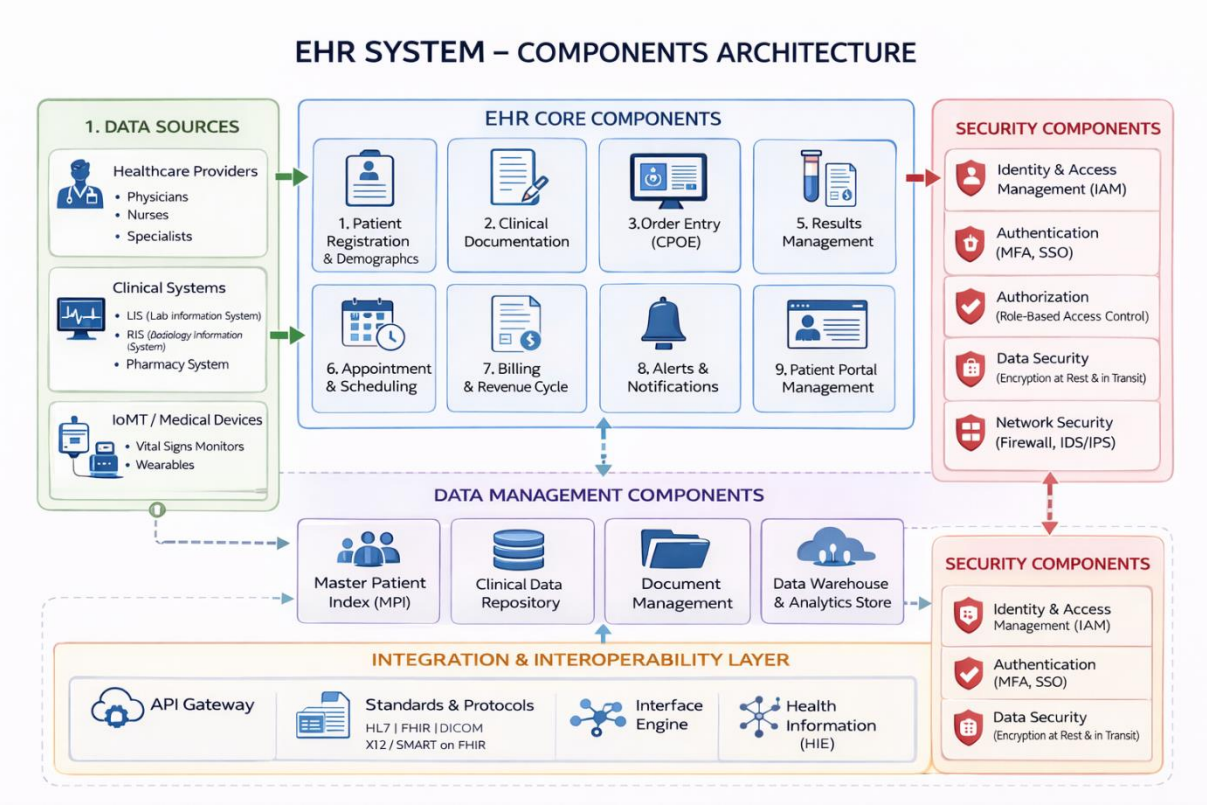


Figure 4 EHR System components architecture Figure generated with LLM (ChatGPT 5.5)

The data management layer`s function is to ensure that data is properly organized and stored. The Integration and interoperability layer is responsible for seamless and quick communication between the heterogeneous systems.

2.3.2 EHR Adoption and Implementation Challenges

EHR systems are highly used in developed nations because of the mix of regulatory requirements, financial incentives, and recognition of clinical benefits. In the United States of America, an act was created called the HITECH act of 2009 which offers financial rewards for healthcare providers who used certified EHR technology to better improve healthcare [35].

Notwithstanding this, healthcare organizations have faced many challenges while trying to implement EHR in their operations.

According to R. S. Evans, healthcare workers still use paper methods instead of fully utilizing the EHR features when the system does not fully work well with clinical workflows [31]. There are still issues related to different IT systems not being able to accurately exchange data and user information in Real-time [29].

Alert fatigue is also another challenge that comes with EHR systems. Once the number of notifications becomes too much, important or critical alerts can be overlooked or ignored [45]. Because of the time spent in data entry, hospital staffs can be faced with increased documentation workload and time that should have been spent to take care of patients is rather spent on navigating through systems and inputting data [46].

2.3.3 EHR Systems as Ransomware Targets

There are many reasons why ransomware attackers target EHR systems. Due to the dependency on EHR systems, any form of attack that can cause an EHR system to be unavailable can have life threatening effects. This has led some healthcare providers to quickly pay the ransom whenever they are faced with ransomware attacks or incidents.

EHR systems are also considered as a high target because of the valuable personal and sensitive information that they hold. According to Healthcare Cybersecurity Statistics 2025 [47], EHRs hold a wide range of protected and personal information which if stolen, can be used for fraud and identity theft. Ransomware attacks that try to publicise stolen health data adds further pressure to health care providers and organizations.

Because EHR systems also connect with many other hospital systems, any ransomware that affects the EHR can cause downtime to different other hospital networks. The large number of data that is in EHR systems combined with the requirements for uptime, data consistency and real time reporting makes it hard to keep clean, accessible backups that can restore quickly from backups after ransomware attacks [48].

Finally, Healthcare organizations are required to adhere to strict regulatory standards under laws like HIPAA to prevent CIA (confidentiality, integrity and availability) issues. Breaches can lead to operational and financial loss to any healthcare organization [47].

2.4 Previous Research on Healthcare Cybersecurity

Research within the area of cybersecurity in healthcare has significantly grown in the last few years in response to the increasing threats to healthcare information and systems. The following review of the literature aims to provide a summary of some of the findings regarding healthcare cybersecurity threats and vulnerabilities, as well as the proposed solutions to those identified issues.

2.4.1 Summary of Key Findings and Contributions

Reviewing the available literature on cybersecurity in the healthcare Industry reveals several concerning patterns. The field has made progress certainly, but significant blind spots remain that leave healthcare organizations vulnerable.

2.4.2 Prevalence of Technology Focused Research

One of the first notable findings regarding the healthcare cybersecurity literature is the continued dominance of technology within research publications. Over half of the published studies focus on the technical aspects of cybersecurity in healthcare environments [49]. Furthermore, only about a third of the available research covers management and organizational cybersecurity issues. In specific areas of the topic, research appears to be even more lacking. For instance, according to Kazi [49], research that investigates software development security practices receives very little attention, with only around 3% of existing cybersecurity research in healthcare dedicating focus to this topic. Furthermore, only about 3% of research dedicated to healthcare cybersecurity covers topics like business continuity and disaster recovery practices, despite the fact that many ransomware attacks are of significant availability concern to the healthcare sector. Finally, research into the physical security of healthcare facilities is a topic that hardly receives any mention within cybersecurity research publications, with only 1% of current research focusing on physical security [50]. Such a focus on technology introduces potential issues into the discussion of healthcare cybersecurity. For instance, if enhancing the cybersecurity technology of healthcare networks will lead to the resolution of an organization's ransomware problems; however, as discussed by Ewoh et al [51], the issue may be rooted in

organizational and human factors. Such organizations may have some of the best cybersecurity technologies in the nation yet still suffer from attacks caused by inadequate security culture, insufficient training of cybersecurity staff, or poor coordination between departments. It is not to imply that technical cybersecurity issues are not important to discuss and analyse. As discussed, researching the vulnerabilities of medical devices or the benefits of implementing network segmentation are important topics of discussion. However, the imbalance of both technical and non-technical research indicates a tendency for the management of cybersecurity in healthcare to be predominantly viewed as a technical issue rather than a sociotechnical issue.

2.4.3 Limited Evidence on Intervention Effectiveness

Here's a frustrating truth, we know very little about which cybersecurity measures work in healthcare. Most studies investigate the threats to healthcare organizations, the vulnerabilities in their systems, the frameworks to improve cybersecurity, or even the technical solutions to those vulnerabilities. However, there are few studies that investigate whether these suggested solutions lower the risk to the organizations, improve their outcomes, or provide a good return on investment for those healthcare systems. This problem extends beyond developed nations. Many studies have investigated the state of cybersecurity in healthcare systems in low- and middle-income countries. In these studies, there is almost no evaluation of the outcomes of the cybersecurity measures that have been deployed in these systems [52]. Out of 20 studies that have been performed on cybersecurity in healthcare in these nations, only one shared the results of the outcomes of healthcare systems with the implementation of these measures. The other 19 studies explained the cybersecurity measures that were implemented in these systems but did not evaluate whether they were effective. Healthcare systems are forced to make difficult decisions regarding where to allocate their limited resources and how to best secure their systems. Should they invest in endpoint detection systems, security training for employees, or backup systems for their data? There is no easy answer to this question, as there is no way of knowing which system would provide the best return on investment for any given healthcare organization. In addition to these implementation and efficacy problems, there is also a problem in evaluating the successes and failures of the cybersecurity measures that have been implemented. Because there is no evaluation of whether the cybersecurity measures that are implemented in healthcare systems are effective, there is no way of learning from either the successes or failures of those systems [53].

2.4.4 Geographic and Organizational Disparity in Research Focus

Looking closely at the research being conducted in the field of healthcare cybersecurity reveals a focus primarily upon large medical centres and health systems within wealthy countries, especially the United States and the European Union [52]. The majority of healthcare within the world is not represented within the literature that has been published on this topic. For instance, community hospitals that may serve smaller populations have different challenges than the large academic medical centres [54].

Many of these community hospitals have much smaller IT and cybersecurity personnel than the hospitals of high academic medical centres, as well as lacking the specialized personnel that may be found within those healthcare systems. Thus, the insights that are gained from researching these institutions may not be reflective of the cybersecurity challenges that many of the smaller hospitals face and experience. According to Ultimate Guide to Cyber Resilience in Healthcare report [55], rural healthcare providers experience even more severe limitations.

Attracting cybersecurity talent is extremely challenging when the nearest city is hours away. Budgets often permit only the most basic security measures. However, ransomware attackers increasingly target rural hospitals because they are seen as easy targets with minimal defenses. Ambulatory care settings such as physician practices, urgent care centers, and outpatient surgery centers are largely absent from cybersecurity research [56]. Yet these organizations are increasingly utilizing EHR systems, exchanging health information electronically, and facing ransomware threats.

Their requirements differ from those of hospitals (no 24/7 operations, different regulatory obligations, smaller scale), but research seldom addresses these differences. Long-term care facilities are another neglected area. Nursing homes, assisted living facilities, and rehabilitation centers handle sensitive health data and are increasingly using connected monitoring technologies, yet cybersecurity research in these environments is still limited [57].

Lastly, healthcare in low and middle-income countries receives very little research focus, despite accounting for most of the global population [52]. These healthcare systems are often overlooked in cybersecurity discussions. These healthcare systems deal with limited resources that are much smaller than those in rich countries, work under different regulations, and face

unique security challenges. This difference is important because cybersecurity advice made for well-funded organizations might not work at all in other places [53]. Suggesting that a rural hospital with only two IT staff and a very tight budget should adopt a full Zero Trust architecture is not practical as it doesn't relate to their situation.

2.4.5 Insufficient Focus on Patient Safety Outcomes

Recognizing the negative impact of ransomware attacks on patients is universal. The victims of these attacks caused treatment delays for patients across the country. Another attack on Ascension forced emergency departments to divert patients away from the departments. Although it is understood that these types of attacks occur on healthcare systems, it is unclear on how it affects patients. Are the outcomes of these patients serious? What aspects of the attack relate to patient outcomes? Several challenges exist that prevent researchers from investigating these questions. For example, it is difficult to determine whether the observed negative outcome in a patient was the result of the ransomware attack, the patient's condition, or a combination of these factors.

Additionally, healthcare systems are often reluctant to reveal information about the attacks and their impact on patients [51]. The reasons for this are likely concerns about the impact of such disclosures on the organization, including liability. Thus, researchers are often unable to access data regarding patient`s outcomes to investigate. For example, current regulations regarding data breaches require patient data to be kept confidential rather than making public the impact that the attacks had on the availability of those systems. Thus, there is a gap in understanding the impact of ransomware attacks on patients. In the absence of solid evidence of the impact of ransomware attacks on patient safety, several issues arise within the healthcare and information technology sectors regarding justifying cybersecurity investments, performing risk assessments, and making planning decisions regarding incident response.

2.4.6 Systematic reviews of Healthcare Cybersecurity

Numerous research studies have performed systematic reviews of the cybersecurity threats, vulnerabilities, and solutions within healthcare environments. Authors Kruse et al., [18] for instance, performed a systematic review of the literature regarding cybersecurity threats and trends within healthcare environments. In their review, the authors found that the healthcare

Industry is significantly behind in relation to cybersecurity practices compared to most other industries [18]. For instance, some of the weaknesses that were identified within the healthcare Industry included a lack of defined individuals responsible for cybersecurity practices, a lack of defined procedures for software updates or responding to a cybertheft incident, a lack of proper segmentation of the hospital network, and the inadequate training of employees to recognize potential social engineering attacks.

A more recent systematic literature review was performed by Ewoh et al [51]. The authors performed a review of the literature for vulnerabilities within healthcare systems relative to cyberattacks, utilizing a sociotechnical viewpoint, they reviewed 70 scholarly articles that were published between 2012 and 2022 [51]. Their results highlighted that cybersecurity issues in healthcare arise from complex interactions among technological, organizational, and human factors rather than from technical shortcomings alone. The authors found that many of the issues related to cybersecurity within healthcare environments are the result of the interaction between technological, organizational, and human factors. Some of the vulnerability categories included in the systematic review were the outdated software that is implemented within legacy systems, a lack of cybersecurity awareness of personnel within the healthcare Industry, the underinvestment of cybersecurity within the healthcare Industry, a lack of experts in cybersecurity within healthcare organizations, and a lack of collaboration between IT teams and other healthcare personnel.

Finally, another research study published within the last few years investigated cybersecurity within low- and middle-income countries; it identified a significant lack of evidence base for cybersecurity practices within these countries, with a variety of different cybersecurity measures being published in research studies [52]. Furthermore, the authors indicated that there is a necessity for more thorough research studies published regarding cyberattack prevention methods and their effects.

2.4.7 COVID Pandemic Impact on Healthcare Cybersecurity

The COVID-19 pandemic also allowed people to observe the vulnerabilities of healthcare cybersecurity. Authors Muthuppalaniappan and Stevenson demonstrated a rise in cyberattacks on healthcare organizations during the pandemic, stating that these attacks were a significant threat to global health during this time [14]. Healthcare organizations faced several operational

challenges as they rapidly adopted remote work, telehealth services, and new digital tools to maintain care delivery during lockdowns.

A scoping review by He et al., [53] explored the cybersecurity challenges and solutions in healthcare, specifically during the COVID-19 pandemic [53]. During this review of 56 studies, the authors discovered several challenges to the cybersecurity of healthcare organizations resulting from the pandemic, including challenges with securing healthcare staff working from home, the use of personal devices, a lack of business continuity plans for pandemics, and the lack of cybersecurity awareness of healthcare staff. Additionally, during the pandemic, many cybercriminals took advantage of the pandemic to execute phishing schemes targeting healthcare workers, distributed denial-of-service attacks on healthcare organizations' websites and services and even conducted ransomware attacks on hospitals treating patients with COVID-19 [16]. Such actions of cybercriminals show that they will take advantage of any opportunity to target healthcare organizations, regardless of the situation surrounding the attacks on these organizations.

2.4.8 Sociotechnical perspectives on Healthcare Cybersecurity

Many recent studies adopt sociotechnical views of cybersecurity, recognizing that cybersecurity results from the interactions among technical, organizational, and human components of the system [51]. Jalali and Kaiser developed a systematic view of hospital cybersecurity, recognizing the importance of addressing cybersecurity at various levels within the organization [17]. Sociotechnical methods for healthcare cybersecurity suggest interventions in several areas such as educational, organizational, technical and collaborative.

Educational intervention is the creation of cybersecurity training programs for healthcare workers, ongoing security awareness sessions, simulation drills for responding to cyber incidents, and incorporating cybersecurity concepts into medical and nursing training [51]. By clearly defining the cybersecurity roles and responsibilities of each department, forming cybersecurity committees, developing thorough security policies and procedures, and fostering a positive security culture within the organization is intervention in organizational method [53].

By gradually replacing outdated systems with secure options, segmenting the network according to zero-trust models, implementing systems to detect and respond to threats to the

network, and purchasing new technology with secure design principles in mind can all be described as technical intervention [58]. By sharing information between healthcare organizations as well as with external parties regarding cybersecurity threats and vulnerabilities to that organization's networks, forming public-private partnerships, working with law enforcement agencies regarding cybersecurity investigations, and forming partnerships with other organizations to establish industry security standards [51].

3 Literature Review and Gap Analysis

3.1 Search Criteria

The gap in the existing literature on the topic of cybersecurity in healthcare was investigated through systematic literature reviews of various databases (PubMed, Web of Science, ScienceDirect, Scopus, IEEE Xplore, and JMIR publications that focus on healthcare cybersecurity). The search strategies for these databases utilized terms related to healthcare, cybersecurity, ransomware, vulnerabilities, and smart hospital technologies. The articles gathered through these searches were analysed using Consensus with keyword searches such as "Articles related to Cybersecurity resilience of smart hospitals against ransomware attacks". The literature review performed utilized peer-reviewed journals, conference proceedings, government publications, industry analyses, and other grey literature databases published between 2020 and 2025, focusing on the most recent five-year period to ensure that any research gaps pertain to current challenges within the described area of investigation rather than historical issues [57]. Additionally, the types of articles included in this research review contained research on ransomware and cybersecurity issues within healthcare settings [52]. Literature eliminated from the review included general cybersecurity journals, purely technical journals focusing on malware analysis, and other literature outdated relative to available research on the described topics. The systematic review used PRISMA guidelines to ensure completeness in the literature review [51]. The articles were independently reviewed by multiple researchers to determine inclusion in the review, with disagreements resolved through discussion among the researchers. Such a thorough review process ensures that any identified gaps in the existing research on this topic are complete and unbiased.

