Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.778004

CYBERSECURITY IN HEALTHCARE MEDICAL DEVICES IN HOSPITALS: APPLICATIONS AND CHALLENGES

Mohammed Alhebbi[1*], Abdualaziz Alshuhri[2], Adel Alzahrani, Ph.D[3]
[1*]King Abdulaziz Medical City- Jeddah, MNGHA, , Saudi Arabia, alhebbi@yahoo.com
[2]King Abdulaziz University, Jeddah, Saudi Arabia, azoz.1666@hotmail.com
[3]King Abdulaziz Medical City- Jeddah, MNGHA, Saudi Arabia, adelabz38@yahoo.com
***Corrresponding Author:** Mohammed Alhebbi
*King Abdulaziz Medical City- Jeddah, MNGHA, , Saudi Arabia, alhebbi@yahoo.com

Abstract
This research explores the diverse landscape of medical technology and healthcare cybersecurity, including many difficulties, issues, and ways to improve the safety and efficiency of healthcare services. The use of information and communication technology (ICT) in radiology and digital laboratories promises to speed up patient care delivery, while teleradiology and tele laboratory services help remote healthcare institutions. The World Health Organization's ASSURED standards for Point-of-Care Testing (POCT) are praised for their potential cost savings and increased clinical laboratory efficiency. A thorough understanding of cybersecurity risks and the "cyber kill chain" within clinical laboratories enables healthcare personnel to proactively counter cyber-attacks. The advent of the Internet of Things (IoT) and networked medical equipment provides significant prospects for improved patient outcomes, but effective cybersecurity measures are required to prevent related dangers. Vulnerabilities in medical equipment, especially outdated systems, risk patient safety and data security, demand collaboration with secure vendors. The necessity of cybersecurity in connected medical devices underpins the accomplishment of universal healthcare coverage, while cyberattacks pose hazards to patient safety and healthcare security. To ensure patient safety inside networked medical equipment, strong security measures, including data encryption, must be implemented. Furthermore, compliance with medical legislation and standards, such as HIPAA and GDPR, is critical in protecting patient data. The use of technology such as firewalls, antivirus and anti-malware applications, encryption, Virtual Private Networks (VPNs), intrusion Detection and Prevention Systems (IDPSs), and penetration testing strengthens healthcare cybersecurity. The introduction of hospital information systems (HIS), electronic medical records (EMR), electronic health records (EHR), and enterprise resource planning (ERP) technologies has simplified healthcare services in the Kingdom of Saudi Arabia. In conclusion, maintaining confidentiality, integrity, and data availability is critical for medical equipment cybersecurity, and a thorough risk management strategy provides a critical roadmap for lowering the risks associated with cyberattacks and data breaches in the arena of healthcare.

Keywords Cybersecurity, medical devices, Applications, Challenges, Hospitals, Healthcare.

Introduction and Literature Review

Cybersecurity is the management of techniques to safeguard the integrity of networks, programs, and data from unauthorized access to protect users or organizations in cyberspace.

According to the International Telecommunication Union, cybersecurity seeks to ensure the attainment and maintenance of security properties of organizations and user assets against cybersecurity risks. General cybersecurity objectives include availability, integrity (encompassing authenticity and non-repudiation), and confidentiality (Seemma et al., 2018)
In addition, cybersecurity has attracted significant political, social, and technological attention as contemporary societies have become increasingly reliant on computation. Today, at least within the Global North, there is an ever-pressing and omnipresent threat of the next "cyber-attack" or the emergence of a new vulnerability in highly interconnected supply chains. However, such discursive positioning of threat and its resolution has typically reinforced, and perpetuated, dominant power structures and forms of violence as well as universalist protocols of protection. (Dwyer et al., 2022)
Moreover, the maintaining of the integrity, security, and accessibility of information in Cyberspace is another definition of cybersecurity. Additionally, cybersecurity is described as measures undertaken to secure a system of computers or other devices against unauthorized access or attack in the Merriam-Webster dictionary (Taherdoost ,2022)
Additionally, provide terminology guidelines in the annex and explain that there is no clear-cut definition of "cyber security" that is agreed universally. This is important for government and nation state examination of national cyber security strategies of European Union member states. They note that some people think information security and cyber security overlap, but no firm conclusion is offered. claiming that a subset of information security is cyber security (Schatz et al.,2017).
In addition, the healthcare industry has experienced rapid growth, contributing to revenue and employment. Previously, diagnosis of diseases was only possible through hospital visits, increasing costs and straining rural facilities. Technological advancements have transformed healthcare systems from hospital-centric to patient-centric, enabling clinical analyses at home and remote communication of clinical data. Technologies like machine learning, big data analysis, IoT, wireless sensing, mobile computing, and cloud computing have improved accessibility and efficiency **(**Pradhan et al., 2021)**.**
Furthermore, Robert Morris developed the notion to estimate the extent of the internet at the end of 1988. To accomplish this, he created a program that would spread via computer networks, hack into Unix terminals using a known vulnerability, and then replicate itself. This most recent directive turned out to be incorrect. Morris worm's relentless replication caused the early internet to sluggishly slow down and do untold amounts of harm. More significantly, this action sparked the creation of the Computer Emergency Response Team (the forerunner to US-CERT), a nonprofit research facility for systemic problems that might have an impact on the entire internet. It seems as though the Morris worm was the beginning of something. Following the Morris worm, viruses began to multiply and infect an increasing number of systems. It appears that the worm foreshadowed the current era of widespread internet outages. You also started to notice the commoditization of antivirus software, with the founding of the first dedicated antivirus company in 1987 (Sentinelone, 2023).
Moreover, since computers got connected to the internet and began exchanging messages, cybercrime has substantially changed. Even if the amount of risk is substantially higher now than it was back then, computer users have been understandably concerned about these threats

