IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# CYBERSECURITY PRIMER FOR PHARMACIST: A REVIEW

***Sub title: Cybersecurity in Healthcare industry***

**RANJITHA C J*, SOWMYA B A, Dr. RAMESH C, ASMA SHAIKH**

Assistant professor, Assistant professor, Professor, Assistant professor

Department of Pharmacology, East West college of Pharmacy, Bangalore-560 091, India

## ABSTRACT:

The use of information and communications technology (ICT) in healthcare systems has been increasing in recent years. With healthcare systems adopting healthcare information systems, the healthcare industry has become more susceptible to cyberattacks. The role of pharmacists in healthcare is changing to a greater degree, as pharmacists can play a key role in the healthcare delivery system. Pharmacists have traditionally focused on health outcomes and medication therapy management and were responsible for the storage, use, and distribution of medications, while pharmacy technicians were responsible for dispensing medications. In addition, the use of mobile technology and the Internet for health care purposes has contributed to increased opportunities for the sharing of personal information. Despite some progress, much remains to be done to protect and promote the privacy and security of health information. Pharmacists are a natural group to take the lead in protecting the privacy of health information as their role is deeply intertwined with health and health care. Additionally, as health information technology advances, pharmacists will be in a unique position to promote privacy and security as a fundamental right for health care.

**Key words:** Healthcares, Software's, Technologies, Pharmacist & Cybersecurity.

## INTRODUCTION:

Cybersecurity is quickly becoming a vital component to every pharmacy practice and it can be a challenging job. Pharmacists are considered some of the highest risk individuals for hackers to infiltrate and this is not the case for a large portion of the population. Cybersecurity is the act of securing the network or data that is stored in electronic form. The pharmacist has the opportunity to play a large part in securing the pharmacy's computer network, the pharmacy's internet presence, and each patient's data that is stored on the pharmacy's server. As a pharmacist, the job as an information security professional is to manage the security of the pharmacy's data. The information being managed here would be patient data, prescription data, patient education and marketing materials and the list goes on and on. The primary goal of information security is to protect patient's data from accidental or intentional misuse by the pharmacy's staff. To protect the safety of the pharmacy's data, it is important to have a plan for how the security system is set up.

It is getting harder to keep up with it all. As part of the pharmacist's continuing education (CE) requirement, it is important to be aware of these challenges and know the fundamentals of what makes up a Cybersecurity threat and how to prepare for them. As pharmacists in charge of patient data and drug information systems (DIS), pharmacist must be aware of the many ways patients' data could be breached and how hackers could gain unauthorized access. Pharmacist have to be familiar with the different types of computer and mobile devices a patient may use, to ensure that their data is kept private and secure. Pharmacist must work closely

with Cybersecurity experts to ensure to take all necessary precautions. Today's pharmacists face increased risk in the form of potential exposure to Cybersecurity threats through information exchange and transactions. Pharmacy is an extremely popular target for cyber attacks. Cyber attackers target vulnerable business systems and seek a route to cause loss of valuable assets, or to obtain personal information. They can steal intellectual property, fraudulently bill consumers, or sell their access to customer health information[1].

Pharmacy's role in healthcare is unique. Pharmacists can help protect patients from adverse effects of medications by identifying drug interactions. By helping patients identify, select, and take the right medication at the right time. Additionally, pharmacist is a key position to protect the public from the dangers of certain controlled substances like heroin and methamphetamines. But they are not prepared to meet the threats that are becoming a greater concern to pharmacists every day. Pharmacists are not immune to the digital threats that are constantly growing and expanding. Pharmacy is considered one of the first high-risk industries to be affected by cyber security threats. Cybersecurity is a complex process of both prevention and response that can occur at any time. Pharmacy needs to stay ahead of the game to prevent cyber attacks from occurring or to counter attack strategies. The most fundamental requirement to safeguard pharmacy from security threats is Cybersecurity training. Security training can be obtained in two different ways: online or through a classroom experience. A combination of both training approaches can also be combined to make training more effective.