3.2 Gap Analysis

The gap analysis method combines techniques from various systematic literature reviews on healthcare cybersecurity [18], [51], [52]. The gap analysis reviews the knowledge gaps, practice gaps, policy gaps, and tool and technological gaps in relation to cybersecurity in smart hospitals. Within the knowledge gaps, there are shortcomings in theoretical knowledge, data, and models regarding ransomware threats and defences for healthcare environments [57]. Additionally, there are gaps within the available knowledge in relation to the application of cybersecurity practices within healthcare environments [53]. These knowledge gaps lead to practice gaps

wherein the recommendations and suggestions for healthcare practices do not lead to enhancements in security for those practices. Related to these practice gaps are policy gaps wherein organizations lack the appropriate policies or incentives to enhance their cybersecurity defences. Furthermore, there are shortfalls in the regulatory frameworks and incentive structures for these organizations to sufficiently tackle the threats of ransomware attacks. In relation to technological tools, there are deficiencies in the technologies, methods, and capabilities of the security systems for healthcare environments to effectively defend against ransomware attacks [54]. These technological tool gaps indicate that there are insufficient technological solutions to meet the technological needs of healthcare environments and resources. Thus, overall, countering the issues of ransomware attacks on smart hospitals requires a simultaneous focus on each of these four areas. Any shortcoming in any of these areas will hinder advancements in the others. Therefore, it is essential to utilize thorough strategies for each of these categories to effectively counteract the threat of ransomware attacks on healthcare organizations.

3.2.1 Gap Categorization and Prioritization

After identifying the gaps in the research area of ransomware, those gaps needed to be categorized. Not all gaps are equally significant or deserving of immediate attention to address. The study utilized various criteria to assess the gaps. One criterion was assessing the severity of each potential gap in the area. Such severity would consider the potential harm or opportunity costs that can result from that gap. For instance, a gap in understanding how ransomware can impact patient safety would have high severity associated with it due to the life- and death-implications of such an issue.

In contrast, a gap in understanding administrative best practices would be less severe in its impact on healthcare and ransomware in general [59]. Another criterion for assessing the gaps was considering the urgency of each category of gap. Urgency relates to how rapidly that gap must be addressed in response to the threats and requirements of the current healthcare systems. For instance, the shift to ransomware that primarily focuses on the exfiltration of data from those systems creates urgency in understanding the threat of this new type of malware, even though ransomware that focused upon encrypting patient data would likely receive more research focus and effort from authors and researchers [55]. Another criterion for assessing gaps is feasibility. This criterion analyses whether it is realistic to address each identified gap

with the available resources [52]. For instance, some gaps may require extensive and costly research initiatives over several years to fill, while other gaps may be resolved through other means.

Finally, one criterion for assessing the gaps was impact. The impact criterion assesses whether resolving one gap will lead to advancements being made in other areas of ransomware analysis and response [56]. For instance, creating an efficient means of assessing the risk of ransomware attacks will allow organizations to make informed decisions about how to allocate their resources to address this threat, make due diligence reports to regulatory authorities, and demonstrate their commitment to improving their security. Such a development would help resolve several different needs of healthcare organizations at once. While the prioritization of these different categories for assessment helps indicate which gaps will be addressed in what order, such a prioritization does not indicate that any gaps with lower priorities will necessarily be ignored altogether. Instead, this prioritization helps to create an understanding of the order in which improvements can be made to resolve these gaps.

3.2.2 Identified Gaps in Existing Research

Despite the growing interest in cybersecurity research, there are still major gaps in the existing literature on the topic. Luna et al., [60] conducted a review of the literature on cybersecurity in healthcare information systems and found a lack of empirical research assessing the security of healthcare information systems [60]. Most of the existing research on the topic is focused on descriptive studies of the current state of cybersecurity in healthcare rather than studies assessing the effectiveness of implemented security measures

Much of the existing research on healthcare cybersecurity focuses on large academic medical centres and health care systems in developed nations. There is a lack of research focusing on community hospitals, long-term care facilities, and health care systems from low- and middle-income nations [52].Most cybersecurity research in healthcare information systems has concentrated on assessing technical vulnerabilities and implementing technical solutions to address those vulnerabilities. There is little attention paid to organizational, economic, regulatory, and human aspects of cybersecurity in healthcare information systems [51].

There is especially a lack of research regarding the impact of cyberattacks on patient safety, the cost-effectiveness of different security measures, the best way to allocate limited cybersecurity budgets, and how to maintain security while ensuring usability and efficiency in clinical workflows [17]. Additionally, the fast-changing threat landscape means that existing research often does not keep up with current attack methods, with little predictive research on new threats like AI-driven attacks, the effects of quantum computing on healthcare encryption, and the innovative use of emerging technologies such as 6G networks and extended reality systems in healthcare [58].

4 Threat Landscape for Ransomware attacks in Smart Healthcare

This section provides more background information on Ransomware and the healthcare sector.

4.1 Overview of Ransomware in the Healthcare Sector

Ransomware has become one of the most urgent and significant cybersecurity threats to the healthcare Industry. Unlike other types of cyberattacks that mainly focus on data confidentiality, ransomware attacks jeopardize all three key aspects of information security such as confidentiality via data theft, integrity through possible data alteration, and most importantly, availability through system encryption and disruption of operations. The distinct nature of this threat makes ransomware especially harmful to healthcare organizations.

4.1.1 Definition and Characteristics of Ransomware

Ransomware is a type of harmful software that is created with the intention of blocking access to computer systems and data until the malicious parties that created the ransomware are paid for the ransom [24]. The majority of ransomware utilizes encryption software to lock into the files and systems of the infected systems until the ransom is paid. Due to the growth of cryptocurrencies, such as Bitcoin, it has become easier for the individuals who are infected with ransomware to pay the ransom demanded of them without traceability [61]. There are a few features of the ransomware that is targeting the healthcare Industry that make it distinct from other forms of ransomware. Attackers that target the healthcare Industry are aware of the inabilities of these systems to experience downtimes, which means that they are under significant pressure to pay the ransoms demanded of them [62].

Due to the above features, healthcare organizations are statistically more likely to pay the ransom demanded of them than organizations within other industries. Data from the healthcare Industry is valuable on the dark web due to the amount of personal and financial information that is included in medical records [9]. As such, the information that is included in these records includes information on the patients' medical histories, social security numbers, and financial information such as insurance information and billing details. Additionally, a cyberattack on healthcare systems can directly impact the lives of patients by making it impossible for the institutions to access the patients' medical records, medical devices, perform required diagnoses on patients, or effectively manage the emergency departments within these hospitals.

This potential threat to the lives of patients makes healthcare system attacks distinct from other potential cyberattacks on nonhealthcare organizations. Furthermore, healthcare organizations are under strict regulations on how their data is managed, such as HIPAA, which ensures the confidentiality, integrity, and availability of their data [47]. When ransomware attacks compromise protected health information, they trigger mandatory breach notifications, regulatory investigations, and potentially hefty financial penalties.

4.1.2 Evolution and Trends in Healthcare Ransomware

The healthcare Industry has seen a steady rise in ransomware incidents over the last ten years. In 2024, there were 444 reported cybersecurity events in healthcare, which included 238 ransomware threats and 206 data breaches, marking the highest total among all critical infrastructure sectors [63]. Healthcare organizations reported 181 ransomware attacks affecting 25.6 million healthcare records in 2024, with average ransom demands of $5.7 million and average payments of $900,000 [64] . The ransomware threat landscape in healthcare shows that the number of ransomware attacks on healthcare providers has surged from 34% of organizations reporting attacks in 2021 to 67% in 2024 [65].

While some other sectors saw a slight decrease in attacks during this time, healthcare has continued to face rising ransomware activity, making it an appealing target. The average cost of recovering from a ransomware attack in healthcare reached $2.57 million in 2024, not including ransom payments, up from $2.20 million in 2023 [66]. The global average cost of healthcare data breaches hit $9.77 million in 2024, marking the fourteenth year in a row that healthcare led all sectors in breach costs [9].

Recovery times from ransomware attacks in the healthcare Industry are increasing. In 2024, 37% of healthcare organizations took longer than one month to recover from ransomware attacks, up from 28% in 2023 [66]. Additionally, the number of organizations reporting recovery in under a week dropped from 54% in 2022 to 22% in 2024. Healthcare organizations are experiencing an increasing number of ransomware attacks with the intention of extorting data from those organizations. In 2025, the percentage of healthcare providers facing extortion-only attacks (where data is stolen but not encrypted) tripled to 12%, up from 4% in previous years [22].

Furthermore, the rate at which data is encrypted during these attacks has dropped to its lowest point in five years, with only 34% of attacks resulting in encrypted data. Finally, ransom

amounts demanded from healthcare organizations have undergone major changes. In 2024, the average initial ransom demand was $4 million, but this decreased by 91% to $343,000 in 2025 [22]. These changes in ransom amounts indicate a shift in attacker strategies, targeting more smaller healthcare providers and moving toward data-extortion models with lower payouts.

4.2 Nature and Characteristics of Ransomware attacks

4.2.1 Ransomware attack lifecycle

The ransomware attack lifecycle consists of some stages that the attackers follow to encrypt and demand ransom over their victims. The stages can be seen in figure 5

Figure 5 Ransomware attack lifecycle Figure generated with LLM (ChatGPT 5.5)

The ransomware attack lifecycle starts from the reconnaissance stage. In this stage, the attackers try to gather as much information as they can about their targets. After the reconnaissance stage, the attacker moves to the initial access stage as seen in figure 5. In the initial access stage, the attackers try to gain access into the environment that they wish to exploit. They do this through crafting and sending of phishing emails or exploiting vulnerabilities found during the reconnaissance stage.

The third stage which is the execution stage is when the attacker tries to launch malicious code into the environment. They can drop ransomware payloads, run malicious scripts etc. After this stage, they moved to stage four which is the Privileged escalation and discovery stage where they try to pivot from a normal user in the system or environment that they exploiting to a super admin user.

The fifth stage is the lateral movement stage where the attacker can freely move across the entire network. Because they have upgraded their privileged to super admin, they can do things that many normal users might need permission for e.g. Remote administration tools like any desk. The next stage which is the sixth stage is the impact and encryption stage where the aim of the attacker is to disrupt operations and maximize pressure.

The final stage is where the attackers demand for ransom payment in exchange for decryption keys or threat to leak stolen data. Figure 5 contains this entire life cycle.

4.2.2 Ransomware Delivery Models

The rise of Ransomware-as-a-Service (RaaS) has changed the ransomware threat landscape significantly [67]. RaaS platforms offer ready-to-use ransomware operations where developers create and manage ransomware code while affiliates carry out attacks in return for a share of the revenue, usually 70-80% of the ransom payments going to affiliates [62].The RaaS model has made it much easier for criminals with limited technical skills to launch advanced attacks using professional-grade ransomware tools, infrastructure, and support services . Notable RaaS operations targeting healthcare include

- LockBit: This is one of the most active RaaS operations, having carried out many attacks on healthcare organizations globally [68]. LockBit is known for its fast encryption

capabilities, data exfiltration features, and advanced leak sites for releasing stolen data when ransoms are not paid.

- BlackCat/ALPHV: This group was behind the severe Change Healthcare attack in February 2024 and runs a very selective affiliate program along with complex extortion tactics [9]. After Change Healthcare paid a ransom of $22 million, the group executed an exit scam, leaving their affiliate unpaid and possibly prompting the affiliate to share stolen data with RansomHub for another extortion attempt.

- RansomHub: This group was the most active in terms of the number of attacks they made in 2024, performing 89 confirmed attacks on various sectors across the United States' economy [69]. The group primarily targets healthcare organizations but also performed data theft in 2024

- Black Basta: This group has carried out numerous attacks on healthcare organizations. One of the most significant of these attacks targeted Ascension Health in May 2024, exposing the data of 5.6 million individuals. Black Basta is known to utilize advanced techniques to gain access to the networks of the organizations they attack [70].

4.2.3 Big game hunting strategy

Ransom demands on the healthcare Industry do involve the use of the "Big Game Hunting" (BGH) strategies, which target a smaller number of high-value victims who can pay for the ransoms rather than attempting to target many victims who can pay smaller ransoms [71]. BGH strategies include researching the victims to which the attackers will direct their attacks, performing the attacks with specificity to the victims' environment and systems, maintaining long-term access to the victims' networks despite attempts at remediation, and setting ransom demands according to the victims' financial situations and insurance coverage for such situations. The healthcare Industry is a target for these types of attacks due to the essential nature of the industry's missions, the data that they store, the complexity of their IT networks, and their willingness to pay the ransoms necessary to regain their data and IT network capabilities [62].

4.3 Attack Vectors in Smart Hospital Environment

Healthcare systems have specific vulnerabilities that are traditionally exploited by cyberattacks seeking to deploy ransomware into this system.

4.3.1 Phishing and Social Engineering

Phishing is the leading method for deploying the ransomware into healthcare systems, accounting for 76% of cloud-based and 69% of on-premises security incident [15]. Additionally, healthcare workers are the primary targets for phishing attacks. These workers are targeted due to their high-stress jobs, their communication with patients and vendors, lack of training in cybersecurity, and their trusting nature [72].

Spear Phishing are highly focused emails sent to specific individuals, often pretending to be trusted sources like colleagues, hospital administrators, regulatory bodies, or healthcare suppliers [73]. Spear phishing emails use information from social media to pose as credible senders. In the business email compromise, the cybercriminals gain access to business emails and use those to send harmful messages that evade the business's security measures and appear as if they come from a very reliable source of information to the business's clients or contacts [74]. BEC schemes typically focus on accounts that have the authority for financial transactions or access to sensitive systems.

Credential Harvesting type of phishing email aim to steal the login credentials of the victims instead of installing the ransomware directly into the victim's machine [71]. Using these credentials, the attacker can log into the victim's systems and move into the machines without detection, allowing for subsequent ransomware attacks to occur. These types of phishing attacks come in the form of emails that contain malicious attachments (files) or links that, when clicked, will install the ransomware dropper that will install the ransomware [73]. These phishing attacks contains malicious attachments and links.

4.3.2 Compromised Credentials and Remote Access

The shift to utilizing various forms of remote access software and technologies following the COVID-19 pandemic has presented hackers with new attack paths for gaining access to private networks. The compromised credentials for VPN and RDP software are the main means of attack for ransomware attacks with healthcare as their target [22]. These credentials for healthcare networks can be gained in a variety of different ways. For example, one way is through the purchase of credentials on the dark web. These credentials come from databases of stolen passwords from past data breaches of the healthcare organizations [62].

Another way in which hackers gain access is through credential stuffing. This attack occurs when hackers utilize software to automatically attempt to login to networks with a variety of stolen usernames and passwords, capitalizing on the fact that some individuals utilize the same password for their personal and work accounts [71]. Additionally, hackers may use a form of brute force attacks on the networks. These attacks involve systematically attempting to guess passwords for accounts, which is made easier for hackers with accounts with weak passwords or no-account lockout policies in place for hackers attempting to gain access.

Finally, hackers can utilize keylogging and information stealing malware, which is a type of malware that is designed to capture the keystrokes from computers and laptops, gaining access to saved passwords in browsers, and reading the credentials from those hacked computers [74].

4.3.3 Vulnerability Exploitation

The analysis of the causes of healthcare ransomware incidents reveals that the exploitation of vulnerabilities in healthcare IT and medical devices has become the leading technical cause of such incidents, responsible for 33% of all healthcare ransomware incidents [22]. The smart hospital setting presents challenges in managing vulnerabilities, especially due to the use of Legacy Medical Devices. According to IoT in Healthcare report [26], about 20% of connected healthcare devices operate on outdated, vulnerable operating systems and firmware that can be exploited by cybercriminals to deploy ransomware with minimal resistance from the device's operating systems.

Medical devices cannot be patched without significant validation and approval, thus exposing the device to malicious actors for years at a time. Smart hospitals also have many software applications and interconnected systems that create large attack surfaces for hackers to exploit [72]. Healthcare organizations often defer applying security updates due to concerns about system stability, patient safety with any updates to the systems, a lack of maintenance windows for critical systems, and the lack of an environment to test updates before they are implemented [25].

Some of the most significant vulnerabilities that have been exploited in the healthcare Industry in recent years include
MOVEit Transfer Vulnerability (CVE-2023-34362) where the Clop ransomware group took advantage of a zero-day SQL injection vulnerability in MOVEit Transfer software, a commonly

used file transfer application, leading to widespread exploitation affecting many healthcare organizations [75]. Unlike the traditional kind of phishing attacks, this kind of attack used solely the vulnerability of the software.

Citrix NetScaler Vulnerabilities happened when Several ransomware groups have exploited the vulnerabilities in the Citrix NetScaler ADC and Gateway products to gain access to the healthcare networks [76].As these devices are accessible over the internet, attackers who gain access to these can access the internal networks of the organization. The remote access solutions of various companies including Pulse Secure, Fortinet, and Palo Alto Networks have also been targeted by the ransomware attackers [73].