for a long time (Bhadwal, 2023). However, the practice of testing for cybersecurity was introduced in the 1970s when researcher Bob Thomas created a computer program called Creeper that could travel throughout the ARPANET network. Ray Tomlinson, who invented email, developed the program Reaper to find and get rid of Creepers. Reaper developed the first-ever computer worms and trojans, making it the first instance of using an antivirus program to detect malware and the first virus that replicated itself (Khurpaderushi, 2022).

On the other hand, the 7 types of cyber security are designed to safeguard mission critical assets. Firstly, mission critical assets refer to the crucial data that requires protection. Secondly, data security controls ensure the secure storage and transfer of data. Thirdly, application security controls focus on securing access to applications, their access to mission critical assets, and the internal security of the applications. Fourthly, endpoint security controls protect the connection between devices and the network. Fifthly, network security controls aim to prevent unauthorized access to an organization's network. Sixthly, perimeter security controls encompass both physical and digital methodologies to protect the business as a whole. Lastly, human security controls recognize that humans are the weakest link in cyber security and include measures such as phishing simulations and access management to counter human threats (Department of information technology, 2021)

Article Body

Application of cybersecurity

Cloud assaults are a developing worry in the current technological era. Companies of all sizes are relying on keeping their data and files in the virtual cloud as a result of the rise of cloud computing. This offers accessibility and ease, but it also leaves room for security flaws. Particularly prevalent cybercrimes that target people online include phishing attacks. Attackers deceive users into disclosing private information like passwords and credit card data by sending bogus emails that look to be from reliable sources. Individuals and organizations must be cautious and adopt the appropriate security measures to guard against these online dangers (Mijwil et al., 2023).

In addition, an example of a cybersecurity threat is email phishing, where employees are tricked into revealing sensitive information through deceptive emails. Lack of awareness, IT resources, and protection software contribute to the success of these attacks, potentially leading to stolen access credentials and damaging the reputation of organizations (Ahmed et al., 2022). However, healthcare organizations face challenges in justifying cybersecurity investments compared to other areas like equipment, materials, training, and personnel. A study from IBM Security and the Ponemon Institute found that data breaches cost healthcare organizations $408 per record in 2018. Cybersecurity now encompasses protecting technology, networks, and databases, including securing computer systems and training personnel (Healthcare & public health sector coordinating councils, 2015).

Moreover, the American Institute of CPAs (AICPA) created a set of compliance requirements known as the SOCs. Simply said, SOC 2 ensures that clear safety measures are up to date with standards established by a third-party audit, preventing any business partnerships from being jeopardized. SOC 2 can create reports that are essential to information security, including

Personal Health Information (PHI), if you are designing a device for healthcare that in some manner manages retains, or transfers sensitive data. Today's companies, however, are dedicated to proving their level of security for protected health information (PHI), such as Software as a Medical Device. Securing sensitive data is equally important to offering high-quality medical care and placing the needs of patients before anything else (Sierra Labs, 2020).
Additionally, password attacks are a common method for cybercriminals to gain user information. These attacks can be carried out through various methods such as guessing, accessing password databases, or sniffing network connections. Keywords can be changed frequently, using unrecognizable words, and having minimum length. Brute force and dictionary attacks are two main techniques used to obtain passwords. (Biju et al., 2019).
Furthermore, a firewall protects an organization's network from threats like viruses, malware, and hackers by acting as a barrier between the network and the internet. It controls inbound and outbound traffic, and can be implemented using hardware or software. Firewalls can be optimized for specific operating systems (Pande, 2017).
Adding to that, formation security theory emphasizes the importance of maintaining confidentiality, integrity, and availability of information to ensure effective security protection. However, networked medical devices are susceptible to various risks. For instance, inadequate access control measures can lead to unauthorized access, compromising confidentiality. Additionally, poor configuration, data corruption, or unauthorized manipulation of information can impact the integrity of medical devices, potentially leading to incorrect clinical decisions and patient safety risks. Furthermore, limited or lost access to data or devices can affect availability, hindering access to critical information and potentially causing harm to patients if critical alerts are not received (Williams & Woodward, 2015).
So, in order to make it simpler to use the newest technological advances for higher-quality, quicker, and more dependable patient care, hospitals throughout KSA have adopted hospital information systems (HIS), electronic medical records (EMR), electronic health records (EHR), and enterprise resource planning (ERP) (Mishah et al., 2019).
Moving swiftly to, cyber-attacks on healthcare organizations that are increasing, with almost 30% of major incidents targeting them. Despite investing over $65 billion in cyber protection, healthcare institutions still face a high volume of attacks. The increasing dependence on technology in the healthcare system presents a new challenge to clinicians, public health experts, and policymakers. Cybersecurity, which protects computer-based technology from disruption, is in critical condition, with challenges such as a shortage of information security professionals, outdated legacy equipment, over-connected technologies, and software vulnerabilities in commonly used devices. The increasing reliance on technology in healthcare presents a new type of disaster, making cybersecurity a critical concern for clinicians, public health experts, and policymakers (Tully et al., 2020).
In addition, poor cybersecurity implementation in healthcare can lead to severe consequences for patient health and data security. The convergence of technology and stakeholder involvement has increased risk, with sophisticated cyber threats posing threats such as disruptions in patient care, deception, data breaches, and blackmail. Despite efforts, healthcare cybersecurity often fails to adequately safeguard patient health (Piggin, 2017).