To prevent this cyber attack it is necessary to educate the Pharmacist. The objective of Cybersecurity training is to educate pharmacists about how Cybersecurity works, why it's so important to understand it, and how it relates to the pharmacy business and workflow. Training also helps pharmacists determine what Cybersecurity solutions can help reduce the possibility of an attack or mitigate against an attack in the first place. When pharmacists are educated about Cybersecurity and what solutions exist, they can create an appropriate plan of defense against cyber threats. The best defense is a strong offense. Pharmacists should educate the entire pharmacy team, including management and patients. Pharmacy is often on the front line when it comes to Cybersecurity threats. Pharmacists should be prepared to answer questions and address any concerns about Cybersecurity. Pharmacists should create a plan to mitigate the threats and attacks that are growing with unprecedented speed.

Education can be achieved in both an online and classroom setting. Online courses are convenient, affordable, and the ability to take them on the go is also great. However, the downside of an online education is the lack of one-on-one interaction between the student and instructor. In classroom settings, pharmacists will have more opportunity to ask questions, ask for help, and be part of the discussion. Both types of training can be effective when the content is effective and the training is personalized for the learner. There are many topics that need to be addressed when it comes to training pharmacists on Cybersecurity. All pharmacies should be familiar with the major areas of Cybersecurity threats that pharmacists. Pharmacy is one of the first high-risk industries to be affected by cyber security threats. Cyber attacks against the healthcare industry are on the rise. There are many reasons why pharmacists need to be prepared to address Cybersecurity issues. The rapid expansion of the Internet of Things (IoT) has increased the number of Cybersecurity vulnerabilities. The exponential growth in Cybersecurity threats and their complexity will continue to increase. It is imperative that pharmacists understand how Cybersecurity works and how it affects pharmacy workflow[2].

## RISK FACTORS FOR CYBER ATTACKS IN HEALTHCARE:

Cyber security has become a prominent issue in the healthcare industry in the recent times. To deal with the cyber threats, Cybersecurity measures, such as secure network design, vulnerability assessment, security incident response and cyber defense have been taken by many enterprises. An effective risk analysis will enable the enterprises to identify potential threats and to reduce risks. A cyberattacks can disrupt IT services and lead to financial losses, which are especially detrimental to a hospital or healthcare facilities. A similar number of attacks hit hospitals around the world in the same year. The threat of cyber attacks to health care industry becomes more severe and urgent. The healthcare sector has the highest volume of data, which makes it easier for hackers to exploit. In the past, the industry has underestimated the threat to patient care and security[3].

In an attempt to mitigate the risk of cyber attacks in healthcare, pharmacist have conducted a risk analysis for three different scenarios in healthcare industry. Pharmacist have identified various security risks and evaluated cyber risk in hospitals. Pharmacists have used the risk analysis results to perform cyber risk management for

healthcare industry. The risk analysis results of three scenarios can provide a foundation for the analysis of a hospital risk, which is needed in risk-based service planning. The rise in cyber attacks is being blamed on the proliferation of malware and ransomware, a type of malicious software that aims to hold information, money or both, ransom, for example for the so called WannaCry virus. The rise in cyber attacks could also have an impact on patient care within the NHS and other organisations that provide care to patients. By developing malware, cyber attackers seek to access a healthcare organisation's IT network and obtain sensitive patient information such as electronic health records. Ransomware is also a problem for healthcare organisations as it has the ability to encrypt files and lock users out of their system until a ransom is paid. In terms of patient care, cyber attacks can have a big impact as they may delay or even prevent patients receiving vital treatment. Ransomware can be used to attack multiple healthcare organisations at the same time, leading to disruption to services and impacting patients care. Ransomware as a technique is growing, becoming more sophisticated and therefore harder to prevent and deal with[4].

### 1.1. User accounts with simple passwords:

Password should be easy to remember, contains special characters and numbers, and is unique to an individual. Most often password is the weakest link to protect data of an individual and its misuse can open the gateway for hacking attacks. A password needs to be unique. So in order to store information and use, the system needs to authenticate the user with that unique password. A password is the most important aspect of user authentication. A user password is a sequence of characters which can be entered into the system by the user and it is the only way by which a user can access the system to perform their work. The password is one of the basic factors for authentication, which is generally comprised of a secret identification number (ID) and a password. The first four-digit ID could be a sequence of randomly generated characters (such as alphanumeric); that should be changed on every new user creation. The following four to six digit ID or password, which is more than four digits, is generally considered as a password. Both the ID and password need to be changed frequently to avoid security vulnerabilities. Many systems offer a simple ID, a password and a PIN as the means of authentication[5].