4.3.4 Supply chain and Third-Party Compromises

The connected nature of the healthcare Industry also puts the supply chain of that industry at risk of cyber-attacks [77]. The recent focus of healthcare ransomware attacks has been on third-party vendors and service providers instead of the healthcare providers themselves. In 2025 alone, there was a 30% increase in attacks on healthcare businesses, including pharmaceutical manufacturers, medical billing providers, and healthcare technology companies, compared to the previous year [77]. This shift by hackers indicates that they are aware that attacking one vendor or service provider for the healthcare Industry can have widespread effects on the various other healthcare clients of that vendor or service provider.

The Change Healthcare attack is an example of the risks associated with supply chain attacks on the healthcare Industry. Change Healthcare is a company that processes around 15 billion healthcare transactions each year. In February of 2024, Change Healthcare was the victim of a ransomware attack that compromised the protected health information of 100 million individuals, disrupted the billing processes of thousands of healthcare providers, and cost UnitedHealth Group over $2.9 billion in losses [9].

4.3.5 Internet of Medical Things (IoMT) Vulnerabilities

The rise of connected medical devices in smart hospitals opens opportunities for ransomware attacks and operational issues. IoMT devices have several exploitable features such as weak authentication and default passwords. According to Amos [11], Many medical devices come with default passwords that are seldom changed, lack strong authentication support, and do not

require complex passwords. Another exploitable feature is the use of unencrypted communications that medical devices use. Medical devices often send sensitive patient information over unencrypted networks, making them vulnerable to man-in-the-middle attacks and credential theft [20].

Outdated software components are also other features affecting IoMT devices. According to Khalil [10], About 60% of IoMT devices operate on outdated systems, making them ongoing vulnerabilities in hospital networks. While being connected to networks allows for remote monitoring and data sharing, it also provides routes for attackers to move laterally from compromised medical devices to critical hospital information systems [72]. Ransomware attacks that target medical devices can lead to immediate life-threatening situations. If ventilators, infusion pumps, patient monitors, or diagnostic imaging equipment are encrypted or disrupted, it directly affects patient care and can lead to death.

4.4 Case Studies of Ransomware Incidents in Smart hospitals

There have been some significant ransomware incidents that have affected hospitals and they are listed below

4.4.1 Change Healthcare Ransomware Attack

The ransomware attack on Change Healthcare has become the largest and most impactful cyberattack on healthcare organizations in U.S. history. On February 12, 2024, hackers from the BlackCat/ALPHV ransomware group gained access to Change Healthcare's servers using stolen credentials [78]. The hackers were able to access the company’s remote access gateway, which did not have multi-factor authentication enabled for access to the system. During the period between February 12 and February 21, 2024, the hackers conducted reconnaissance of the company’s systems, mapped the network, gained additional access and elevated privileges, accessed sensitive information, and began to install the ransomware packages onto the company’s internal servers [9].

Upon detecting the cybersecurity attack, Change Healthcare took actions to contain the damage and restore the affected systems, bringing in incident response teams and cybersecurity specialists to fix the issue [78]. However, on March 1, 2024, Change Healthcare had to pay a ransom of 350 Bitcoin, which was worth around $22 million to the BlackCat/ALPHV

ransomware group [9]. However, the BlackCat/ALPHV group later executed an exit scam by closing their operations and receiving the ransom payment without restoring Change Healthcare's systems or paying their affiliate the ransom payment [79]. The affiliate company, which was not paid by the BlackCat/ALPHV ransomware group, later disclosed that they had shared the stolen data with another ransomware group, the RansomHub ransomware group, which attempted to extort Change Healthcare Group again [80].

This unprecedented situation of being blackmailed twice by the same ransomware group demonstrates the significant unreliability of these groups. The cyberattack impacted the protected health information (PHI) of around 100 million individuals, which represents roughly one-third of the United States population [78]. Change Healthcare disrupted its services for around 80% of healthcare providers and pharmacies in the United States [9]. The restoration of the impacted systems took time, with payment services and prescription claim services becoming available again on March 7, the electronic payments platform on March 15, and it took several months for the company to fully restore their systems [78].

The parent company of Change Healthcare, UnitedHealth Group, initially reported that the cost of the attack would amount to $870 million for the first quarter of 2024. However, they later confirmed that their total loss from the attack would surpass $2.9 billion [9]. The losses that the company reported include the $22 million payment to the ransomware attackers, the cost of restoring their systems, the advanced payments to the healthcare providers impacted by the attack, regulatory fines, legal costs, and the improvement of their cybersecurity systems to prevent such attacks from happening again in the future.

4.4.2 Ascension Health Ransomware Attack

Ascension, one of the largest nonprofit health systems in the United States with 142 hospitals in 19 states, was attacked by the Black Basta ransomware group [70]. The first breach occurred on February 29, 2024, but it went unnoticed for more than two months [81]. On May 8, 2024, Ascension detected unauthorized activity in its systems and quickly began its incident response. The attackers took advantage of the long period during which they were undetected to thoroughly explore the network and identify targets and methods for causing the most damage when they were eventually detected.

The attack on Ascension's electronic health record system prevented the use of the system in all 142 hospitals [82]. Specific effects included Emergency departments at several facilities went on divert status, redirecting ambulances to other hospitals, Manual, paper-based methods were used for patient documentation, orders, and care coordination. Elective procedures and surgeries were postponed; Pharmacy operations and medication administration workflows were disrupted. Access to historical patient records, test results, and clinical documentation was lost. The healthcare workforce faced strain as they had to work without standard digital tools.

The EHR outage lasted about four weeks, during which staff had to work under very difficult conditions using manual processes that were meant to be temporary solutions rather than long-term operational methods. The attack compromised protected health information for 5.6 million people, ranking as the third-largest healthcare data breach of 2024 [82]. The data that was compromised included Medical details , Payment information, Insurance details, Government Ids,Personal details, e.t.c. Ascension reported a loss of $1.3 billion in operating margin by the end of its fiscal year, with the ransomware attack being a major factor [83].

4.5 Consequences on Patient Safety, Operations and Costs

Ransomware attacks on healthcare organizations generate multidimensional consequences that extend far beyond immediate financial losses or data breaches.

4.5.1 Patient Safety and Clinical Outcomes

The most important and unique feature of healthcare ransomware is how it directly affects patient safety. Studies have shown that ransomware attacks lead to measurable consequences for patient safety. Hospitals hit by ransomware attacks saw longer patient waiting times, with the average waiting room time rising from 21 minutes before the attack to 31 minutes during it [84].

Hospitals in the same areas that were not affected also reported significant increases in patients leaving without being seen, longer waiting times, and extended stays for admitted patients as they took in patients from the impacted facilities [85]. Ransomware attacks often lead to delays in elective surgeries, diagnostic tests, and routine appointments as hospitals focus on emergency care and work with compromised systems.

These delays can have serious health implications, especially for urgent conditions like cancer diagnosis and treatment. Losing access to electronic health records hinders clinicians' ability to

check patient histories, allergies, past test results, and current medications, raising the risk of medical errors, harmful drug interactions, and incorrect treatments [86]. Even if medical devices are not directly affected by ransomware, network-wide measures such as isolating systems and disconnecting devices to stop the spread of ransomware can render essential monitoring and treatment equipment inoperative [72].

Although it is difficult to directly link patient deaths to specific ransomware attacks due to complex causation and healthcare organizations' hesitance to report negative outcomes, existing evidence indicates that ransomware attacks can and do lead to patient mortality through delayed emergency care, malfunctioning medical devices, and lack of access to vital patient information [4].

4.5.2 Operational Disruptions

In 2024, 37% of healthcare organizations took over a month to recover from ransomware attacks [66]. The average time to recover from ransomware attacks is increasing as there are increasingly complex and severe ransomware attacks. In 2024, only 22% of organizations recovered from ransomware attacks in under a week, which is a significant decrease from the 54% of organizations that were able to recover in under a week in 2022 [87]. Hospitals that are attacked by ransomware must use paper documentation, as they are unable to use their online documentation systems [88]. Additionally, hospitals must manually create prescriptions and deliver patients' prescriptions, as well as communicate their test results to the patients [78]. The Change Healthcare company is one such company that was attacked by ransomware, which resulted in thousands of provider organizations losing billing revenue across the entire United States. Attackers frequently target the data and backup systems of organizations to prevent those organizations from restoring their data and systems without having to pay the attackers' ransoms. In 2024, 95% of the healthcare organizations that were attacked by ransomware had their backup systems attacked by ransomware attackers, with 66% of those attacks being successful [65].

4.5.3 Financial Consequences

Healthcare organizations must bear the cost of responding to cybersecurity incidents, which include forensic investigators, lawyers, external cybersecurity specialists, PR professionals, individuals who will notify the media and the public, and credit monitoring services for those affected by the security breach [89].

The average cost of recovering from these attacks, not counting the ransom payments, is $2.57 million in the healthcare Industry; however, some organizations, like Change Healthcare, have paid close to $1 billion in total costs [66]. In 2024, 53% of healthcare organizations that were attacked with ransomware paid the ransom to the attackers; these organizations paid on average $4.4 million for these ransoms [65]. Only 15% paid the initial ransom amount, while 28% negotiated for lower payments, and 57% ended up paying more than what was initially asked [65].

The choice to pay ransoms involves complicated trade-offs regarding recovery speed, data safety, and ethical issues. Downtime from system failures results in lost income due to cancelled procedures, delayed billing, fewer patients, and redirected emergency services specifically, the decision to pay the ransom to these attackers involves a complex set of trade-offs for the organization. System failures due to the ransomware attacks results in lost income for those organizations due to the cancellation of medical procedures, lost billing revenue, fewer patients visiting these organizations, and emergency medical services getting redirected from these organizations [90].

Healthcare organizations lose around $900,000 each day due to these system failures and the resulting lost income [91]. Finally, healthcare organizations also must pay for system upgrades and enhancements in cybersecurity to deal with these attacks, purchase cybersecurity insurance, and lose patients and employees due to the data breaches [89]. Despite having cybersecurity insurance, healthcare organizations are seeing an increasing number of attacks that result in increased premiums for these insurance policies. Some insurance companies are limiting the policies they offer for healthcare organizations related to ransomware attacks and requiring those organizations to meet specific cybersecurity standards before they receive such insurance policies [92].

4.5.4 Workforce and Psychological Impact

Healthcare ransomware attacks pose psychological challenges to the healthcare workforce, including stress and anxiety. Around 37% of healthcare organizations reported that their workers experienced anxiety and stress regarding the possibility of ransomware attacks in the future after suffering from a data breach with a ransomware attack [65].

The combination of difficulties experienced during the attack, the concerns for the patient`s safety, and the stress of potential data breaches from those organizations creates psychological challenges for the workers. Another challenge for the healthcare workforce is staff absence caused by ransomware attacks. Almost 25% of healthcare organizations exposed to ransomware attacks reported that their staff was absent from the organizations due to the stress that the attacks created [65]. These absenteeism challenges exacerbate the difficulties that the organizations face in their operations.

Finally, the long hours that the workers are required to put in to compensate for the breakdown of their systems, the increased manual tasks required of their staff, and the emotional challenges caused by the need to provide inadequate care to their patients will result in burnout and staff turnover within the healthcare Industry.

5 Assessment of Existing Security Frameworks in Healthcare Infrastructure

5.1 Existing Cybersecurity Standards and Regulations

Healthcare organizations are required to comply with a complicated web of regulations that establish minimum security standards for protecting patient information and ensuring the continued stability of healthcare organization operations. This section looks at the main cybersecurity standards and regulations that apply to healthcare systems, especially regarding their importance in defending against ransomware.

5.1.1 Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Security compliance framework, established in 2003 and enforced by the Department of Health and Human Services Office for Civil Rights, sets national standards for safeguarding electronic protected health information (ePHI) [93]. This framework applies to HIPAA-covered entities such as healthcare providers that electronically transmit health information, health plans, and healthcare clearinghouses, along with their business associates who create, receive, maintain, or transmit ePHI for these entities [94].

5.1.2 NIST Cybersecurity Framework and Healthcare Integration

The National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a voluntary guide for organizations to comprehend, communicate, and handle cybersecurity risks. It was first introduced in 2014 as a response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," and was updated to version 2.0 in February 2024 [95]. The NIST Cybersecurity Framework 2.0 is structured around six main functions, and they are Govern, Identify, Protect, Detect, Respond and Recover.

5.1.3 HHS 405(d) Program and HICP

The Health Care Industry Cybersecurity Practices (HICP) were created under Section 405(d) of the Cybersecurity Act of 2015. They offer voluntary cybersecurity guidelines specifically designed for healthcare organizations [96]. The HHS 405(d) program unites healthcare and cybersecurity professionals from both government and private sectors to create, share, and support the application of cybersecurity best practices. The HICP outlines ten cybersecurity

threats that are the most significant risks to healthcare organizations. Five of these threats are directly linked to ransomware and related attack methods: email phishing attacks, ransomware attacks, loss or theft of equipment or data, insider data loss or theft, and attacks on connected medical devices.

For each of the threats to health information that are identified in the HICP, various technical and operational security measures are established for healthcare organizations of all sizes. The Cybersecurity Act of 2015 specifically recognizes the practices established by HHS 405(d) and the NIST Cybersecurity Framework as "recognized security practices." The use of these practices is a means of showing the healthcare organization's good faith attempts to implement the actions necessary to provide reasonable cybersecurity protection to the organization's systems and networks [94]. These recognized security practices can be used in the determination of whether a healthcare organization is to be held liable for any cybersecurity incidents. Thus, these practices can be used to provide a defense against cybersecurity lawsuits, encouraging healthcare organizations to adhere to the guidelines established in the HICP.

5.1.4 Additional Healthcare Cybersecurity Regulations

Beyond the HIPAA and NIST frameworks, there are other regulations that impact the cybersecurity of healthcare organizations.

- FDA Medical Device Cybersecurity Guidance: The Food and Drug Administration has published guidance for medical device manufacturers regarding cybersecurity, both prior to and after the release of the medical devices that they manufacture. The FDA requires these manufacturers to identify and resolve any cybersecurity vulnerabilities or incidents relating to the medical devices that they manufacture. Programs for the disclosure of any discovered vulnerabilities are to be implemented, as are programs to install updates and patches to those devices to resolve any discovered vulnerabilities [97].
- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) CIRCIA: The CIRCIA was enacted in 2022 and requires the individual's healthcare organizations that are classified as critical infrastructure within the United States to report any cyber incidents and ransom payments made to those critical infrastructure organizations to the Cybersecurity and Infrastructure Security Agency (CISA) [98].

- Medicare Promoting Interoperability Program: Healthcare providers that are considered to be participating in the Medicare program are required to meet certain objectives and measures regarding their implementation of electronic health record (EHR) technology, including performing risk analyses of those EHR technology systems [99]. Should they not meet these requirements, adjustments will be made to the payments that are made to those healthcare providers as part of the Medicare program.

5.2 Assessment of Current Defense Mechanisms

Healthcare organizations employ a variety of technical and operational defence mechanisms to protect themselves against ransomware and other cyber threats. Defence mechanisms can be divided into several primary categories

5.2.1 Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) platforms represent a significant advancement compared with antivirus software. EDR software provides monitoring, detection, and response features for endpoint devices in a network [100]. Endpoint detection and response software gathers information from endpoint devices, analyses the information to detect potential security threats to the network, and allows for the response to those detected threats. In the healthcare Industry, there are several issues that can be tackled with EDR software. The healthcare Industry includes various types of endpoint devices, from desktop and laptop computers within clinics to the mobile devices used by healthcare professionals and the servers that run the IT applications within these facilities [101].

With EDR software, healthcare facilities can detect threats such as ransomware that would typically result in important files getting encrypted, changed across the network, credentials being stolen, systems moving laterally within the network without permission, and security measures getting disabled. There has been a significant amount of progress in the healthcare Industry in the deployment and utilization of EDR technology.

According to the Picus security report for 2024, the effectiveness of EDR software in healthcare environments increased by 20 percentage points from 56% in 2023 to 76% in 2024 because of the significant investments that the healthcare Industry has made in the area of security validation and endpoint protection software [101]. This percentage indicates that healthcare

facilities are effectively implementing EDR technologies into their security operations. Nonetheless, there are still challenges for the implementation of EDR software within healthcare facilities.

Many medical devices that are utilized in these facilities are older and cannot accommodate the installation of the EDR agent software [72]. Furthermore, many of these healthcare facilities are experiencing alert fatigue as they are receiving such a high number of alerts from the endpoint devices within their network that their security staff is becoming overwhelmed in their response to these alerts.

5.2.2 Security Information and Event Management (SIEM)

SIEM platforms are tasked with the collection and analysis of log data from a variety of sources within the healthcare IT field [102]. These systems provide a centralized view of security events, correlate events from different sources to identify complex attack patterns, automate alerts for suspicious activities, and facilitate incident investigations through searchable log repositories.

For ransomware protection, SIEM platforms can identify attack indicators throughout different stages of the ransomware lifecycle, including initial compromise via phishing or credential abuse, reconnaissance activities like network scanning and Active Directory enumeration, lateral movement between systems using stolen credentials, data exfiltration activities that create unusual network traffic patterns, and pre-ransomware actions such as deleting backups or disabling security tools.

However, the implementation of these platforms into the healthcare field presents some challenges to their effectiveness. For instance, the Picus security report for 2024 revealed that the number of alerts generated for healthcare organizations fell from 23% in 2023 to only 5% in 2024, despite improvements in the number of logs collected by those organizations [101].