Moreover, remote work security assurance, endpoint device management, human errors, a lack of security awareness, a lack of business continuity plans, a lack of coordinated incident response, budget and resource constraints, and the vulnerability of medical systems are the main cybersecurity challenges facing the health sector. These difficulties encompass both the security-related issues brought on by the COVID-19 pandemic as well as the inherent security difficulties in the healthcare industry that could be exploited by attackers during the COVID-19 pandemic. It is essential that healthcare organizations recognize these issues and take precautionary measures (He et al., 2021).

Although healthcare organizations' cybersecurity programs may not be as mature as they should be, there are several reoccurring problems that will reduce some hazards. For instance, there may be a dependency on systems that are built on legacy software for operations because the type of technology used within healthcare is specific to their context. These outdated systems, which need the Microsoft Windows 7 operating system to function, put operations at risk because the vendor does not support them and they do not have the newest security measures. Healthcare organizations should continue to run effective asset and lifecycle management programs to assess the size of their support infrastructure and pinpoint the dangers of outdated software. In addition, Due to the temporary condition of the job done on site, identity management can be challenging in large healthcare enterprises. Healthcare workers must be mobile within the hospital to interact with patients who need varied degrees of care in various places (Killeen et al., 2023).

Furthermore, Hospital ransomware attacks that become more severe have the potential to shut down entire healthcare systems. The 'White Hacker' discovery of health technology security flaws has raised concerns even more, raising the unsettling potential that pacemakers and insulin pumps could be remotely controlled (Coventry & Branley, 2018).

In addition, The Internet of Things and other innovations make remote medical care and precise healthcare delivery possible. However, security and privacy must be balanced with the usefulness and safety of therapeutic care. The hospital network has many networked devices, and there are significant amounts of clinical data that must be exchanged securely. However, these devices also have built-in constraints that make them vulnerable. They frequently lack the necessary security protections because they lack the battery life or internal resources to effectively apply security measures like malware detection, forensic processing, and encryption (Argaw et al., (2020).

Meanwhile, Medical device readiness to function in the current cybersecurity environment is also impacted by the lack of cybersecurity testing. For instance, manufacturers frequently utilize a clearly defined methodology to assess the safety of medical devices and test them using the FDA-recommended notions of "intended use" and "unintended misuse." However, this paradigm typically does not take into consideration a situation where there are active online enemies (Schwartz et al., 2018).

However, Medical equipment is susceptible to cyber-attacks since they are primarily made with medical purposes in mind (such as heart monitoring, insulin pumps, x-ray imaging, etc.) rather than cyber security requirements. Additionally, even though medical devices do not store patient data, hackers can still use them to gain access to the computer system (on the server) and carry out additional malicious use (which is not limited to information stealing; in

the worst-case scenario, the attacker could take over the medical devices and threaten lives of the patients). Additionally, email phishing is also considered to be one of the challenges facing medical devices in hospitals and labs which can steal patients' data. Moreover, ransomware attacks are also of great importance when it comes to challenges facing medical devices in labs and hospitals (Sendelj & Ognjanovic, 2022).

Moreover, Trickery of staff members with spoof email or fraudulent websites in order to obtain credentials for login or install malware, inadvertent or planned "Insider threat," that may represent a serious risk because of an absence of trust within an organization, loss of patient information, particularly electronic protected health information (ePHI), data theft, information leakage and loss of assets, blackmail, and extortion are just a few examples of the threats that can disrupt care and services and potentially result in patient deaths. phishing emails and ransomware assaults are further threats that put patients' safety at risk (Piggin, 2017).

Interoperability of medical devices is crucial for improving healthcare, reducing costs, and improving clinical decision-making. Addressing issues like accurate transmission, secure data reception, and data optimization is essential. Cybersecurity risks must be managed, and digital literacy can help reduce attacks and their frequency (Longras et al., 2023).

However, in Saudi Arabia in order to mitigate the risk of breakdown because of a cyberattack, that might have started by the infiltration of malware into the medical or by unauthorized utilization of configuration settings in medical devices and hospital networks, the SFDA advises hospitals to take the necessary precautions. In addition, Hospital incidents and malware can appear in a variety of ways. Clinics must have the capacity to acknowledge and take into account the following: Medical devices connected to the network or configured with malware that has disabled them; Malware affecting hospital computers, mobile devices, and tablets, targeting wireless technology on mobile devices to obtain patient data, devices for implanted patients and monitoring systems; Unrestricted password distribution, passwords that can't be changed, and hard-coded passwords for applications designed for privileged device access, such as workers in the administration, technology, and maintenance); Not updating and patching medical software in a timely manner to address relevant vulnerabilities in outdated medical devices, networks, and models of devices (legacy devices) (SFDA, 2019).