Password strength has become a hot topic with the introduction of stronger password authentication mechanisms. Password length and length constraints have become the most important component of the standard security approach of a given authentication system. As the complexity and length of passwords have increased, the number of potential passwords has also increased exponentially. In order to reduce the vulnerability of a password, a password needs to meet at least one of the following conditions: Password should be easy to remember, Password should be strong, Password should be unique, Password should be different from all other passwords, Password needs to be changed after being used & Password should be different from its original form.

### 1.2. Unrestricted remove access:

The Healthcare sector can be considered as one of the most attacked sectors in the world due to the high volume of data generated by the patients and their related treatments. The patients often want to protect themselves through the protection and control of their data. So, the patients request for an access control to be performed in their electronic records to protect their data. The patients want to maintain an up to date and secure Electronic Records (EHRs) at all times. This can be achieved by granting an access to the users that are allowed to have access to certain electronic records. The EHRs are considered to be a valuable data in the patient's life. They will need to store their data in the data centers to protect their data from the threats. If this is not possible, they can take a backup of their data in the EHR's cloud services. As these electronic records are considered as a high risk in the healthcare sector, it is important that the healthcare sectors comply with the security standards and perform security best practices. In order to protect the EHRs and the patients' data from the threats, it is important to perform a risk analysis and a risk assessment[6].

The first step is to perform a risk analysis to identify the risks related to the electronic records. This is usually achieved through the use of a risk analysis matrix. The matrix can be used to determine the risks that may occur due to the potential exposure to data breaches and risks that are associated with certain use cases. The exposure may occur as a result of a hack, an unauthorized access, a lost device or unauthorized disclosure of information etc. Critical assets are usually the assets that are considered to be a high risk in case of a data breach or a data theft. For example, the patients' health information and data records are considered to be critical assets as the information could be used by unauthorized parties to steal the patient's identity. These are the processes that are

being performed in an organization. It is usually considered as high risk if the data that is collected during the performance of the processes is unencrypted and stored[7].

**1.3. Outdated or Unsupported software's:**

The cyber risk factor is quite common for the Hospitals and other healthcare providers. It is due to lack of robust security, vulnerable networks and poorly implemented network monitoring and firewalls. Lack of robust security is the main risk factor. To provide the quality health services to its consumers, it needs to have robust security. The security is an enabler, which is an essential for organizations, to achieve its financial and operational goals[6]. So the healthcare providers should have robust and flexible security that can identify threats before they cause any damage. It is the only security layer that can provide comprehensive defense from all cyber-attacks. It has been estimated that the cyber security incident costs can range from 2.5% to 5% of the organization's annual budget. And this expense is the main risk factor, to cyber risk in the healthcare industry. In some organizations the security costs can be much higher, that may reach up to 11% of the organization's annual budget[8]. To deal with this kind of security threat, healthcare organizations are moving towards the use of digital health records, e-prescribing, electronic health records (EHR), online medical records, telemedicine, tele-monitoring etc.

For a smooth operation, the security monitoring and the network firewalls are essential. If they are not properly configured and managed, they can increase the risk and cause the loss of data. For instance, the hackers can hack the patient data that leads to an identity theft. Due to its misuse, the healthcare organizations spend a huge amount of money for the IT services to maintain its safety. Moreover, this expenditure also increases the cyber risk, due to the improper implementation of cyber-security. To deal with this issue, the use of new technologies for monitoring and firewalls is also essential. For instance, it is suggested to combine the cloud-based security with the traditional security for an efficient monitoring and security solution. With the cloud-based security, it can provide real-time security monitoring. It will have a better visibility and faster reaction to any cyber-attack. And the cloud-based security can be easily managed by the help of its application management tools. Moreover, it has the flexibility to work as per the requirement[9].

**1.4. Outdated anti-virus software's:**

The healthcare industry has been the target of cyber attacks for a long time. Nowadays, the number of cyber-attacks in the healthcare sector has increased dramatically. The industry that is the most affected by these cyber-attacks is the healthcare services, where the personal data and information are highly confidential. Every healthcare system is the most complex system to handle the attacks, the hackers are looking to gain access to the system to perform cyber-attacks with the help of outdated anti-virus. Healthcare is an expensive area for the IT managers and the administrators. With the increasing number of online activities, cyber-attacks on the Healthcare have increased with the number of healthcare users. The Healthcare is vulnerable to cyber-attack, as the data in the healthcare centers are stored on unsecured endpoints. There is hundreds of patient information on unsecured databases. The hacker can easily access these databases through the cyber attack. The hackers can compromise the security of the system with the help of outdated anti-virus software. The healthcare data in the unsecured systems is easily accessed by the hackers. All the patient data is stored on multiple servers, unpatched or vulnerable servers are also making the healthcare system vulnerable to the cyber-attack[10].