This indicates that healthcare organizations are not effectively utilizing these alerts. Some of the reasons for the challenges of the effectiveness of these systems within the healthcare Industry include the lack of cybersecurity staff and expertise to set up detection rules, adjust alert thresholds, and investigate alerts.

5.2.3 Extended Detection and Response (XDR)

Next-generation detection (XDR) platforms indicate the advancement that has been made in EDR and SIEM technologies by combining telemetry data from numerous domains into a cohesive security operations platform [102]. XDR platforms allow for the integration and correlation of security data from various domains within an organization to provide increased visibility into security threats while minimizing false positives, automating investigation processes, and responding to threats across the organization's security tools.

Healthcare organizations are turning to these XDR platforms as a means of resolving the integration and alert fatigue that results from using separate EDR, network detection, and SIEM tools. The capability of these platforms to correlate events from multiple domains is especially useful in detecting instances of ransomware that may affect different systems within the organization and use various methods to avoid being detected by only using security systems dedicated to monitoring for specific types of threats.

The benefits of using XDR platforms in the healthcare Industry include having a unified view of the security of the organization's IT systems without having to purchase and manage multiple separate security platforms. Additionally, healthcare organizations may find their analyst's workload reduced as the automation of certain tasks can present only the threats of most concern to the organization's security team.

Other benefits of using XDR platforms include the ability to detect and respond to security threats more quickly within the healthcare Industry, as well as to increase the accuracy with which those threats are detected [102]. Despite the benefits that can be provided to healthcare organizations by implementing these platforms, the adoption of XDR platforms is still in its early stages.

Barriers to adoption by healthcare organizations include the high costs of XDR platforms, the vendor lock-in restrictions that many manufacturers of these platforms require organizations to use their own security products for each monitored domain, the complexity of implementing such systems into an already well-established security infrastructure for healthcare organizations, and the need for personnel with appropriate skill levels to effectively operate and monitor the XDR platforms for their organization.

5.2.4 Zero Trust Architecture

Zero Trust Architecture (ZTA) indicates a major change from traditional security models to a model based on the idea of "never trust, always verify" [100]. Zero Trust Architecture assumes that no user, device, or application is to be trusted with access to any resources by default. Each entity must be continually verified before being permitted access to any resources of the organization. The following are the key components of Zero Trust that help defend against healthcare ransomware

Identity and Access Management (IAM) that verifies the identity of each entity attempting to access the ePHI in question. Such methods include using multi-factor authentication, single sign-on with robust authentication protocols, and risk-based conditional access to ensure that only authorized parties can access the ePHI [103].

Micro-segmentation is when technology divides the IT and network infrastructure into small segments with access controls between each segment [103]. Should a cyberattack occur on one segment of the network, the others will remain unaffected due to the inability of the attack to traverse the access controls between segments

Continuous monitoring and analytics is when an organization can continually monitor the activities of each user, device, and network for any unusual activity that may indicate a cyberattack [102]. Zero Trust Architecture continuously evaluates the trustworthiness of each entity in the network based on their current activities instead of the initial steps to access the network.

Least Privilege Access means each user or device is given the minimum level of access required to perform the functions of their provided role [100]. Should a cyberattack occur with the gaining of access to a user with least privilege access, the damage is likely to be limited to the resources of that initial user only

5.3 Limitations in current defense mechanisms

Despite the use of several advanced defence systems in the healthcare Industry, the sector continues to be plagued by ransomware attacks.

5.3.1 Detection and response gaps

The growing divide between the prevention and detection capabilities of the healthcare Industry is arguably one of the weakest aspects of the industry's cybersecurity. According to a report from cybersecurity firm SonicWall, while the healthcare Industry has increased its prevention scores to 76% in 2024, its alert score has dropped to only 5% [101]. This indicates that the industry is failing to effectively produce alerts regarding potential security threats. As a result, ransomware attackers can remain within the system for long periods before being detected. For example, during the Ascension Health ransomware attack, attackers remained undetected for more than two months, from the initial breach on February 29, 2024, until it was discovered on May 8, 2024, [104].

During this time, the attackers were able to survey the network, identify points of interest, steal data, and prepare to deploy the ransomware to inflict as much damage as possible. Some of the reasons for the gaps in detection and response within the healthcare Industry include the lack of Security Operations Centre (SOC) staffing. Many healthcare organizations are suffering from a staff shortage in their SOC departments. For example, many hospitals have SOCs that are understaffed and unable to provide round-the-clock security monitoring for their networks.

Consequently, these organizations cannot dedicate the resources necessary to investigate security alerts or to create custom detection rules for their networks. The number of alerts produced by the SOC tools is also another gap in healthcare detection and response. Many security tools produce healthcare organizations a huge number of alerts. These alerts can lead to alert fatigue for security analysts in healthcare organizations whose SOC is understaffed [101].

Furthermore, many healthcare organizations lack the integration of threat intelligence tools that would allow them to monitor for cybersecurity threats specifically targeting the healthcare Industry [74]. The default security rules implemented in the SIEM and EDR platforms that numerous healthcare organizations use do not provide custom detection rules that account for threats specific to the healthcare environment [101]. Thus, the creation of detection rule libraries would require a deep understanding of both cybersecurity threats and healthcare environments, both of which are areas of knowledge lacking within the healthcare Industry.

5.3.2 Backup and recovery challenges

Backup systems act as the last line of defence against ransomware attacks and allow organizations to restore their systems and data without having to pay the attackers' ransom demands. As such, ransomware attackers specifically target the data backup systems of the organizations they target. For example, in 2024, attackers attempted to compromise the backup systems of healthcare organizations in 95% of the ransomware attacks on these organizations, yet they were successful in compromising the data backups in 66% of these attacks [65].

Healthcare organizations encounter various challenges with their backup systems, including but not limited to accessibility of those backup systems. Traditional backup systems for healthcare organizations store their data on accessible networks that the ransomware attacks can access and encrypt. Even if the data is protected, the ransomware can still encrypt the backup catalogues and systems of these organizations [105].

Another challenge for these organizations is the fact that they do not often test their backup systems to ensure the data is backed up successfully. When these organizations are attacked by ransomware, they often encounter issues with the backed-up data, including corruption and ineffective backup and restoration procedures. Additionally, these organizations may encounter challenges in recovering the amount of time that they require for recovery from a ransomware attack.

Because healthcare organizations require high availability of systems and data to provide necessary services to their patients, they require that their data and systems are restored rapidly in the case of a cyber-attack. However, restoring these systems after a ransomware attack usually takes several days or even week [66].

The high demands of the healthcare Industry for data that must be stored and accessed 24/7 each can pose a challenge for the organizations because backing up and restoring data amounts to terabytes or petabytes requires significant technical expertise. Finally, another challenge for these organizations is that although cybersecurity experts recommend that healthcare organizations keep backups that are located in a way that makes it impossible for ransomware to access or alter that data, many of these organizations have yet to implement such backup

systems due to the high costs, technical challenges, and operational limitations of the industry as a whole.

5.3.3 Legacy System Vulnerabilities

Healthcare settings have a lot of old infrastructure that poses a security threat. About one in five connected healthcare devices uses outdated operating systems that the manufacturer no longer supports and provides security updates [26]. The outdated operating systems lead to issues regarding ransomware protection for these devices. For instance, because the older versions of medical devices and systems are typically released with the understanding that updates must be performed prior to reintroducing the devices into a healthcare facility, the systems cannot be updated to fix any security vulnerabilities that are discovered after their initial release [25].

Additionally, the manufacturers may no longer offer security update contracts or warranties for these systems, meaning that the healthcare facilities cannot install updates to these systems. Furthermore, these old systems cannot be configured to run EDR security agents or systems that can authenticate users to those systems [72].

To combat the threats that come from these outdated devices, the organizations must implement compensating controls. This typically involve segmenting the networks to which these devices are connected so they are unable to pose a threat to the remainder of the organization’s information systems. Replacing these outdated medical devices and systems incurs a significant financial investment and poses challenges to the medical facility’s staff. Because of these challenges, medical facility staff are unlikely to want to replace these devices and systems out of resistance to the changes that would have to be made to their current processes.

6 Gaps in Security against Ransomware attacks

There are specific gaps within the topic that indicate the field's inability to effectively assist organizations in their ransomware defences.

6.1 Insufficient understanding of Ransomware attack chains in healthcare

Beyond the lack of understanding of general ransomware attacks, there is also a lack of understanding of how those attacks specifically occur within healthcare environments [57]. For instance, medical device manufacturers have published research notes on the vulnerabilities of their devices. However, there is limited research on how cyberattacks take advantage of these noted vulnerabilities [72].

Additionally, some research indicates that attackers may perform their attacks at specific times related to healthcare facilities. For instance, would an attacker target a hospital during shift changes, flu season, or on the weekends when there are fewer staff members? While there is some evidence that attackers do take these factors into account, there is limited research on this topic [59]. Another area of lack of research is the healthcare supply chain. For instance, Change Healthcare is a company that provides software as a service to numerous healthcare organizations. If an organization like Change were to be attacked by ransomware, what implications would that have for those other organizations that rely on the same software as Change Healthcare?

There is limited research on how attackers find these critical supply chains in the healthcare Industry [77]. Related to data exfiltration is the question of what data is targeted by attackers. If an organization is attacked by ransomware, the attackers often exfiltrate the organization's data before they begin to encrypt its systems. What data is exfiltrated by attackers? Does it relate to health records, financial data, or other sensitive healthcare records and information of those organizations? If that information can be understood, healthcare organizations may be able to develop better defences against ransomware attacks. Overall, the lack of understanding of these specific details of ransomware attacks indicates that healthcare organizations lack the threat intelligence they require to develop effective defence strategies against ransomware attacks.

6.2 Lack of Validated Risk Assessment Methodologies

When individuals within the healthcare security industry are asked to share their approach to assessing the threat of ransomware, there are a variety of answers that will be given. Some will cite their use of established cybersecurity frameworks, such as NIST. Others will utilize frameworks from other industries, and many will have developed their own unique methods for such an assessment [106]. In the healthcare Industry, however, there is an absence of validated techniques for assessing the risk of ransomware attacks. One main reason for this lack of established methods is that risk assessments in healthcare must include elements often overlooked by other industries. For instance, risk assessments in healthcare must consider the potential impact on patient safety and health.

Questions that must be answered by such a risk assessment framework include, for example, whether a ransomware attack on the EHR system will result in negative patient outcomes [59]. Yet most existing risk assessment frameworks treat all systems within the facility the same. In addition, the systems within a healthcare facility are often interconnected in ways that are overlooked by most existing risk assessment framework [107]. The EHR system, for instance, may be dependent on the network, which in turn depends on the facility's power distribution system. Alternatively, the pharmacy systems may depend on the EHR system and automated dispensing cabinets. Other departments that may be interconnected with the EHR system include the laboratories and their diagnostic equipment. An assessment of these interdependencies and their risks is often omitted by most risk assessment frameworks.

Finally, another complex element of risk assessments for healthcare IT systems is the recovery time for the affected systems. How long will it take to recover the data for the EHR system? There may be additional steps required to fully recover the EHR system, such as validating the data, performing additional software checks and tests, power system checks, and potentially retraining staff who used the EHR system after recovery. In many cases, these types of attacks are only recognized after they have occurred, and facilities discover that their estimated recovery time for the EHR system was much shorter than what is required to restore the system to continue providing patient care [106].

Because of the lack of proper risk assessment tools for healthcare IT systems, individuals within an organization often find themselves hard pressed to make informed decisions regarding their

security. For instance, they may have spent significant resources to safeguard vital systems that are not critical for patient care, while neglecting to protect the systems that are critical for providing the required care. Additionally, due to underestimated risks and the complexity of recoveries for those systems, they may find themselves panicked and unprepared in the event of a ransomware attack on their IT system.

6.3 Gap between Security Research and Clinical Practice

Walk into any IT security office in a hospital, and you will likely hear complaints about the gap between academic cybersecurity research and real-world clinical situations. Many of the solutions recommended in research are ideal in theory but unworkable in practice due to issues like usability. Security measures that require three extra steps to authenticate users may sound reasonable to IT personnel. However, adding such steps to the clinical workflow during a cardiac arrest will prompt clinicians to seek alternative authentication methods that will undermine the security of the system altogether [53].

Most cybersecurity research focuses on the effectiveness of a security measure rather than the usability of that measure within a hospital setting. As a result, many solutions recommended for hospitals are ones that cannot be implemented within that organization. Another area that is largely ignored in academic cybersecurity research is the operational impact of suggested security measures. Most security suggestions require hospitals to take the organization's systems offline to implement the security. Hospitals, however are required to be operational around the clock. Taking a patient monitor or ventilator offline will threaten the lives of patients who are monitored or ventilated in that hospital. Any research that suggests security solutions that require taking systems offline does not consider the operational reality of hospitals in its research [107].

Many cybersecurity research studies do not consider how the regulatory requirements of medical devices threaten the ability of the research to be implemented in hospital environments. Medical devices are regulated by the FDA, and any changes to those devices require validation and documentation by the manufacturers to ensure that the changes will not threaten the safety and effectiveness of the devices [97]. Any research that suggests hospitals should immediately patch all of their medical devices to fix security vulnerabilities does not consider the possibility of regulatory obstacles to such patching. Such considerations would include the regulatory limitations on the patching of medical devices.

Cybersecurity research largely ignores cost factors in its research efforts [55]. Most research studies propose a variety of expensive cybersecurity tools and platforms to hospitals to increase security. Yet, community hospitals have very tight budgets and cannot afford to purchase the various security tools recommended by research studies. Such recommendations do not consider the financial challenges that hospitals face in implementing such solutions.

The complexity of implementing recommended security solutions is also largely ignored in academic research. Most of the suggested security measures require technical skills in the healthcare organization that are not common and not easily found. These solutions may require the organization to have certain resources such as a security operations centre and staff members that are available around the clock to deal with cybersecurity challenges, resources that are largely absent in most healthcare organizations [54].

There needs to be better collaboration between academic researchers and healthcare practitioners to address the gap between research and practice. Research should be conducted into implementation science to determine not just if a security solution will be effective in an organization, but how to apply the solution in that organization effectively. Such research would pay closer attention to the operational, regulatory, financial, and workflow impacts that certain security solutions will have on the organization that implements them [52].

6.4 Insufficient Sociotechnical Perspectives

For too long, cybersecurity within healthcare has mainly been viewed as a technical issue [51]. Upgrading firewalls, using new cybersecurity detection tools, and upgrading vulnerable systems are steps that should be taken to improve the cybersecurity of health institutions. However, these steps are not nearly enough. The resilience of health institutions against ransomware attacks is dependent upon the interaction of several factors ranging from their technology to their culture [108]. The study of these factors is surprisingly scarce within cybersecurity research. The aspect of an organization's culture is rarely discussed in cybersecurity research literature. How do the leadership of an organization view cybersecurity? How do different departments within that organization interact with one another? How does the culture of that organization translate into how they allocate funding towards their cybersecurity programs compared to other programs within the organization? These types of questions are rarely asked of any organization in the healthcare sector.

Furthermore, the human factor in cybersecurity is also often overlooked [53]. How do clinicians and staff members interact with cybersecurity in their everyday jobs? How do the dynamics within a staff team impact cybersecurity within that organization? Are there any psychological elements within the staff that impact their cybersecurity knowledge and actions? These types of questions have been explored by other research communities yet are overlooked entirely by healthcare cybersecurity research.

Finally, there are also questions regarding governance of cybersecurity within healthcare organizations that remain unanswered [108]. How should cybersecurity be allocated as a job within the organization? How should governance models ensure oversight of cybersecurity by the board and executives of the organization? On what terms should the organization be held accountable for its cybersecurity practices? These types of questions are important and need to be addressed in healthcare cybersecurity research.

Additionally, training and awareness programs for employees in healthcare organizations are surprisingly limited in their research studies [51]. What types of training have been successful in changing the behaviour of staff members in healthcare organizations? How should training for cybersecurity vary based on the role of the staff member within the organization? How can the effectiveness of training be retained over time? These types of questions may be answered through the viewpoints of the field of behavioural economics, yet such perspectives are hardly found within existing healthcare cybersecurity research studies [108].

To answer these and other emerging questions, interdisciplinary methods must be used within cybersecurity research [51]. Cybersecurity researchers must work alongside researchers from fields like psychology, behavioural economics, and the improvement of implementations of programs within organizations to address these issues. While collaboration between these groups is currently rare, it is one that is emerging as essential to addressing the cybersecurity challenges facing healthcare organizations today.

7 Integrated Cyber Resilience Model

The gaps in this analysis of the current methods for establishing cyber resilience in healthcare indicate a crucial need for a unified cyber resilience model that is specifically tailored to the types of smart hospitals at risk of ransomware attacks. The current methods for securing healthcare are too scattered, focusing instead on individual aspects of cybersecurity rather than establishing complete models that cover all necessary areas while considering the limitations of the healthcare Industry itself.

7.1 Characteristics of effective resilience models

What then, would a successful model for establishing cyber resilience in healthcare look like? There are several features that would be necessary for such a model. First, the model should be as comprehensive as possible in covering all aspects of ransomware and cyber resilience. For example, many current models invest significant resources into preventive measures for cyber resilience but fail to consider methods for detecting, responding to, and recovering from cyberattacks [107].

Because of this, if an attack penetrates the preventive measures created for healthcare organizations, the institution is often left unprepared for the attack. Secondly, such a model would need to be contextualized for the healthcare Industry in particular; there are numerous adjustments that would need to be made to any generic framework to account for the specifics of healthcare [106].