On the other hand, according to a recent analysis by Proofpoint Inc., the majority of the best hospitals in the United Arab Emirates and Saudi Arabia are lagging behind on fundamental cybersecurity measures. The report's conclusions are based on a DMARC analysis (Domain-based Message Authentication, Reporting and Conformance) study.

Only 28% of the top hospitals studied in the study had implemented the necessary level of DMARC protection, a validation procedure that safeguards domain names from fraudsters (Arabian Business, 2023).

Furthermore, according to a survey by the top cybersecurity firm Proofpoint Inc., most of the best hospitals in the UAE and KSA are falling behind on fundamental cybersecurity measures. A Domain-based Message Authentication, Reporting and Conformance (DMARC) examination served as the foundation for the conclusions. DMARC adds three degrees of protection to email communication security: monitor, quarantine, and reject. Only 28% of hospitals in the UAE and KSA have adopted the highest degree of protection, "reject,"

according to the report, leaving many consumers vulnerable to potential email fraud (Henshaw, 2023).

However, cybersecurity of medical devices can be achieved by maintaining confidentiality by protecting these devices from unauthorized disclosure, integrity by protecting these products from unauthorized modification, and availability of data by protecting these products from loss of function. A medical data breach, which is the release of secure or private/confidential information to an untrusted environment, can represent a security risk, a safety risk, or both. Five steps for a hospital or medical organization to improve medical device cybersecurity include establishing a risk management plan, building a protection framework, following basic security hygiene, including security in contracts, and building a zero-trust network. Hospitals that act to improve medical device cybersecurity will decrease the risk of privacy breaches, financial ransom, and harm to patients (Yuan et al., 2018).

In addition, the healthcare sector has integrated comprehensive models to improve services and prioritize individual needs. Cybersecurity helps monitor disease spread and track vaccine and drug supply. Data management is the main focus for digital healthcare, as these technologies significantly impact health services and service delivery. (Paul et al., 2023)

Moreover, healthcare organizations, maintain and transmit huge amounts of data to support the delivery of efficient and proper care. Nevertheless, securing these data has been a daunting requirement for decades. Complicating matters, the healthcare industry continues to be one of the most susceptible to publicly disclosed data breaches. In fact, attackers can use data mining methods and procedures to find out sensitive data and release it to public and thus data breach happens. While implementing security measures remains a complex process, the stakes are continually raised as the ways to defeat security controls become more sophisticated. As a result, it is crucial that organizations implement healthcare data security solutions that will protect important assets while also satisfying healthcare compliance mandates. Technologies in use Various technologies are in use for protecting the security and privacy of healthcare data (Abouelmehdi et al., 2017).

Healthcare devices are an integral part of present-day healthcare services. From the patients' imaging and diagnosis of the diseases to the treatment, healthcare devices are a key asset for the patients as well as the doctors. Since most of the healthcare devices nowadays are connected through the network, the vulnerabilities and cyber-attacks are also increasing. (Alhakami et al. 2021). While, Cybersecurity safeguards medical data, patient information, and assets from illegal access, disclosure, and usage. The number of possible digital gateways for cybercrime grows as technology advances. Regarding tracking patients' health, the Internet of Things (IoT), in conjunction with the cloud and big data, has opened up a new world of possibilities. (Javaid et al, 2023)

Furthermore, healthcare records have migrated from hard copy to primarily digital form over the last decade. These digital pictures are easy to distribute, which speeds up the diagnostic process. Of course, the fact that healthcare pictures may now be uploaded, shared, and kept digitally on personal mobile devices such as smartphones and tablets make them a target for cybercriminals. PACS (Picture archiving and communication system) also communicates with a variety of other systems, including electronic health records, regulatory registries, hospital (Coutinho et al, 2023).

From basic wooden tongue depressors and stethoscopes to extremely advanced computerized medical equipment, medical gadgets come in all shapes and sizes. A medical device is additionally defined by the World Health Organization (WHO) as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article" intended for use in the detection, avoidance, monitoring, and treatment of disease or other conditions. Medical equipment is deemed to be security-critical by hospitals if it performs some type of processing and communication, often by running software on specialized hardware and frequently using a variety of sensors. Sensing devices security risk since incorrect sensor readings could lead to clinicians' or devices' making incorrect treatment judgements afterwards. Information that is necessary for safety has an impact on a person's or an environment's level of safety (FDA, 2022)

While, Premendment Devices are devices that were lawfully marketed in the U.S. before May 28, 1976. These devices were in business distribution and were considered legal at that time. On the other hand, post-amendment devices are medical devices that have been marketed since 1976. The advancements in medical technology have significantly changed since then. Transitional devices, on the other hand, were regulated as new drugs before 1976. Micro medical devices, such as small controllers, are compact computers designed to control the operation of embedded systems and complex medical devices. Nano medical devices, on the other hand, involve cellular-scale sensors that provide high-resolution measurements of cellular-scale phenomena. (Devanandan & Shanmugasundaram, 2017)

Additionally, ICT used in radiology has been proposed to reduce turnaround times, allowing for faster availability of results. Digital laboratories have been reported as beneficial experiences, particularly in hospitals (when compared with primary care). Services like teleradiology and tele laboratory seem useful, particularly in outlying rural healthcare facilities. The World Health Organization (WHO) has established the ASSURED standards for POCT (Point-of-Care Testing) , which include being accessible to all individuals, equipment-free, robust, sensitive, specific, and user-friendly. Due to their speed and little reagent usage, which also lessens their environmental impact, these approaches have the potential to save costs in clinical laboratories and enhance efficiency (Fragão-Marques & Ozben, 2023).

To elaborate more, it is important for laboratory directors, managers, and supervisors to be familiar with the different types of cybersecurity risk and threat present today, in addition to the cyber kill chain. Briefly, the cyber kill chain is a reproducible model describing the different stages of a typical cyberattack, with each stage an opportunity to identify vulnerabilities and proactively defend against or react to an attack. The common stages include: (a) Reconnaissance; (b) Weaponization; (c) Delivery; (d) Exploitation, (e) Installation; (f) Command and control; and (g) Action. The kill chain has been used to trace the various steps adversaries pass through before successfully breaching a network or specific system, such that the progression of an attack can be understood and potentially mitigated (Patel et al., 2023).

While the following list includes benefits of medical technology. Medical technology benefits I'll start by listing each benefit of medical technology in turn.1. Hospital Communication Systems in Healthcare There are numerous tools available for patients to contact their doctors

or nurses. These digital devices are created for patients and installed in hospital patient wards or rooms. Patients can press the button on these gadgets in an emergency. It provides the doctors or nurses with the patient's arrival time information. This is one of the main advantages that technology offers to both patients and doctors. Using this type of equipment, the doctor can reach the patients swiftly and save their lives.2. Technology Improving Healthcare in Hospitals Numerous technical devices and tools have enhanced patient care or therapy. The portable defibrillator, drug management technology, MR system, and electronic IV monitors are a few recent technological advancements that have improved patient care.3. Hospital patient electronic health records Nowadays, computers are used to store the patient's medical history. Typically, medical facilities or specialized doctors keep complete patient health records on computers. (Marcos, 2023).

The penalty of not using IoT devices, however, can be far higher. Healthcare providers may enhance patient outcomes, decrease costs over the long term, and streamline processes with IoT devices. For instance, remote patient monitoring equipment can lower healthcare costs and avoid hospital readmissions. IoT devices can also offer predictive maintenance, enabling healthcare institutions to find and fix equipment flaws before they escalate into expensive concerns. Despite the possibly significant initial expenditure, healthcare providers should consider it because of the possible cost savings and increased productivity (Frackiewicz 2023). Over the past century, advancements in medicine have transformed treatment methods, with the discovery of electromagnetic radiation waves in 1895 by Wilhelm Conrad Rontgen. Today, medical devices, such as CT, fluoroscopy, and X-rays, are used in medical practices and hospitals. However, vulnerabilities have been demonstrated by Halperin, who reverse-engineered communication protocols to compromise medical devices. As technology continues to evolve, medical devices will become more interconnected, necessitating increased security measures. The USFDA, device manufacturers, and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) have joined forces to find and fix security flaws in equipment like pumps, ventilators, defibrillators, and monitors. To protect patient safety, hospitals are under pressure to partner with firms and suppliers who provide robust security features, such as data encryption (Greer, 2018).

While the UN Sustainable Development Goal 3 strives for universal health coverage, which includes inexpensive access to necessary medications and vaccines as well as financial risk protection, high-quality healthcare services. However, linked medical devices, including those based on AI, may become subject to cyberattacks if makers and stakeholders don't take steps to reduce cybersecurity risks. This might pose health concerns and erode patients' confidence in the security of healthcare (Kamenjašević, 2023).

Furthermore, reconnaissance, exploitation, and installation are the cyber kill chain stages that are most relevant for clinical labs because they are connected to the numerous potential security flaws that these facilities may have in their instrumentation, software, and system infrastructure. The presence of older, legacy systems that are no longer completely supported by the vendor or cannot be upgraded with modern cybersecurity solutions causes a number of instrumentation and software problems in clinical labs. In addition, Consequently, any cyberattack-related outages will almost probably have an impact on the clinical laboratory,

possibly significantly or even catastrophically. Clinical laboratories must therefore assume that a cyberattack will have an impact on their operations WHEN, not IF (Patel et al., 2023).

Discussion

While many studies have agreed upon a wide range of challenges facing medical devices in healthcare whether in labs or in hospitals, however there was a consensus on major specific challenges that should be put into consideration including: cyberattacks, poor cybersecurity, outdated software in medical devices, ransomware, malware attacks, lack of security protection measures and email phishing.

In addition, many studies confirmed that email phishing is a real threat that faces the devices which can have a significant impact on patients' safety by stealing their data (Piggin, 2017; Sendelj & Ognjanovic, 2022; Ahmed et al., 2022; Mijwil et al., 2023). On the other hand, other studies were fixated on ransomware attacks that severely impacts the healthcare systems. It is also of great importance when it comes to challenges facing medical devices in labs and hospitals while on the same time it threatens the lives of patients by stealing their data (Piggin,2017; Coventry & Branley, 2018; Sendelj & Ognjanovic, 2022).