Such aspects may include considerations of 24/7 operations of healthcare facilities, the need for certain systems to be operational within the facility, regulatory requirements of healthcare institutions, the need to secure access to medical devices, and the resource constraints of healthcare institutions. Thirdly, a successful model would include provisions for integrating the various stakeholders of a healthcare institution. These stakeholders may include the institution's IT departments, its security teams, its clinicians who must ensure that the model does not impact the provision of quality care to patients, the medical device manufacturers that must ensure device security, various regulatory agencies, and the patients of the institution [55].

Fourthly, the model would need to be scalable and flexible to account for the diversity within the healthcare Industry. For example, one model for a large academic medical centre may be

different from another model for a small rural hospital due to the different resources, capabilities, and limitations that exist between these two types of facilities [56]. Additionally, the model should focus on continuous improvement of the model itself. Any model that is created is likely to become obsolete in the face of the rapidly evolving nature of ransomware attacks and cyber threats [52]. Therefore, a successful model should include methods for evaluating the model over time, adjusting it to new information and new threats to the healthcare Industry and its data.

7.2 Integration across Cybersecurity Domains

Healthcare organizations have traditionally managed cybersecurity in separate areas of the organization; for example, one area might manage network security while others manage endpoint security and identity management [109]. These separate areas for cybersecurity management are vulnerable to attacks from cyberthreats like ransomware. To build effective models of cybersecurity resilience, the organization needs to have a unified view of all these separate areas.

Security teams need to have a complete understanding of the situation across the organization to take appropriate actions to address any threats [107]. Another aspect of integrating these separate security systems is the need for each of these systems to work together to create a system of defences of various depths to cover for possible failures in any of those other layers of the security system [109]. For instance, network segmentation can prevent the spread of a threat to other systems on the network, endpoint detection can identify systems that are under threat that cannot be protected by other means, and identity management can limit the access of any threatened credentials to the data of the organization. Taken together, these security systems provide for the overall cybersecurity resilience of the organization.

Furthermore, the organization also needs to have synchronized response capabilities for each of these areas. If a system is identified as having ransomware within it, the response to that system should occur simultaneously across each of the areas. For instance, the system can be isolated from the network, the system can be disabled from using any recognized credentials, and any data that could potentially be at risk from that system can be safeguarded [107].

Comprehensive recovery planning is also crucial. Business continuity strategies must consider the interdependencies among IT systems, medical devices, facility infrastructure, and third-

party services [106]. Restoring the EHR while laboratory systems are still down does not allow normal operations because the EHR relies on lab results. Recovery plans must adopt these system's thinking approach.

7.3 Addressing the people, process and technology

An effective resilience model needs to focus on people, processes, and technology which are the essential trio of organizational capability [108]. Focusing too much on technology while ignoring people and processes results in predictable failures. Technology offers vital tools, but advanced security tools are useless without skilled individuals using them properly [51].

A top-tier SIEM produces a lot of data, but without trained analysts who comprehend healthcare operations and can tell normal activities from unusual ones, that data becomes noise instead of valuable insights. People are both the biggest asset and the most significant risk [53]. Well-trained, security aware staff can detect security threats and respond appropriately to security incidents to increase the overall security resilience of the organization. Staff that is not properly trained or overwhelmed with dealing with security incidents themselves can easily fall into phishing scams, make mistakes in the configuration of systems, or make further developments in an incident response that make the problem worse.

Overall processes are essential for providing effective security to an organization's systems [106]. Good processes will help to ensure that security measures are consistently applied to the organization's systems rather than depending upon the individual security staff members to know and apply those measures. Good processes will also help to prevent future security incidents by learning from past incidents. Finally, processes can help to respond to security incidents during periods of high stress when plans cannot be made spontaneously.

Effective models for increasing the security resilience of an organization will dictate the development of each of these three components of security [51]. Such models will include suggesting specific security technologies to implement but also focusing upon the development of the organization's staff and increasing their security capabilities. Such models will also dictate the creation of specific governance processes for the organization's systems. Each of these three components must be developed in a coordinated way to provide the organization with improved security.

7.4 Regulatory alignment and Compliance Integration

Healthcare organizations are already burdened by numerous regulations. Adding cybersecurity requirements to the plethora of regulations that organizations must adhere to creates challenges in the implementation of cybersecurity measures unless there is a focus on regulatory requirements [94].

The models for enhancing resilience should aid organizations in meeting these regulations rather than creating friction between the two areas [106]. For instance, complying with the HIPAA Security Rule requires many of the same cybersecurity capabilities as ransomware resilience requires. Combining the regulatory compliance requirements with cybersecurity resilience models will allow organizations to meet both requirements.

The HIPAA amendments for December 2024 requires all organizations to implement network segmentation to increase the cybersecurity protections of their networks [103]. Resilience models for the healthcare Industry must keep up with regulations and allow organizations to understand how the compliance requirements relate to and support one another. Additionally, regulatory bodies like the FDA have published requirements for medical devices that use AI, such as the CIRCIA incident reporting requirements.
State regulations require organizations to notify patients of any data breaches that occur within their systems, as well as rules related to Medicare programs and the meaningful use of technology in healthcare organizations [94]. These regulations all create compliance requirements for healthcare organizations that relate to cybersecurity. Models that assist organizations in navigating these regulations while enhancing their cybersecurity will provide a valuable function to these models.

7.5 Metrics and Maturity Assessment

The old saying in the management world holds true for the topic of cybersecurity. “You can't manage what you don't measure.” Yet, measuring the effectiveness of cybersecurity in an organization can be challenging [56]. Any model that intends to reflect the cybersecurity resilience of an organization must include a means of measuring that cybersecurity in relation to their current state and to provide reports to the organization’s leadership. Table 1 provides a metrics table that can be used to measure the effectiveness of cybersecurity in any organization.

Table 1 showing an effective metrics and assessment framework

Security Domain	Security Metric	Description	Purpose / Measurement Goal
Technical Security Metrics	Number of Vulnerabilities	Measures identified vulnerabilities within systems, applications, and networks.	Evaluates exposure to cyber threats and weaknesses.
Technical Security Metrics	Patch Management Status	Percentage of systems updated with latest security patches.	Assesses system maintenance and vulnerability reduction efforts.
Technical Security Metrics	Security Control Coverage	Measures extent of deployed security controls across infrastructure.	Determines effectiveness and completeness of security implementation.
Technical Security Metrics	Cybersecurity Hygiene	Evaluates adherence to security best practices such as password policies, MFA, and secure configurations.	Reflects overall technical security posture of the organization.
Operational Security Metrics	Incident Detection Time	Measures taken time to identify a cybersecurity incident.	Evaluates monitoring and threat detection capabilities.
Operational Security Metrics	Incident Response Time	Measures time required to respond after incident detection.	Assesses efficiency of incident response processes.
Operational Security Metrics	Backup Frequency	Measures how often organizational data is backed up.	Ensures data availability and ransomware recovery readiness.
Operational Security Metrics	System Restoration Time	Measures time needed to restore critical systems after disruption.	Evaluates disaster recovery and business continuity capabilities.
Organizational Maturity Metrics	Cybersecurity Roles Maturity	Assesses clarity and effectiveness of cybersecurity responsibilities and governance.	Evaluates organizational structure and accountability.
Organizational Maturity Metrics	Risk Management Process Maturity	Measures effectiveness and maturity of risk assessment and mitigation processes.	Determines ability to manage and reduce cybersecurity risks systematically.
Organizational Maturity Metrics	Cybersecurity Training Maturity	Evaluates employee awareness and frequency of cybersecurity training programs.	Measures human-factor resilience against cyber threats.
Threat Landscape Metrics	Threat Awareness Level	Measures organization's understanding of current cyber threats targeting its environment.	Evaluates threat intelligence and situational awareness capabilities.
Threat Landscape Metrics	Threat Monitoring Capability	Assesses ability to continuously monitor emerging threats and attack trends.	Improves proactive defense and preparedness.
Cybersecurity Resilience Metrics	Overall Cybersecurity Resilience	Combines technical, operational, and maturity indicators into an overall resilience assessment.	Measures the organization's ability to prevent, respond to, and recover from cyber incidents.
Cybersecurity Resilience Metrics	Continuous Improvement Capability	Measures how effectively the organization improves security processes over time.	Supports long-term cybersecurity maturity growth.
Maturity Model Assessment	Current Security Maturity Level	Determines the organization's current cybersecurity maturity stage.	Provides benchmark for improvement planning.
Maturity Model Assessment	Security Enhancement Recommendations	Identifies gaps and recommended improvements.	Guides strategic cybersecurity development and resilience enhancement.

8 Actionable Recommendations for Smart-Hospitals Stakeholders

8.1 Healthcare providers and Administrators

Healthcare providers are on the front line of the fight against ransomware. They experience the impact of a successful attack on the health care organization. Most hospitals are not ransomware-secure firms with unlimited budgets. Hospitals are organizations trying to protect their health care facilities with limited resources and knowledge.

8.1.1 Adoption of Recognized Cybersecurity Frameworks

One of the smartest decisions healthcare organizations can make is to adopt a recognized cybersecurity framework. In many ways, adopting these frameworks is a legal safeguard. The Health Information Technology for Economic and Clinical Health (HITECH) Act provides a safe harbour for healthcare organizations that adopt recognized cybersecurity practices; the Department of Health and Human Services is required to consider the adoption of those recognized practices when determining penalties that may be placed upon those organizations [110] Thus, by adopting these frameworks, organizations may not only be protected from the impact of ransomware attacks on the organization, but also from potentially severe penalties if those attacks occur anyway. There are three frameworks that are particularly important for healthcare organizations, and they are

- HHS Cybersecurity Performance Goals (CPGs): These were specifically developed for the healthcare Industry through the collaboration between HHS, CISA, and the Healthcare and Public Health Sector Coordinating Council [111]. The value of the CPGs is that they focus on the most impactful practices to defend against the most common attack methods targeting the healthcare Industry: vulnerabilities, phishing emails, and stolen credentials. These are the types of attacks that were seen in both the Change Healthcare and the Ascension attacks. Furthermore, these goals are designed for organizations of all sizes [112].
- Health Industry Cybersecurity Practices (HICP): This program details the top ten threats to the healthcare Industry's networks, including the threat of ransomware. The most recent edition of the HICP was published in 2023 and consists of a main document with two technical volumes of information. There are resources available for organizations of all sizes utilizing the HICP, though there are separate recommendations for organizations that have more resources within the healthcare Industry. For instance,

there are separate recommendations for organizations that have an IT staff of two persons compared to healthcare organizations with more extensive security departments [113].

- NIST Cybersecurity Framework 2.0: This framework was launched in February 2024 with the goal of having a common language to discuss cybersecurity among organizations of all shapes and sizes. The NIST framework consists of six functions that work together as a strategy to enhance cybersecurity for organizations: govern, identify, protect, detect, respond, and recover [114]. Furthermore, the updated publication of NIST SP 800-66r2 maps the NIST Cybersecurity Framework 2.0 to the requirements of the HIPAA Security Rule, indicating how implementing this framework will aid in meeting those compliance requirements [94].

The EU does not have a single framework that all organizations must comply with. Instead, there are general directives and guidelines for each sector. Hospitals must comply with the NIS2 directive but also follow specific guidelines from ENISA, such as Cyber Hygiene in the Health Sector handbook. Others include the EHDS (European Health Data Space) regulation and the Cyber Resilience Act (CRA). The important part is to choose one framework and use it consistently, instead of selecting bits from various sources or letting it sit unused. Those that have implemented these frameworks report that they have created more organized approaches to cybersecurity for their organization [56].

8.1.2 Implementation of Basic Cyber Hygiene Controls

Many healthcare organizations are targeted by ransomware not due to advanced zero-day exploits, but because they lack basic security measures. The proposed changes to the HIPAA Security Rule by HHS in December 2024 highlight this issue by making previously 'addressable' controls mandatory, including network segmentation. The mandatory controls include implementing Multi-Factor Authentication (MFA) everywhere. The Change Healthcare attack was partly successful because compromised credentials allowed access to a remote gateway that did not have MFA. This single gap in control led to one of the most severe cyberattacks in healthcare history. MFA should secure every remote access point, including VPNs, cloud applications, administrative accounts, and privileged access. While staff may grumble about the extra step, MFA effectively prevents most credential-based attacks, making it one of the best security investments available [115]. In 2025, the exploited vulnerabilities of

systems became the top technical cause of ransomware attacks on healthcare systems, accounting for 33% of all incidents [22]. These vulnerabilities were known and had patches that could have been installed on the systems to fix the issues for months, if not years, prior to the occurrence of these attacks. The issue does not lie in the availability of patches for these vulnerabilities, but rather the failure of the organizations to promptly install such patches. The processes for healthcare systems to patch their systems should consider the risks that each system poses to the network. Systems that are exposed to the internet and systems with vulnerabilities should be patched first. Additionally, while the FDA requires more careful management of the patches for their medical devices, they still have the same requirements to establish processes for patch management for their networks.

Another stipulation of the HIPAA Security Rule updates will be network segmentation to prevent ransomware from spreading [103]. While only seven of Ascension's 25,000 servers were originally hit with the ransomware, it made its way to the rest of their systems due to inadequate segmentation policies [82]. One way to segment networks within healthcare institutions is to ensure that all medical devices are segmented from the IT networks, guest Wi-Fi networks are segmented from the systems that receive patients, and various facilities within an organization are segmented from one another. Furthermore, segmented networks could include features that make it harder for individuals to laterally move from one network to the next within the organization [100]. Though network segmentation sounds good in theory, it takes time to create segmented networks for all vital systems within the healthcare institution.

The effectiveness of preventive measures used in healthcare organizations increased by 20 percentage points between 2023 and 2024, bringing the total to 76% [101]. This result reflects a shift toward employing endpoint detection and response systems on a higher scale. All devices within a healthcare organization should have endpoint protection software. This can range from software that detects the presence of ransomware to antivirus and more. However, medical devices cannot be protected the same way as the other devices in the organization. Instead, those systems would be protected by creating segmented networks for such devices, implementing network traffic monitoring for those devices, implementing access controls, and performing regular vulnerability assessments of those systems [20].

8.1.3 Development and Testing of Incident Response Plan

When ransomware attacks, having a thorough incident response plan can ultimately mean the difference between effectively managing the situation and chaos unfolding before the organization's eyes. During the 2024 attack season on healthcare organizations, many were found to be using outdated or non-existent incident response plans to prepare for such attacks [116]. An effective incident response plan for ransomware attacks in healthcare must include several elements, such as

- Pre-Designated Response Teams with Clear Roles: Who will decide to take the systems offline? Who will decide who gets to tell patients about their cancelled appointments? Who will deal with the media? What teams will get to work with law enforcement? These answers cannot be asked during a ransom attack. Teams should include individuals from the healthcare organization who have an understanding of the impact of an attack on healthcare delivery, those who understand the technical aspects of the organization's network, legal advisors, individuals in charge of communication, and the executives in charge of making the tough call about whether or not to pay the ransom to regain access to the organization's data [107].
- Effective Downtime Procedures: Every hospital has procedures in place in case there is an IT system failure. However, those procedures were created for downtimes caused by system crashes rather than the challenges of ransom attacks that last for several days. The procedures failed in many of the attacked organizations during the past year when the IT teams were required to work beyond a few hours without these procedures established for ransom attack [48]. There needs to be a plan for downtimes in essential IT systems for the hospital, such as medication orders systems, lab results systems, patient history access, scheduling, registration, and billing systems. When the EHR system was down during the Ascension hospital attack, many of these systems failed, and the hospital was unable to provide the level of care to its patients [117].
- Backup Systems That Can Truly Restore: In 2024, ransomware attackers attempted to compromise healthcare organizations' data backups 95% of the time and were successful in obtaining access 66% of the time [65]. As a result of this attack, healthcare organizations found out that their data backups were also compromised and would take several weeks to restore their data from backup drives. To avoid these challenges, healthcare organizations should establish best practices to protect their data backups.

This includes ensuring backups are created offline or in air-gapped networks to avoid access by ransomware, backups that are immutable to prevent ransomware from corrupting the backup, regularly testing backup systems to restore data (at least once per quarter), creating multiple versions of data backups for data redundancy, and ensuring documentation of backup systems that any qualified IT staff members within the organization can follow to restore their data [56].

- Communication Plans for Various Audiences: During a ransom attack, there are various individuals and audiences that need to be communicated with, including patients, employees, regulatory bodies, and possibly law enforcement [107].

8.1.4 Address Third-Party and Supply Chain Risks

The Change Healthcare incident showed dramatically that healthcare functions as an interconnected ecosystem [9]. When a significant vendor is affected, the impact reaches thousands of dependent organizations. However, many healthcare providers have limited insight into their third-party risks.

To manage vendor risks effectively, consider these practical steps:

- List All Third Parties with Access to Your Systems or Data: Many organizations find during incident investigations that they have more vendors with network access or data-sharing agreements than they thought [116]. Begin with thorough discovery and ask relevant questions such as
  - ✓ Who has VPN access?
  - ✓ Who gets data feeds?
  - ✓ Who offers cloud services?
  - ✓ Who oversees medical devices remotely?
- Establish Vendor Risk Assessment Processes: Not all vendors pose the same level of risk. The access of a landscaping company differs from that of your EHR vendor. Risk assessments should be proportional, considering factors such as what data or systems the vendor can access, their security controls, any past breaches, and their backup or business continuity plans [56].
- Incorporate Cybersecurity Requirements in Contracts: Typical vendor contracts often lack specific cybersecurity requirements or audit rights. Ask vendors to include clauses in any new or renewed vendor contracts that require them to adhere to certain security

standards, allow audits of their security measures, notify the organization of any security incidents, and maintain certain insurance policies [118].