Moreover, according to Sendelj & Ognjanovic (2022), Since medical devices are typically created with medical applications in mind (such as heart monitoring, insulin pumps, x-ray imaging, etc.) rather than cyber security requirements, they are vulnerable to cyber-attacks. Furthermore, despite the fact that medical devices do not store patient data, hackers can still use them to access the server's computer system and engage in other types of malicious activity (which isn't restricted to information theft; in the most serious scenario, the attacker could take control of the medical devices and endanger the lives of the patients). likewise, one of the difficulties faced by medical gadgets in hospitals and labs that can steal patients' data is email phishing.

Likewise, Tully et al. (2020), and He et al. (2021), both confirmed that software vulnerability and poor security protection in devices are two great challenges to cybersecurity in medical devices in hospitals. however, Tully et al. (2020), continued to elaborate concluding that cybersecurity, which guards against disruption of computer-based technology, is in critical condition due to problems such a lack of information security personnel, out-of-date legacy equipment, overly-connected technologies, and software flaws in frequently used gadgets. Cybersecurity is a crucial worry for physicians, public health professionals, and legislators since the growing reliance on technology in healthcare creates a new form of calamity.

While medical device readiness to function in the current cybersecurity environment is also impacted by the lack of cybersecurity testing (Schwartz et al., 2018). Furthermore, the SFDA advises hospitals to take the necessary precautions in Saudi Arabia in order to reduce the risk of breakdown due to a cyberattack, which may have started by the infiltration of malware into the medical or by the unauthorized utilization of configuration settings in medical devices and hospital networks (SFDA, 2019). However, it also agrees with (Piggin, 2017; Argaw et al., 2020; SFDA, 2019). that malwares are of great risk for medical equipment's in hospitals.

Moreover, KSA are falling behind on fundamental cybersecurity measures. A Domain-based Message Authentication, Reporting and Conformance (DMARC) examination served as the foundation for the conclusions. DMARC adds three degrees of protection to email communication security: monitor, quarantine, and reject. while also Saudi Arabia are lagging behind on fundamental cybersecurity measures. The report's conclusions are based on a DMARC analysis (Domain-based Message Authentication, Reporting and Conformance) study (Henshaw, 2023; Arabian Business, 2023).
On the other hand, according to Munir et al. (2023) and Pande, (2017), they both agreed on the crucial role of firewall. This upholds previously stated security guidelines. Additionally, by serving as a firewall between a private internal network and the open Internet, sensitive information and computer systems are protected from cyber threats. Also, by serving as a firewall between a network and the internet, safeguards a company's network from risks like viruses, malware, and hackers. In addition, antivirus and anti-malware programs, process of encryption, Virtual Private Networks (VPNs), intrusion Detection and Prevention Systems (IDPSs) and Penetration testing are all types of cybersecurity applications that are beneficial against cyberattacks (Munir et al., 2023).
Moreover, A comprehensive plan should include security controls at the technical, operational, and administrative levels to protect the device, the data, and the network. The ultimate objective is to reduce the vulnerabilities in medical imaging equipment connectivity through a system of security controls and risk management tools at each step of the device's life, from operational usage and support through the end of product life (Healthcare, 2015).

Likewise, according to Claroty (2023), there are medical regulations and standards that have been discussed and implemented in order to increase the efficiency and effectiveness of medical devices as well as protecting patient’s data and ensures his safety, for example, HHS Section 405(d): To create a risk-based framework for a methodical approach to risk reduction, , IPAA A federal statute in the United States called the Health Insurance Portability and Accountability Act (HIPAA) sets tight guidelines for the security and privacy of patient health information (PHI), GDPR The General Data Protection Regulation (GDPR), a comprehensive data protection and privacy law in the European Union (EU), is similar to HIPAA. This law has a substantial impact on the security and privacy protocols connected to medical equipment that handles personal data (Claroty, 2023). While, if you are building a healthcare equipment that in any way handles, stores, or transfers sensitive data, SOC 2 can produce reports that are crucial to information security, including Personal Health Information (PHI) (Sierra Labs, 2020).

More precisely in the Kingdom of Saudi Arabia, to make it simpler to use the most recent digital solutions for higher-quality, quicker, and more dependable patient care, hospitals throughout KSA have adopted hospital information systems (HIS), electronic medical records (EMR), electronic health records (EHR), and enterprise resource planning (ERP) (Mishah et al., 2019).
On the opposite extreme, advantages can be introduced in the literature by starting with maintaining confidentiality by preventing unauthorized disclosure, integrity by preventing

unauthorized modification, and availability of data by preventing function loss are all ways to ensure the cybersecurity of medical equipment. hospital or medical facility to upgrade medical equipment Building a protective framework and creating a risk management plan are both aspects of cybersecurity. As a result of increased device cybersecurity, there will be less risk of patient damage, financial extortion, and data breaches (Yuan et al., 2018).

Cybersecurity aids in keeping an eye on the distribution of medications and vaccines as well as the spread of disease. Given that these technologies have a considerable impact on health services and service delivery, data management is the primary area of concern for digital healthcare. & preserving the privacy of data, and also safeguards medical data, patient information, and assets from illegal access, disclosure, and usage ((Paul et al., 2023; Abouelmehdi et al., 2017; Javaid et al, 2023)

Conclusion and Future Work

In cybersecurity age, many opportunities and challenges are arising rapidly considering how fast and dynamic is the progress in the environment. In addition, in healthcare sector cybersecurity plays a vital role in enhancing and improving the functionality of medical devices in hospitals and labs. This paper covers the challenges, applications and advantages of cybersecurity in healthcare medical devices in both labs and hospitals. in addition, challenges including data breach, ransomware, malware, data theft, phishing emails, cyberattacks, poor cybersecurity measures, outdated software that can lead to the fall or shut down of the healthcare system and lack of cybersecurity testing for medical devices readiness to function. Applications on the other hand, includes, Firewall program with its various types, antivirus and anti-malware programs, process of encryption, Virtual Private Networks (VPNs), intrusion Detection and Prevention Systems (IDPSs) and Penetration testing are all types of cybersecurity applications that are beneficial against cyberattacks. And finally, advantages including Iot, big data and cloud, data management in order to safeguard data, information and valuable assets from infiltration or breach and to keep tracking patient's health. While, also shedding the light on the level of development of cybersecurity in the Kingdom of Saudi Arabia's hospitals which Only 28% of the top hospitals studied in the study had implemented the necessary level of DMARC protection, a validation procedure that safeguards domain names from fraudsters. However, the Kingdom is adopting a new approach by including cybersecurity in the Saudi's vision 2030 which will reflect positively on the healthcare sector. Furthermore, as this paper investigated the cybersecurity in healthcare medical devices and labs in the Kingdome of Saudi Arabia, still the field needs more research to tackle different aspects of cybersecurity's correlation with medical devices in hospitals and labs like including big data. As patient's data is huge, thus there is a need to tackle more challenges and applications facing the total integration of data when covering millions of people.

References

1. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80. https://doi.org/10.1016/j.procs.2017.08.292

2. Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy*, *2*(4), 853-861. https://doi.org/10.3390/jcp2040043
3. Alhakami, W., Baz, A., Alhakami, H., Ahmad, M., & Khan, R. A. (2021). Healthcare Device Security: Insights and Implications. *Intelligent Automation & Soft Computing*, *27*(2), 409- 427. https://doi.org/10.32604/iasc.2021.015351
4. Arabian Business, (2023, July 12). *UAE, Saudi hospitals putting patients at cybersecurity risk*. https://www.arabianbusiness.com/industries/healthcare/uae-saudi-hospitals-putting-patients-at-cybersecurity-risk-report-says
5. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, 1-10. https://doi.org/10.1186/s12911-020-01161-7
6. Bhadwal, A. (2023, Sep. 15). *The History of Cyber Security: A Detailed Guide. Knowledge hut upgrade*. Knowledgehut. https://www.knowledgehut.com/blog/security/history-of-cyber-security
7. Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber-attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), 4849-4852.https://www.irjet.net/archives/V6/i3/IRJET-V6I31244.pdf
8. Claroty. (2023, Jan 26). *Cyber Patient Safety and Medical Device Effectiveness.* https://claroty.com/blog/protecting-patient-safety-and-medical-device-effectiveness.
9. Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. *Computers & Security*, *129*, 1-19. https://doi.org/10.1016/j.cose.2023.103189
10. Coventry, L., & Branley, D. (2018). *Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. Maturitas, 113, 48–52.* https://doi.org/10.1016/j.maturitas.2018.04.008
11. Department of information technology. (2021). *Digital notes on cyber security*. Malla reddy college of engineering & technology. https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf
12. Devanandan, P. & Shanmugasundaram, P. (2017). Comprehensive review on various types of medical devices used in hospitals. *Journal Of Advanced Pharmacy Education and Research,* *7*(3), 171-174. https://www.researchgate.net/publication/322655855_Comprehensive_review_on_various_types_of_medical_devices_used_in_hospitals
13. Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What can a critical cybersecurity do? *International Political Sociology*, *16*(3),1-26. https://doi.org/10.1093/ips/olac013
14. Frackiewicz, M. (2023, March 2). *The Advantages and Disadvantages of IoT in Healthcare*. T52. https://ts2.space/en/the-advantages-and-disadvantages-of-iot-in-healthcare/