- Create Contingency Plans for Vendor Outages: What will happen if your vendor is struck with a ransomware attack? The attack on Change Healthcare forced many providers to find ways to deal with the lack of backup plans for specific functions within their organizations [116]. Ensure that alternative vendors or processes for essential services are in place and ready to go online if your vendors fall victim to a ransomware attack.

8.2 Policymakers and Regulatory Authorities

Policymakers and regulators influence the environment in which healthcare organizations operate. The policies that are created can impact the healthcare Industry and either encourage advancements in security or create negative incentives that hinder the organization's security objectives. The suggestions provided aim to address these concerns and create a policy that is supportive of the organizations yet one that reinforces the necessary requirements for those organizations to comply with the policies established.

8.2.1 Modernize and Strengthen HIPAA Security rule requirements.

The proposed updates to the HIPAA Security Rule in December 2024 mark the most significant changes to healthcare cybersecurity regulations in over twenty years [119]. These changes are a step in the right direction because they make network segmentation mandatory, remove the confusing distinction between "required" and "addressable" implementation specifications, and mandate specific baseline controls like multi-factor authentication. However, there are several areas that need focus as these regulations approach finalization and they include

Offer Clear, Actionable Guidance on Implementation. Since the rule already provides for the flexibility of creating solutions that fit the individual organizations' needs, there is some uncertainty regarding what those solutions will be [120] . The way the mapping of NIST SP 800-66r2 to HIPAA requirements was done could be followed for creating a mapping of each of the requirements to the HIPAA regulations [94]. Because many organizations will include medical device environments and possibly some antiquated systems that are difficult to replace, it will take time for the organizations to reach full compliance [121]. A timeline can be created

that includes phases during which certain organizations can focus on compliance, allowing them to reach the level of information security required of them over time.

It is likely that a 25-bed rural hospital will have different information security requirements than a 1,000-bed medical centre that serves hundreds of students each year [55]. While the smaller organization will have to adhere to the same standards as the larger organization, there are likely differences in their capabilities. Requirements for smaller organizations could be implemented according to the model established by the Health Information for Community Practice (HICP) regulation.

8.2.2 Strengthening the Oversight of Healthcare Technology Vendors

The systemic risks created by the concentration of healthcare services in the few major vendors are exemplified by the Change Healthcare attack [116]. The fact that one vendor processes close to 15 billion healthcare transactions each year makes the security of that vendor a concern for all healthcare providers involved. Several policies that could mitigate the risks created by these vendors are

- Broaden Cybersecurity Performance Goals to Include Business Associates: Currently, the cyber performance goals of the HHS CPGs are directed towards care providers. However, many ransomware attacks target business associates and vendors of healthcare organizations [116]. In 2025 alone, the number of ransomware attacks on healthcare businesses increased by 30% compared to those that targeted healthcare providers [77]. Expanding these cyber performance goals or baseline requirements to include business associates will help to increase the cybersecurity standards across the healthcare Industry.
- Mandate Independent Security Audits for Essential Healthcare Service Providers: Companies that provide essential services to the healthcare Industry, such as claims clearinghouses, pharmacy benefit managers, and electronic health record (EHR) vendors, should be required to undergo regular independent information security audits. The results of these audits should then be submitted to HHS [121].
- Create Certification Programs for Healthcare Technology Vendors: Just as the HITRUST certification program requires covered entities to comply with certain cybersecurity standards, certification programs for healthcare information technology vendors could be created that require those vendors to adhere to minimum cybersecurity

standards [56]. Healthcare organizations could then require that their vendors be certified to mitigate the risk of cyberattacks from those vendors.

- Implement reporting Requirements for Vendor Incidents: Currently, if a vendor that provides significant services to a healthcare organization is attacked with ransomware, the Office for Cybersecurity and Information Sharing within HHS and the Cybersecurity and Infrastructure Security Agency (CISA) should be informed of the attack. Regardless of whether the vendor's data is the data that was encrypted by the attack, notifying these government agencies will allow other organizations within the healthcare Industry to be informed of the attack and to take necessary preparations to protect their organizations [120].

8.2.3 Provision of Funding and Resources for Under-Resourced Providers

The robust cybersecurity requirements may not be accompanied by funding to meet those requirements, leading to a divided cybersecurity system [121]. There are various legislative proposals regarding funding for cybersecurity systems. However, the implementation of these legislative proposals is more crucial than the intention of the legislators behind these bills. Some strategies for funding cybersecurity systems include

- Cybersecurity grant programs for healthcare: The Health Care Cybersecurity and Resiliency Act of 2025 suggest grants to assist healthcare organizations with limited resources in enhancing their cybersecurity. These grants should be given to rural hospitals and health centers that cater to vulnerable populations, who often have the least security measures in place to begin withs [119].
- Subsidized access to security tools and services: Instead of each organization paying the full price for commercial security tools, federal programs could negotiate bulk licenses for security software, threat intelligence services, or managed security services, allowing participating healthcare organizations to access them at a lower cost or even for free [122]. CISA already offers some free services like vulnerability scanning and expanding this approach could greatly benefit resource-strapped organizations.
- Technical assistance and expertise programs: Simply providing funds does not resolve security issues if organizations lack the know-how to utilize them effectively. Programs that offer cybersecurity consulting, architecture assessments, incident response help, and training should work alongside funding. CISA's regional cybersecurity advisors

offer this support, but their capacity should grow to address the needs of the healthcare sector [123].

8.2.4 Improved Information Sharing and Coordination

Ransomware operators exchange details about effective attack methods, weaknesses of victims, and payment records. Healthcare defenders require similar information sharing to create a fair environment. Some of the measures that are required to be in place are

- Quick incident reporting with safeguarded information sharing: CIRCIA mandates reporting for critical infrastructure, but the specifics of implementation are crucial [124]. Healthcare-specific guidelines should ensure quick information sharing that aids other organizations in preparing for similar attacks while protecting against regulatory overreach that could deter reporting. Organizations that report quickly and collaboratively should be given regulatory leniency, while those that conceal incidents should face penalties.
- Enhance Health-ISAC and broaden involvement: The Health Information Sharing and Analysis Center offers threat intelligence to its members, but joining is optional and many organizations do not participate actively [125]. Policymakers should encourage participation through regulatory protections, preference in grants, or other incentives. They should also secure funding to expand the services offered by Health-ISAC to cover the entire
- Promote coordination Among federal agencies: Several federal agencies are already involved in healthcare and cybersecurity, such as the HHS, CISA, the FBI, the FDA, and others [123]. The Healthcare Cybersecurity Act of 2025 calls for the improvement of coordination between the HHS and the CISA to avoid any redundancies within the federal government regarding cybersecurity in the healthcare sector [126]. Furthermore, the bill calls for the creation of a coordinator for cybersecurity within the healthcare sector in the federal government to ensure that all significant cybersecurity incidents in the healthcare sector are responded to in a unified matter by the federal government.

8.3 Technology Developers and Vendors

Technology vendors and developers have specific responsibilities in the realm of healthcare cybersecurity. The products and services that they provide have the potential to either enhance or weaken the cybersecurity posture of every organization that utilizes their technology

vendor's offerings. From medical device vendors to healthcare IT companies, all these vendors have a role to play in the cybersecurity of healthcare organizations.

8.3.1 Implementation of Security by Design

Security is often incorporated into products after the development process. However, this method introduces vulnerabilities to the product throughout its life cycle [115]. Healthcare technology providers must incorporate security from the beginning of product development. The following are recommendations to follow for the implementation of security by design.
Conducting threat modelling during the design phase of development will allow the team to identify the threats to the product prior to beginning the coding process. For medical devices, such threats can include malicious actors possessing the credentials to access devices, network attacks, tampering with devices, and harmful software updates [118].

Implementing secure development lifecycles will ensure that security is integrated into every stage of product development, from the initial concept and requirement stage until the product is launched into the market [115]. Security testing should occur prior to the launch of the product to ensure that vulnerabilities are identified and fixed. Default configurations for the products should be secure to prevent illicit access to the devices and information stored on the devices. Manufacturers can create the products to default to secure settings for features such as authentication, communications, logging, and software updates [100]. Users can be given the option to change these settings to match their specific needs for the devices, but the default settings should be secure.

8.3.2 Support long term Security Maintenance

FDA regulations and operational needs in healthcare create obstacles to frequent replacements. This extended lifespan means that vendors must provide long-term security support. Long time security support can be achieved by sticking to the following principles

- Provide timely security updates throughout product lifecycles: When vulnerabilities are found, vendors should quickly create and distribute patches. For vulnerabilities that are actively being exploited, emergency patches may be needed within days. Even for older products nearing the end of their life, essential security updates should continue until organizations can realistically transition to newer systems [118].

- Establish clear end-of-life and support timelines: Healthcare organizations require advance notice when products will stop receiving security updates. Vendors should announce end-of-life dates several years ahead and offer migration paths to newer supported products. They should also provide extended support options for organizations that cannot immediately replace systems due to regulatory, technical, or financial constraints [26].
- Implement coordinated vulnerability disclosure programs: Researchers who find vulnerabilities should have clear ways to report them to vendors [97]. The FDA's cybersecurity guidance now mandates that medical device manufacturers set up coordinated vulnerability disclosure programs. Healthcare IT vendors should also adopt similar programs, even if they are not regulated by the FDA, to create safe environments for researchers and establish processes for evaluating, fixing, and communicating about vulnerabilities.

8.3.3 Design for Resilience and Recovery

In addition to stopping attacks, healthcare technology must be built to keep operations running during incidents and aid in quick recovery when breaches happen. For health care organizations, the ability to restore systems in the case of a ransomware attack is essential. Features such as automated backups, the ability to restore specific data within the system instead of entire systems, and data integrity for backups prior to recovery are essential [56]. If the systems are unable to operate at full functionality due to the ransomware attack, the products should be able to operate in reduced functionality modes to ensure essential systems and operations can remain operational. An example of this would be an electronic health record system that can operate in read-only mode to still provide access to important patient data. In the case that a health care organization should encounter these incidents, the organization will require logs to investigate the issues and plan a recovery process for the impacted systems. These logs should be able to track security-related events, be tamper-proof, and be exportable to an external device to be further examined by external parties, logs that include documentation that explains the different formats and contents of each log [118].

8.3.4 Participation in sector wide security efforts

Vendors need to engage with Health-ISAC, sector coordinating councils, and working groups that create cybersecurity guidelines. They could also exchange threat intelligence between their

products, contribute to the creation of security standards, or coordinate their efforts to mitigate threats to the industry altogether. New cybersecurity standards will be created, such as those from the NIST frameworks, the FDA, and the healthcare Industry itself. It will be essential for the cybersecurity industry to adopt these standards to provide additional competitive edges to their current products for their healthcare clients [111]. Because the cybersecurity industry knows so much about information security, they should contribute to the creation of open-source security tools, research studies regarding the threats to the healthcare Industry, and support the research publications on the topic of cybersecurity in healthcare [115].

8.4 Patients and the General Public

At first, it may appear that patients are just passive victims of ransomware attacks, not active players in cybersecurity. However, patients and the public play crucial roles in advocating for improved security and in safeguarding themselves.

8.4.1 Demand for Transparency about Cybersecurity Practices

Healthcare consumers should expect and demand clarity on how organizations safeguard their health information. Just as patients inquire about clinical quality metrics and safety records, they should also ask about cybersecurity. They should Inquire about Security Practices with Healthcare Providers. During the process of choosing healthcare, patients can pose questions such as: Do you implement multi-factor authentication? How is patient data secured? When was your last security evaluation? Have you faced any cybersecurity issues? These survey questions show that patients care about cybersecurity [120].

When organizations experience a cybersecurity breach, they are required to send a letter to the individuals impacted by the data breach. These letters contain information regarding the nature of the breach and the steps that the organization will take to protect the affected individuals [118]. Patients should read these letters and follow the steps to protect their data. If healthcare organizations put security as a top priority, patients will show their support for these efforts. By incentivizing organizations to establish rewards for good cybersecurity and data protection practices, these organizations will continue to invest in improving their security measures [59]

8.4.2 Practice Good Personal Cybersecurity Hygiene

Healthcare organizations are mainly responsible for protecting patient health data. However, patients can also do certain things to protect their data. Patients must create strong, unique passwords for Patient Portals. Reusing the same username and password for many different websites or portals poses a risk if one of those websites is hacked. Password managers can help people create strong and unique passwords for each account they have online [100]. Many patient portals and healthcare applications uses multi-factor authentication [115]. Patients should use this added layer of security when logging into their health information portals.

Phishing emails can be a pathway for cybercriminals attempting to obtain personal information [113]. Patients should not click on links in emails they did not send. Patients should contact the organization by which the data is being sent to confirm the legitimacy of the communication.
Data that is stolen from patients can be used to perform medical identity theft or to engage in health insurance fraud [118]. Patients should regularly monitor their health data and financial accounts to ensure that no fraudulent charges are made to their health accounts. In the case that fraud is found, it may be possible to limit the damage done to the patient by catching and reporting it early.

8.4.3 Understand rights and advocate for better protection

Patients have legal rights concerning their health information, and public pressure can lead to better policies. Patients should understand their HIPAA Rights. According to HIPAA, patients can access their health records, ask for corrections to wrong information, receive notifications about breaches, and file complaints regarding privacy issues. Knowing these rights empowers patients to advocate for themselves when problems occur. Healthcare cybersecurity policies improve when patients and the public voice their concerns. Reaching out to elected officials, taking part in public comment periods for proposed regulations, and supporting patient advocacy groups all play a role in shaping policy [125].
When patients face negative impacts from healthcare cyberattacks such as delayed care, inconvenience, and privacy issues, sharing these experiences while safeguarding personal information helps others see the importance of cybersecurity [59]. Raising public awareness puts pressure on the system for improvements.

9 Conclusion and Future Research Directions

9.1 Summary of Findings

Given the growing ransomware attacks on healthcare organizations and the lack of defensive capabilities of these organizations, it is important to take a closer look at the literature regarding this critical issue. Through reviewing the threat of ransomware, the current defensive measures within healthcare organizations, the gaps in the current research regarding this topic, and the recommendations to address the concerns created by these threats, several important findings emerge from the research on this topic.

Firstly, the threat of ransomware to smart hospitals is of a different nature than those experienced within other industries. For instance, if the systems of a banking organization are encrypted by a hacker, while there are no fatalities that may result from such an attack, there may be financial and reputational damages to that organization. In contrast, should a hacker encrypt the electronic health records (EHR) systems of a hospital during a period of high patient demand, the lives of those patients can be threatened by the hospital's inability to provide appropriate medical treatments to those patients.

According to the data from 2024, there were 444 cybersecurity incidents in healthcare organizations worldwide, 181 of which were ransomware attacks that impacted 25.6 million patient records, and the average ransom demand from those attacking the organizations was $5.7 million [63]. Additionally, there are growing issues with the smart infrastructure of hospitals. While the smart infrastructure allows hospitals to better provide care for their patients, such infrastructure also creates new vulnerabilities for hackers to access those organizations. For instance, 60% of medical devices in hospitals utilize outdated software that cannot be updated, and 88% of all healthcare organizations have experienced data breaches because of these vulnerabilities of their connected medical devices [10], [11].

Furthermore, hackers have developed new methods for attacking the data of healthcare organizations. For instance, the number of data breaches within healthcare organizations that result in the theft of data without the need to encrypt those systems has tripled since 2025 compared to 2022/2023 [22]. Additionally, hackers are also targeting organizations like Change

Healthcare, which provides critical supply chain services to over 200 healthcare organizations, and are targeting the users of those organizations through credential-based attacks.

Furthermore, the defensive measures for healthcare organizations are lacking. For instance, while the effectiveness of current prevention strategies for healthcare organizations is reported to have increased to 76% in 2024 [101], the scores for alerts that trigger those defenses have dropped dramatically to 5%. Thus, 73% of the alerts that are triggered within these organizations do not lead to detections of hackers within those organizations [101].

In addition, the research that has been performed on the topic of cybersecurity within healthcare organizations reveals several gaps in that research. For instance, most of the research on cybersecurity within healthcare organizations is related to technology, comprising over half of the publications on the topic [49]. Furthermore, the research is biased in relation to the locations of the organizations that are discussed in these publications, and research regarding community hospitals and rural healthcare providers is underrepresented in these publications.

Finally, the research that has been performed on the topic in relation to testing the effectiveness of current countermeasures for hackers is lacking; there is more information available regarding the variety of current issues within healthcare organizations than there is information regarding the suggested solutions for resolving those issues. Additionally, the research recommendations for healthcare organizations do not consider the operational realities of the organizations; for instance, a small rural hospital will not have the same capabilities for implementing cybersecurity as a large urban medical centre, yet the research publications do not reflect this difference in the current literature.

9.2 Contributions to the Field

This research makes several contributions to the existing literature in a way that aims to advance the scholarly discussion on the topic of healthcare and ransomware. In terms of academic significance, this study contributes to the academic literature on healthcare cybersecurity by addressing important gaps. It tackles the gap in knowledge regarding the cybersecurity of smart hospitals by conducting a thorough analysis of the threats posed by ransomware to these facilities. It combines knowledge from various fields to provide a well-rounded view of ransomware threats to smart hospitals. The systematic gap-analysis method used in this research

offers a repeatable framework that can be modified to pinpoint shortcomings in other specific cybersecurity areas and new technology environments.
By providing practical suggestions for improving the cybersecurity of smart hospitals across prevention, detection, response, and recovery, this research informs the development of more secure smart hospitals. Each suggestion is tailored for different stakeholder groups within smart hospitals, and considers real-world limitations such as budget constraints, staffing issues, clinical workflow needs, and regulatory requirements, thereby bridging the gap between theoretical cybersecurity concepts and their practical application.

This study identifies regulatory gaps at organizational, regional, and national levels and suggests policy frameworks that align stringent security needs with healthcare operations, innovation goals, and economic viability. The results can assist healthcare regulators, lawmakers, standards organizations, and industry groups in creating more effective, balanced, and practical cybersecurity governance systems.

Given healthcare's vital role in society and its designation as critical infrastructure in many areas, improving the cybersecurity resilience of smart hospitals has clear and significant effects on public health, patient safety, and overall societal wellbeing. This study helps safeguard essential healthcare services from interruptions, preserves public confidence in digital health technologies, ensures care continuity during cyber incidents, and supports the sustainable growth of smart healthcare infrastructure.

In 2024, the worldwide average cost of healthcare data breaches reached $9.77 million, making healthcare the dominant sector for the 14th consecutive year [89]. Ransomware attacks impose substantial financial burdens through ransom payments, system-restoration costs, operational disruptions, lost revenue, regulatory fines, legal liabilities, and reputational damage. This thesis offers evidence-based, cost-effective strategies for prevention and mitigation, helping healthcare organizations minimize financial losses, use limited cybersecurity resources more efficiently, and improve the return on security investments.

The ultimate significance of this work lies in its potential to contribute to safer, more secure, and more resilient smart healthcare infrastructure that can withstand and rapidly recover from ransomware attacks while maintaining quality of patient care, ensuring safety, and preserving trust in digital healthcare technologies.

9.3 Limitations of the study

There are various limitations to the study that was conducted for this analysis. The healthcare technology and the threats to the information that is contained in those networks change at a rapid rate. The strategies for ransomware attacks on healthcare information systems that are in use today could soon be replaced with entirely new forms of attack in the near future.

Furthermore, there will always be the introduction of new technologies into the healthcare Industry that can potentially make the information within those systems more secure or more vulnerable to data breaches due to those new technologies. This literature review takes a closer look at the state of healthcare information technology and cybersecurity in the 2024-2025 timeframe and in recognition of some of its limitations.

A review of the available literature on the topic of healthcare information technology cybersecurity inevitably overlooked some studies on the topic. Due to the various fields and publications that publish research on the topic, it is possible that even a thorough search for literature on the topic of healthcare information technology cybersecurity overlooked some studies that could have been relevant to the discussion of the topic. Thus, the identified gaps in the available literature on the topic of healthcare information technology cybersecurity represent the shortcomings of the published literature as opposed to the gaps in all the knowledge that exists on the topic.

Furthermore, the recommendations for various stakeholders are based upon the information presented in this literature review and real-world events but have not been empirically tested for their validity and potential to provide improved outcomes for the healthcare organizations that adopt such recommendations. The research for such an analysis would require additional research to be performed. Additionally, although the focus on smart hospitals in developed nations indicates a potential area for increased concern regarding cybersecurity in healthcare, the findings of this research may not be applicable to other types of healthcare organizations.

Many of the other healthcare organizations in the U.S. and around the world, including clinics, long-term care facilities, and healthcare provision in low- and middle-income countries, require additional research to be performed on their specific challenges in information technology and cybersecurity. The focus on this topic and the depth of the research that was performed for this

literature review indicate a commitment to providing information on the topic, but at the sacrifice of the breadth of the types of studies that could have been performed on the topic.

Furthermore, the information that was collected for this literature review was based upon publicly available information from healthcare organizations, many of which may have chosen to keep their management of these attacks on the radar and to provide as little information about the attacks as possible to avoid potential liabilities, competitive challenges, and other issues that may arise from the public disclosure of the management of such attacks. Thus, the complete scope of the attacks on healthcare organizations with ransomware is still somewhat unclear.

Finally, the discussion of cybersecurity for healthcare information technology mainly covers the defensive aspects of the topic. While the defence against cybersecurity attacks in healthcare information technology is an essential aspect of the security of healthcare organizations, a full understanding of the topic would include aspects related to the offensive security of those information technologies as well.

9.4 Future Scope

The gaps in the current literature also present numerous opportunities for future research. The use of artificial intelligence and machine learning in healthcare cybersecurity presents an area for future research. Due to the impact of artificial intelligence on both cyber threats and cyber defenses, it is critical to investigate how machine learning can be used to detect threats in healthcare systems while avoiding creating false alerts. Additionally, the growing use of artificial intelligence by cyber criminals to create phishing scams and malware also presents an area for future research.

Furthermore, the implementation of Zero Trust architecture in healthcare environments presents an area for future research. The concept of Zero Trust architecture is appealing for healthcare systems but presents challenges in their implementation. Future research can investigate the best methods for implementing Zero Trust in healthcare systems of various sizes, especially with the inability of many medical devices to install security agents required by Zero Trust architectures. Additionally, Zero Trust architecture can be researched in regard to the best ways to implement them to maximize the benefits to healthcare systems.

The importance of supply chain security after the Change Healthcare cyberattack presents an area for future research. For example, research can investigate methods of assessing the cybersecurity of hundreds of third parties that provide services to healthcare organizations, methods of incorporating incentives into the contracts with those third parties, and the technologies that can be used to monitor the security of those third parties.

Finally, research in the ways to recover from cyber-attacks and to increase the cybersecurity resilience of those impacted healthcare organizations presents another area for future research. For example, research can investigate recovery strategies that minimize the impact on patient care in the aftermath of a cyber-attack, factors that contribute to the successful recovery of a healthcare organization over time compared to those that struggle to recover, and strategies for the validation and testing of methods for restoring those systems to their original state of operation.

References

[1] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0," Journal of Industrial Information Integration, vol. 18, p. 100129, June 2020, doi: 10.1016/j.jii.2020.100129.

[2] P. Germanakos, C. Mourlas, and G. Samaras, "A Mobile Agent Approach for Ubiquitous and Personalized eHealth Information Systems," in Proceedings of UM05 Workshop on Personalisation for eHealth, Edinburgh, United Kingdom, 2005, pp. 67–70.

[3] M. Javaid and I. H. Khan, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," Journal of Oral Biology and Craniofacial Research, vol. 11, no. 2, pp. 209–214, April 2021, doi: 10.1016/j.jobcr.2021.01.015.

[4] H. T. Neprash, P. Song, S. S. Colla, and A. B. Jena, "Trends in Ransomware attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021," JAMA Health Forum, vol. 3, no. 12, p. e224873, Dec. 2022, doi: 10.1001/jamahealthforum.2022.4873.

[5] T. B. Slayton, "Ransomware: The Virus Attacking the Healthcare Industry," Journal of Legal Medicine, vol. 38, no. 2, pp. 287–311, April 2018, doi: 10.1080/01947648.2018.1473186.

[6] J. X. Jiang, J. S. Ross, and G. Bai, "Ransomware attacks and Data Breaches in US Health Care Systems," JAMA Network Open, vol. 8, no. 5, p. e2510180, May 2025, doi: 10.1001/jamanetworkopen.2025.10180.

[7] R. Moody, "Healthcare Ransomware Roundup: Q1-Q3 2025 stats on attacks, ransoms, and data breaches," Comparitech, Accessed: Jan. 3, 2026. [Online]. Available: https://www.comparitech.com/news/healthcare-ransomware-roundup-q1-q3-2025-stats-on-attacks-ransoms-and-data-breaches/

[8] W. J. Gordon, A. Fairhall, and A. Landman, "Threats to Information Security — Public Health Implications," New England Journal of Medicine, vol. 377, no. 8, pp. 707–709, Aug. 2017, doi: 10.1056/NEJMp1707212.

[9] D. Bonderud, "Ransomware on the rise: Healthcare Industry attack trends 2024," IBM, Accessed: Jan. 3, 2026. [Online]. Available: https://www.ibm.com/think/insights/healthcare-industry-attack-trends-2024

[10] M. Khalil, "IoMT Vulnerabilities Statistics & Security Trends 2025," DeepStrike, Accessed: Jan. 3, 2026. [Online]. Available: https://deepstrike.io/blog/iomt-vulnerabilities-statistics-2025

[11] Z. Amos, "IoT Devices Are a Leading Vulnerability in Healthcare Data Breaches," IoT For All, Accessed: Jan. 3, 2026. [Online]. Available: https://www.iotforall.com/iot-devices-vulnerability-healthcare-data-breaches

[12] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1121–1167, Feb. 2020, doi: 10.1109/COMST.2020.2973437.

[13] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things (IoMT) Enabled Healthcare Systems: A Survey," IEEE Access, vol. 7, pp. 183339–183355, Dec. 2019, doi: 10.1109/ACCESS.2019.2960617.

[14] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health," International Journal for Quality in Health Care, vol. 33, no. 1, p. mzaa117, Feb. 2021, doi: 10.1093/intqhc/mzaa117.

[15] H. Landi, "Healthcare remains top target for cybercriminals with an uptick in hacking attacks in 2024," Fierce Healthcare, Accessed: Jan. 5, 2026. [Online]. Available: https://www.fiercehealthcare.com/health-tech/healthcare-remains-top-target-cybercriminals-uptick-hacking-attacks-2024

[16] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," Internet Technology Letters, vol. 4, no. 2, p. e247, March 2021, doi: 10.1002/itl2.247.

[17] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," Journal of Medical Internet Research, vol. 20, no. 5, p. e10059, May 2018, doi: 10.2196/10059.

[18] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," Technology and Health Care, vol. 25, no. 1, pp. 1–10, Feb. 2017, doi: 10.3233/THC-161263.

[19] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?," BMJ, vol. 358, p. j3179, July 2017, doi: 10.1136/bmj.j3179.

[20] G. Miller, "Considerations and Safeguards Addressing Potential Vulnerabilities in Connected Medical Devices and the Internet of Things (IoT)," Healthcare IT Today, Accessed: Jan. 7, 2026. [Online]. Available: https://www.healthcareittoday.com/2024/10/29/considerations-and-safeguards-addressing-potential-vulnerabilities-in-connected-medical-devices-and-the-internet-of-things-iot/

[21] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the Internet of Things for Smart Healthcare," IEEE Communications Magazine, vol. 56, no. 4, pp. 38–44, April 2018, doi: 10.1109/MCOM.2018.1700809.

[22] H. Landi, "How healthcare ransomware attacks shifted in 2025," Fierce Healthcare, Accessed: Jan. 7, 2026. [Online]. Available: https://www.fiercehealthcare.com/health-tech/how-healthcare-ransomware-attacks-are-shifting-2025

[23] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, July 2018, doi: 10.1016/j.maturitas.2018.04.008.

[24] S. Aurangzeb, M. Aleem, M. A. Iqbal, and M. A. Islam, "Ransomware: A Survey and Trends," Journal of Information Assurance and Security, vol. 12, no. 6, pp. 301–318, 2017.

[25] N. Eddy, "Thousands of medical devices and systems pose IoT security risk," Healthcare IT News, Accessed: Jan. 7, 2026. [Online]. Available: https://www.healthcareitnews.com/news/thousands-medical-devices-and-systems-pose-iot-security-risk

[26] "IoT in Healthcare: The Expanding Threat Landscape and Strategies to Mitigate It," BreachLock, Accessed: Jan. 7, 2026. [Online]. Available: https://www.breachlock.com/resources/blog/iot-in-healthcare-the-expanding-threat-landscape

[27] C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo-de-Gea, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," Medical & Biological Engineering & Computing, vol. 62, no. 1, pp. 257–273, Jan. 2024, doi: 10.1007/s11517-023-02912-0.

[28] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0," Journal of Industrial Information Integration, vol. 18, p. 100129, June 2020, doi: 10.1016/j.jii.2020.100129.

[29] L. Rajaee, "The History of Electronic Health Records (EHRs)," Elation Health, Accessed: Jan. 23, 2026. [Online]. Available: https://www.elationhealth.com/resources/blogs/the-history-of-electronic-health-records-ehrs

[30] O. Boyles, "The Evolution of Electronic Health Records: From Paper to Digital," ICANotes, Accessed: Jan. 23, 2026. [Online]. Available: https://www.icanotes.com/2019/04/16/a-history-of-ehr-through-the-years/

[31] R. S. Evans, "Electronic Health Records: Then, Now, and in the Future," Yearbook of Medical Informatics, vol. 25, no. S 01, pp. S48–S61, Aug. 2016, doi: 10.15265/IYS-2016-s006.

[32] S. Abdulmalek, B. Mustafa, N. Ali, K. Jawad, and K. Khaldoon, "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review," Healthcare, vol. 10, no. 10, p. 1993, Oct. 2022, doi: 10.3390/healthcare10101993.

[33] M. Alsabah, M. I. Qureshi, A. Khan, and S. Borawake, "A comprehensive review on key technologies toward smart healthcare systems based IoT: technical aspects, challenges and future directions," Artificial Intelligence Review, vol. 58, no. 11, p. 343, Aug. 2025, doi: 10.1007/s10462-025-11342-3.

[34] J. Atherton, "Development of the Electronic Health Record," AMA Journal of Ethics, vol. 13, no. 3, pp. 186–189, March 2011, doi: 10.1001/virtualmentor.2011.13.3.mhst1-1103.

[35] "How Electronic Health Records Revolutionized Healthcare," Record Nations, Accessed: Jan. 23, 2026. [Online]. Available: https://www.recordnations.com/white-papers/electronic-health-records-revolutionized-healthcare/

[36] A. Kumar, M. Masud, M. H. Alsharif, N. Gaur, and A. Nanthaamornphong, "Integrating 6G technology in smart hospitals: challenges and opportunities for enhanced healthcare services," Frontiers in Medicine, vol. 12, p. 1534551, April 2025, doi: 10.3389/fmed.2025.1534551.

[37] D. Schönberger, "Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications," International Journal of Law and Information Technology, vol. 27, no. 2, pp. 171–203, June 2019, doi: 10.1093/ijlit/eaz004.

[38] "The Smart Hospital Technology Revolution Powered by AI and IoT," MDForLives, Accessed: Jan. 23, 2026. [Online]. Available: https://mdforlives.com/blog/smart-hospital-technology-revolution/

[39] A. Shalimov, "How Smart hospitals Are Shaping the Future of Healthcare," Eastern PEAK, Accessed: Jan. 23, 2026. [Online]. Available: https://easternpeak.com/blog/how-smart-hospitals-are-shaping-the-future-of-healthcare/

[40] E. Pashkovskaya, "How IoT Medical Devices Benefit Healthcare Organizations, Doctors, and Patients," NEKLO, Accessed: Jan. 23, 2026. [Online]. Available: https://neklo.com/blog/iot-medical-devices

[41] R. Heaton, "What is a smart hospital?," TechTarget, Accessed: Jan. 23, 2026. [Online]. Available: https://www.techtarget.com/healthtechanalytics/definition/smart-hospital

[42] S. Pradeesh, "How IoT in Healthcare is Transforming Patient Care with IoT Medical Devices," Cavli Wireless, Accessed: Jan. 24, 2026. [Online]. Available: https://www.cavliwireless.com/blog/nerdiest-of-things/iot-in-healthcare

[43] V. Struk, "Fundamentals of Smart Healthcare System Using IoT," Relevant Software, Accessed: Jan. 23, 2026. [Online]. Available: https://relevant.software/blog/smart-healthcare-system-using-iot/

[44] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Arlington, Virginia, USA, July 2017, pp. 179–181, doi: 10.1109/ISI.2017.8004904.

[45] D. F. Sittig and H. Singh, "A new sociotechnical model for studying health information technology in complex adaptive healthcare systems," Quality and Safety in Health Care, vol. 19, no. S3, pp. i68–i74, Oct. 2010, doi: 10.1136/qshc.2010.042085.

[46] B. Whittaker, "History of EHRs in healthcare technology," Tebra, Accessed: Jan. 29, 2026. [Online]. Available: https://www.tebra.com/theintake/ehr-emr/history-of-ehrs-in-healthcare-technology

[47] "Healthcare Cybersecurity Statistics 2025," Total Assure, Accessed: Jan. 29, 2026. [Online]. Available: https://www.totalassure.com/blog/healthcare-cybersecurity-statistics-2025

[48] P. Kobus, "2025 Year in Review: Healthcare Cybersecurity Enters a High-Stakes Era," Healthcare Innovation Group, Accessed: Jan. 29, 2026. [Online]. Available: https://www.hcinnovationgroup.com/features/article/55340080/2025-year-in-review-healthcare-cybersecurity-enters-a-high-stakes-era

[49] N. F. Kazi, "Cybersecurity in healthcare: a narrative review of trends, threats and ways forward (2024)," Journal of Cybersecurity, vol. 10, no. 1, p. oyad003, March 2024, doi: 10.1093/cybsec/oyad003.

[50] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," Journal of Medical Internet Research, vol. 20, no. 5, p. e10059, May 2018, doi: 10.2196/10059.

[51] P. Ewoh and T. Vartiainen, "Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review," Journal of Medical Internet Research, vol. 26, p. e46904, May 2024, doi: 10.2196/46904.