15. Fragão-Marques, M., & Ozben, T. (2023). Digital transformation and sustainability in healthcare and clinical laboratories. *Clinical Chemistry and Laboratory Medicine (CCLM)*, *61*(4), 627-633. https://doi.org/10.1515/cclm-2022-1092
16. Greer, B. J. (2018). *Cybersecurity For Healthcare Medical Devices* (Doctoral dissertation, Utica College). Specialusis ugdymas. https://www.researchgate.net/publication/325746918_CYBERSECURITY_FOR_HEALTHCARE_MEDICAL_DEVICES
17. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of medical Internet research*, *23*(4), 1-18. https://doi.org/10.2196/21747
18. Healthcare & public health sector coordinating councils. (2015). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf
19. Henshaw, C. (2023, Aug. 29). *Strategies to protect Saudi Arabia healthcare from cyberattack*s. Omnia Health. https://insights.omnia-health.com/saudi-arabia/strategies-protect-saudi-arabia-healthcare-cyberattacks
20. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1-13. https://doi.org/10.1016/j.csa.2023.100016
21. Kamenjašević, E. (2022). *Cyber(in)security of medical devices*. KU Leuven Centre for IT & IP Law.https://sdgs.un.org/sites/default/files/2023-05/A3%20-%20Kamenjasevic%20-%20 Cyberinsecurity%20of%20medical%20devices.pdf
22. Khurpaderushi. (2022, June 22). *History of Cyber Security. DSA*. https://www.geeksforgeeks.org/history-of-cyber-security/
23. Killeen, R., Burrell, J., Lawlor, A., Quinn, C., & Kelly, B. (2023). Cybersecurity in Healthcare. *Trends of Artificial Intelligence and Big Data for E-Health*, 213–231. https://doi.org/10.1007/978-3-031-11199-0_11
24. Longras, A., Pereira, T., & Amaral, A. (2023). Cybersecurity Challenges in Healthcare Medical Devices. In *International Conference on Internet of Everything* (pp. 66-75). Springer, Cham. https://doi.org/10.1007/978-3-031-25222-8_6
25. Marcos, K. (2023). *Advantages and Disadvantages of Medical Technology in Healthcare*. Sultan Kudarat State University. https://www.studocu.com/ph/document/sultan-kudarat-state-university/biology/advantages-and-disadvantages-of-medical-technology-in-healthcare/24051870
26. Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian journal of cybersecurity*, *2023*, 57-63. https://doi.org/10.58496/MJCS/2023/010
27. Mishah, N., Bukhari, A., Almutairi, B.S., & Mohreq, M. (2019). Status of e-security and privacy protection in Saudi hospitals. *Comput. Methods Programs Biomed., 171*, 5-6. https://doi.org/10.1016/j.cmpb.2018.12.012
28. Munir, S., Khan, K., Aslam, D. N., Abid, K., & Rehman, M. (2023). Humanoid Robots: Cybersecurity Concerns and Firewall Implementation. *VFAST Transactions on Software Engineering*, *11*(1), 85–100. https://doi.org/10.21015/vtcs.v11i1.1454

29. Pande, J. (2017). *Introduction to cybersecurity*. Uttarakhand Open University. https://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
30. Patel, A. U., Williams, C. L., Hart, S. N., Garcia, C. A., Durant, T. J., Cornish, T. C., & McClintock, D. S. (2023). Cybersecurity and Information Assurance for the Clinical Laboratory. *The journal of applied laboratory medicine*, *8*(1), 145-161. https://doi.org/10.1093/jalm/jfac119
31. Paul, M., Maglaras, L., Ferrag, M., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express, 9*(4), 571-588. https://doi.org/10.1016/j.icte.2023.02.007
32. Piggin, R. (2017). *Cybersecurity of medical devices addressing patient safety and the security of patient health information*. BSI. https://www.medical-device-regulation.eu/wp-content/uploads/ 2020/09/White_Paper___Cybersecurity_of_medical_devices.pdf
33. Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-based applications in healthcare devices. *Journal of healthcare engineering*, *2021*, 1-18. https://doi.org/10.1155/2021/6632599
34. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2),53- 79. https://doi.org/10.15394/jdfsl.2017.1476
35. Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., ... & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical instrumentation & technology*, *52*(2), 103-111. https://doi.org/10.2345/0899-8205-52.2.103
36. Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *Ijarcce, 7* (11), 125–128. DOI:10.17148/IJARCCE.2018.71127
37. Sendelj, R., & Ognjanovic, I. (2022). Cybersecurity Challenges in Healthcare. In *Achievements, Milestones and Challenges in Biomedical and Health Informatics* (pp. 190-202). IOS Press. http://dx.doi.org/10.3233/SHTI220951
38. Sentinelone. (2023, Oct. 3). *The History of Cyber Security — Everything You Ever Wanted to Know*. https://www.simplilearn.com/introduction-to-cyber-security-article#:~:text=Enroll%20 now!-,What%20is%20Cyber%20Security%3F,confidence%20in%20products%20and%20 services.
39. SFDA. (2019). Guidance to Medical Devices Cybersecurity for Healthcare Providers. https://www.sfda.gov.sa/sites/default/files/2019-10/MDS-G36_0.pdf
40. Sierra Labs. (2020, Oct. 1). The Importance of SOC 2 Certification for Healthcare. https://blog.sierralabs.com/the-importance-of-soc-2-for-healthcare-organizations
41. Taherdoost, H., (2022). Cybersecurity vs. Information Security. *Procedia Computer Science 215*(6), 483-487. https://doi.org/10.1016/j.procs.2022.12.050
42. Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health security*, *18*(3), 228-231. https://doi.org/10.1089/hs.2019.0123

43. US food and drug (FDA). (2022, Sep. 29). *How to Determine if Your Product is a Medical Device.* https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device
44. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305-316. https://doi.org/10.2147/MDER.S50048
45. Yuan, S., Fernando, A., & Klonoff, D. C. (2018). Standards for medical device cybersecurity in 2018. *Journal of diabetes science and technology*, *12*(4), 743-746. https://doi.org/10.1177%2F1932296818763634