[52] K. Hasegawa, N. O'Brien, M. Prendergast, C. A. Ajah, A. L. Neves, and S. Ghafur, "Cybersecurity Interventions in Health Care Organizations in Low- and Middle-Income Countries: Scoping Review," Journal of Medical Internet Research, vol. 26, p. e47311, Nov. 2024, doi: 10.2196/47311.

[53] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," Journal of Medical Internet Research, vol. 23, no. 4, p. e21747, April 2021, doi: 10.2196/21747.

[54] J. Hughes, "Understanding barriers to cyber resilience in healthcare," TechTarget, Accessed: March 2, 2026. [Online]. Available: https://www.techtarget.com/healthtechsecurity/answer/Understanding-barriers-to-cyber-resilience-in-healthcare

[55] G. Hulme, "Bridging the Cybersecurity Gap Among America's Underfunded Healthcare Providers," Nexus, Accessed: March 9, 2026. [Online]. Available: https://nexusconnect.io/articles/bridging-the-cybersecurity-gap-among-americas-underfunded-healthcare-providers

[56] "Ultimate Guide to Cyber Resilience in Healthcare," Censinet, Accessed: March 9, 2026. [Online]. Available: https://www.censinet.com/perspectives/ultimate-guide-to-cyber-resilience-in-healthcare

[57] S. Kumari, P. Pattanaik, and M. Z. Khan, "Impact of Cybersecurity Measures in the Healthcare Sector: A Comprehensive Review of Contemporary Approaches and Emerging Trends," International Journal of Education and Management Engineering, vol. 14, no. 6, pp. 1–19, Dec. 2024, doi: 10.5815/ijeme.2024.06.01.

[58] "2025 Horizon Report: The state of cybersecurity in healthcare," Fortified Health Security, Accessed: Jan. 29, 2026. [Online]. Available: https://fortifiedhealthsecurity.com/horizon-report/2025-horizon-report/

[59] S. Zeijlemaker and M. Siegel, "How to prioritize cyber resilience in the healthcare sector," World Economic Forum, Accessed: March 9, 2026. [Online]. Available: https://www.weforum.org/stories/2026/02/how-to-prioritize-cyber-resilience-in-the-healthcare-sector/

[60] R. Luna, E. Rhine, M. Myhra, R. Sullivan, and C. S. Kruse, "Cyber threats to health information systems: A systematic review," Technology and Health Care, vol. 24, no. 1, pp. 1–9, Jan. 2016, doi: 10.3233/THC-151102.

[61] "Ransomware & Healthcare," U.S. Department of Health and Human Services, Accessed: Feb. 3, 2026. [Online]. Available: https://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf

[62] "US Healthcare at risk: Strengthening resiliency against ransomware attacks," Microsoft, Accessed: Feb. 3, 2026. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks

[63] "Report: Health care had most reported cyberthreats in 2024," American Hospital Association, Accessed: Feb. 3, 2026. [Online]. Available: https://www.aha.org/news/headline/2025-05-12-report-health-care-had-most-reported-cyberthreats-2024

[64] S. Alder, "2024 Was Another Bad Year for Healthcare Ransomware attacks," The HIPAA Journal, Accessed: Feb. 3, 2026. [Online]. Available: https://www.hipaajournal.com/2024-was-another-bad-year-for-healthcare-ransomware-attacks/

[65] P. Mahendru, "The State of Ransomware in Healthcare 2024," Sophos, Accessed: Feb. 3, 2026. [Online]. Available: https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-healthcare-2024

[66] S. Alder, "Healthcare Ransomware attacks Continue to Increase in Number and Severity," The HIPAA Journal, Accessed: Feb. 3, 2026. [Online]. Available: https://www.hipaajournal.com/healthcare-ransomware-attacks-2024/

[67] N. Masakapalli and R. Vodapally, "Ransomware as a Service (RaaS): Emerging Threats and Proactive Defense Tactics," IRE Journals, vol. 8, no. 10, pp. 45–52, April 2025.

[68] "U.S. and U.K. Disrupt LockBit Ransomware Variant," U.S. Department of Justice, Accessed: Feb. 5, 2026. [Online]. Available: https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

[69] S. Gihon, "Ransomware Groups Report 2024 – Q3," Cyberint, Accessed: Feb. 5, 2026. [Online]. Available: https://cyberint.com/blog/research/ransomware-trends-2024-report/

[70] S. Zurier, "5.6 million patients affected by Ascension Health cyberattack," SC Media, Accessed: Feb. 5, 2026. [Online]. Available: https://www.scworld.com/news/5-6-million-patients-affected-by-ascension-health-cyberattack

[71] "Top Ransomware Attack Vectors: How to Defend Against Them," Censys, Accessed: Feb. 5, 2026. [Online]. Available: https://censys.com/blog/top-ransomware-attack-vectors

[72] D. Das, "Exploiting Medical Devices: Attack Vectors, Cyber Threats, and Advanced Defense Mechanisms," Security Boulevard, Accessed: Feb. 5, 2026. [Online]. Available: https://securityboulevard.com/2025/02/exploiting-medical-devices-attack-vectors-cyber-threats-and-advanced-defense-mechanisms/

[73] "Ransomware Activity Targeting the Healthcare and Public Health Sector," Cybersecurity and Infrastructure Security Agency (CISA), Accessed: Feb. 5, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a

[74] "Healthcare Cyber Threat Intelligence Report 2024," Health-ISAC, Accessed: Feb. 5, 2026. [Online]. Available: https://health-isac.org/wp-content/uploads/H-ISAC_2024-Annual-Report.pdf

[75] "HHS Issues Alert on Critical Vulnerability in 'MOVEit,' File Transfer Platform Used by Health Care Sector," American Hospital Association, Accessed: Feb. 5, 2026. [Online]. Available:

https://www.aha.org/advisory/2024-06-28-hhs-issues-alert-critical-vulnerability-moveit-file-transfer-platform-used-health-care-sector

[76] "Citrix Bleed attacks impact health sector," SC Media, Accessed: Feb. 5, 2026. [Online]. Available: https://www.scworld.com/brief/us-health-sector-subjected-to-citrix-bleed-attacks

[77] "Healthcare ransomware attacks surge 30% in 2025, as cybercriminals shift focus to vendors and service partners," Industrial Cyber, Accessed: Feb. 5, 2026. [Online]. Available: https://industrialcyber.co/reports/healthcare-ransomware-attacks-surge-30-in-2025-as-cybercriminals-shift-focus-to-vendors-and-service-partners/

[78] "Change Healthcare Ransomware Attack: A chronological timeline," Cyber Management Alliance, Accessed: Feb. 7, 2026. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/change-healthcare-ransomware-attack-a-chronological-timeline

[79] S. Schappert, "UnitedHealth rumored to have paid $22M to ALPHV/BlackCat hackers," Cybernews, Accessed: Feb. 7, 2026. [Online]. Available: https://cybernews.com/news/unitedhealth-22-million-ransom-paid-alphv-blackcat-hackers/

[80] L. Abrams, "Ransomware gang starts leaking alleged stolen Change Healthcare data," BleepingComputer, Accessed: Feb. 7, 2026. [Online]. Available: https://www.bleepingcomputer.com/news/security/ransomware-gang-starts-leaking-alleged-stolen-change-healthcare-data/

[81] A. Fox, "Ascension confirms data breached in Black Basta ransomware attack," Healthcare IT News, Accessed: Feb. 7, 2026. [Online]. Available: https://www.healthcareitnews.com/news/ascension-confirms-data-breached-black-basta-ransomware-attack

[82] S. Alder, "Ascension Ransomware Attack Affects 5.6 Million Patients," The HIPAA Journal, Accessed: Feb. 7, 2026. [Online]. Available: https://www.hipaajournal.com/ascension-cyberattack-2024/

[83] B. Herman, "Hospital giant Ascension recorded about $1.3 billion in losses from its cyberattack," STAT News, Accessed: Feb. 7, 2026. [Online]. Available: https://www.statnews.com/2024/09/18/ascension-financials-cyberattack-cost-losses/

[84] J. Davis, "Data ties healthcare cyberattacks to greater disruptions at nearby hospitals," SC Media, Accessed: Feb. 7, 2026. [Online]. Available: https://www.scworld.com/news/data-ties-healthcare-cyberattacks-disruptions-nearby-hospitals

[85] K. Jercich, "Ponemon study finds link between ransomware, increased mortality rate," Healthcare IT News, Accessed: Feb. 7, 2026. [Online]. Available: https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

[86] J. L. Tully, R. A. Gabriel, R. S. Waterman, and C. J. Dameff, "Digital Disasters: The Growing Threat of Healthcare Ransomware," Anesthesiology, vol. 142, no. 6, pp. 1005–1008, June 2025, doi: 10.1097/ALN.0000000000005442.

[87] M. Elgan, "Roundup: The top ransomware stories of 2024," IBM, Accessed: May 28, 2026. [Online]. Available: https://www.ibm.com/think/insights/roundup-the-top-ransomware-stories-of-2024

[88] S. Vogel, "Ascension posts $1.1B net loss for 2024 after May cyberattack," Healthcare Dive, Accessed: Feb. 7, 2026. [Online]. Available: https://www.healthcaredive.com/news/ascension-cyberattack-hurts-2024-earnings/727470/

[89] D. Bonderud, "Cost of a data breach 2024: Financial industry," IBM, Accessed: Jan. 14, 2026. [Online]. Available: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

[90] "The Hidden Cost of Healthcare Cyber Attacks: Beyond Ransoms and Regulatory Fines," HIMSS, Accessed: Feb. 7, 2026. [Online]. Available: https://www.himssconference.com/the-hidden-cost-of-healthcare-cyber-attacks-beyond-ransoms-and-regulatory-fines/

[91] N. Eddy, "Ransomware downtime costs U.S. healthcare organizations $1.9M daily," Healthcare IT News, Accessed: Feb. 7, 2026. [Online]. Available: https://www.healthcareitnews.com/news/ransomware-downtime-costs-us-healthcare-organizations-19m-daily

[92] S. Alder, "Cyber Insurance Claims Fall But Ransomware Losses Increase," The HIPAA Journal, Accessed: May 28, 2026. [Online]. Available: https://www.hipaajournal.com/cyber-insurance-claims-fall-ransomware-losses-increase/

[93] "The Security Rule," U.S. Department of Health and Human Services, Accessed: Feb. 10, 2026. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/security/index.html

[94] J. A. Marron, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," National Institute of Standards and Technology, Special Publication 800-66r2, Feb. 2024, doi: 10.6028/NIST.SP.800-66r2.

[95] "NIST Releases Version 2.0 of Landmark Cybersecurity Framework," National Institute of Standards and Technology, Accessed: Feb. 10, 2026. [Online]. Available: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

[96] "Cyber Safety is Patient Safety," HHS 405(d), Accessed: Feb. 10, 2026. [Online]. Available: https://405d.hhs.gov/

[97] "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions," U.S. Food and Drug Administration, Feb. 2026. Accessed: Feb. 10, 2026. [Online]. Available: https://www.fda.gov/media/119933/download

[98] "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity and Infrastructure Security Agency (CISA), Accessed: Feb. 10, 2026. [Online]. Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

[99] "Promoting Interoperability Programs," Centers for Medicare & Medicaid Services, Accessed: Feb. 10, 2026. [Online]. Available: https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs

[100] D. Larson, "Cybersecurity in Healthcare," CrowdStrike, Accessed: Feb. 19, 2026. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/cybersecurity/healthcare-cybersecurity/

[101] "Healthcare Cybersecurity in 2024: Building a Better Defence Against Rising Costs and Threats," Picus Security, Accessed: Feb. 19, 2026. [Online]. Available: https://www.picussecurity.com/resource/blog/healthcare-cybersecurity-in-2024

[102] Ł. Szymański, "Cyber Security Landscape 2024-2025: defense strategies and security technologies," nFlo, Accessed: Feb. 19, 2026. [Online]. Available: https://nflo.tech/knowledge-base/cyber-security-landscape-2024-2025-defense-strategies-and-security-technologies/

[103] "Automating Zero Trust in Healthcare: From Risk Scoring to Dynamic Policy Enforcement Without Network Redesign," The Hacker News, Accessed: Feb. 19, 2026. [Online]. Available: https://thehackernews.com/2025/04/automating-zero-trust-in-healthcare.html

[104] R. Pradhan and K. Wells, "Cyberattack led to harrowing lapses at Ascension hospitals, clinicians say," National Public Radio, Accessed: Feb. 19, 2026. [Online]. Available: https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses

[105] P. Szanowski and G. Burke, "Ransomware Backup Protection Strategy: Why Most Fail and What Actually Works," Object First, Accessed: Feb. 19, 2026. [Online]. Available: https://objectfirst.com/guides/ransomware/ransomware-backup-protection/

[106] "Healthcare Sector Cybersecurity Framework Implementation Guide," Cybersecurity and Infrastructure Security Agency (CISA), Accessed: March 9, 2026. [Online]. Available: https://www.cisa.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

[107] M. Gregory, "What Is Cyber Resilience, and How Should Healthcare Organizations Approach It?," HealthTech Magazine, Accessed: March 9, 2026. [Online]. Available: https://healthtechmagazine.net/article/2024/06/what-cyber-resilience-and-how-should-healthcare-organizations-approach-it

[108] A. Alharbi and A. Alkhalifah, "Cybersecurity governance in the healthcare sector during digital transformation: an integrated model and hybrid analytical approach," Frontiers in Public Health, vol. 13, p. 1703689, Nov. 2025, doi: 10.3389/fpubh.2025.1703689.

[109] "Cybersecurity in Healthcare: Risks, Best Practices & Frameworks," SentinelOne, Accessed: March 9, 2026. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-in-healthcare/

[110] "Recent Developments in Health Care Cybersecurity and Oversight: 2024 Wrap Up and 2025 Outlook," Epstein Becker Green, Accessed: March 10, 2026. [Online]. Available:

https://www.healthlawadvisor.com/recent-developments-in-health-care-cybersecurity-and-oversight-2024-wrap-up-and-2025-outlook

[111] "HPH Cybersecurity Performance Goals," HHS Cyber Gateway, Accessed: March 10, 2026. [Online]. Available: https://hhscyber.hhs.gov/performance-goals.html

[112] J. Riggi, "2025 Cybersecurity Year in Review, Part One: Breaches and Defensive Measures," American Hospital Association, Accessed: March 10, 2026. [Online]. Available: https://www.aha.org/news/aha-cyber-intel/2025-10-07-2025-cybersecurity-year-review-part-one-breaches-and-defensive-measures

[113] "Health Industry Cybersecurity Practices," HHS 405(d), Accessed: March 10, 2026. [Online]. Available: https://405d.hhs.gov/cornerstone/hicp

[114] "Framework for Improving Critical Infrastructure Cybersecurity Version 2.0," National Institute of Standards and Technology, Accessed: March 10, 2026. [Online]. Available: https://www.nist.gov/cyberframework

[115] B. Aldosari, "Cybersecurity in Healthcare: New Threat to Patient Safety," Cureus, vol. 7, no. 5, p. e83614, May 2025, doi: 10.7759/cureus.83614.

[116] J. Riggi, "A Look at 2024's Health Care Cybersecurity Challenges," American Hospital Association, Accessed: March 10, 2026. [Online]. Available: https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges

[117] E. Olsen, "Ascension cyberattack exposes data from 5.6 million people," Healthcare Dive, Accessed: March 10, 2026. [Online]. Available: https://www.healthcaredive.com/news/ascension-cyberattack-data-breach-5-6-million/736167/

[118] "Healthcare Cybersecurity Challenges & Threats – 2026 Update," Rubrik, Accessed: March 10, 2026. [Online]. Available: https://www.rubrik.com/insights/healthcare-cybersecurity-challenges-threats-2025

[119] S. Alder, "Bill Reintroduced to Strengthen Healthcare Cybersecurity," The HIPAA Journal, Accessed: March 10, 2026. [Online]. Available: https://www.hipaajournal.com/health-care-cybersecurity-resiliency-act-2025/

[120] G. Golani, "New Healthcare Cyber Regulations: What Security Teams Need to Know," Sentra, Accessed: March 10, 2026. [Online]. Available: https://www.sentra.io/blog/new-healthcare-cyber-regulations-what-security-teams-need-to-know

[121] "Health Care Cybersecurity and Resiliency Act of 2025: What It Signals for Healthcare Security," Clearwater Security, Accessed: March 10, 2026. [Online]. Available: https://clearwatersecurity.com/blog/health-care-cybersecurity-and-resiliency-act-2025/

[122] "Healthcare and Public Health Sector: Know the Risks, Use Cyber Hygiene," Cybersecurity and Infrastructure Security Agency (CISA), Accessed: March 10, 2026. [Online]. Available: https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare/use-cyber-hygiene

[123] A. Zellers, "The Healthcare Cybersecurity Act of 2025: What It Means for Your Risk Strategy," Chart Request, Accessed: March 10, 2026. [Online]. Available: https://www.chartrequest.com/articles/healthcare-cybersecurity-act-proposal

[124] "The Healthcare and Public Health Sector Highlights," U.S. Department of Health and Human Services, Accessed: March 10, 2026. [Online]. Available: https://aspr.hhs.gov/cyber/bulletins/Pages/20Dec2024.aspx

[125] "Health-ISAC Hacking Healthcare 3-5-2026," Health-ISAC, Accessed: March 10, 2026. [Online]. Available: https://health-isac.org/health-isac-hacking-healthcare-3-5-2026/

[126] "Healthcare Cybersecurity Act of 2025," U.S. Congress, Accessed: March 10, 2026. [Online]. Available: https://www.congress.gov/bill/119th-congress/house-bill/3841/text