The healthcare data is stored on end-points of the healthcare systems. As these end-points are not protected with the Anti-virus, the hackers can easily attack the endpoint through the data theft. The healthcare systems are stored with the unpatched or unsecured servers, and the hackers can easily attack these servers with the help of cyber-attack tools. The endpoint has the open ports, the hackers can easily attack the system. The outdated anti-virus software is one of the risk factors for cyber-attacks in healthcare. The outdated anti-virus software can easily capture the data from the system, and the hackers can easily attack the system with the help of information obtained. The IT system in the healthcare can be a potential target for cyber-attack. The IT system in the healthcare is vulnerable to attacks. This is because the healthcare IT system has more vulnerability due to the security lapses or errors in the healthcare systems. There are more risks and threats for the IT system in the healthcare. As the IT system in the healthcare is open to all the attackers, the IT system in the healthcare is a risk area for hackers. The healthcare systems are open to all the attacks, and the IT systems in the healthcare are a good target for hackers. The healthcare IT systems have more risks due to its openness and access, the hackers can easily attack the system with the help of exploits, by the help of an exploit kit, and the hacker can easily attack the system.

**BEST PRACTICES TO PREVENT CYBERATTACKS:**

Cybersecurity is one of the biggest concerns of health systems and healthcare IT. Most healthcare organizations and medical facilities are already well aware of the threats to their IT infrastructure, but they still lack a comprehensive and integrated strategy to prevent cyberattacks. Cybersecurity is not a new issue but have a lot of challenges associated with it. Healthcare organizations and health IT vendors are focusing on how to effectively secure their data in order to avoid getting hacked. Healthcare organizations, including hospitals and health systems are being targeted to access patients' sensitive data. While organizations have started to address these risks, a lack of security expertise and the inability to effectively address the risks have hindered their ability to prevent and effectively mitigate the threat. Healthcare organizations are being attacked and it is no longer only high-end healthcare organizations, but also medium and low-tier ones. Healthcare organizations need to be aware of the threats and the potential dangers associated with it, especially with data. Healthcare organizations are spending a lot of money and resources to mitigate the risks of threats and hackers. However, a lot of them still believe that they can avoid a lot of potential risks. It is important to understand that hacking, a data breach, frauds and unauthorized data access is always possible[11].

**2.1. Eliminate Local & Generic users:**

Many users from different organizations can use the same username and passwords for different web applications on the organization's website. For example, a local user from accounting department can use the same username and password to access the company's stock database. The same username and password can be reused by a malware or ransomware to attack the stock database. Generic user accounts (like admin and user) can be created on user databases for all applications on the company's website. The generic user accounts are a common way for attackers to login to the company's systems with the same credentials to access all the company's systems. Criminals and hackers use these kinds of tricks to steal data from their victims, the local and generic usernames and passwords they use for authentication to their networks should not be the same as their personal or commercial usernames and passwords. The purpose of using generic users is not only to prevent hackers from stealing data from the network, but to prevent healthcare business owners from committing fraud[12].

The healthcare organizations have some of the most critical applications they need to protect, ranging from Electronic Health Records, Electronic Imaging, Electronic Prescription, Electronic Claims, and more. Many of them are running on legacy operating systems with no or limited security, using only default configurations of the operating system or software. They are also the most vulnerable to DDoS attacks. Due to the nature of their applications and the way healthcare is organized, healthcare organizations are considered to be very high-risk targets. Healthcare's security infrastructure is not built to deal with DDoS and IoT attacks, and the security teams usually find it difficult to cope with the complexity of these situations, as they require the cooperation of many different specialists to understand the potential impact of these attacks and to take immediate actions[13,14]. The good news is that as healthcare organizations adopt new technologies and the right security tools, they are now able to reduce the impact of such attacks on their services, as well as the financial, medical, legal and personal data in their systems. Also, they will be able to provide the best possible healthcare to their patients. As healthcare organizations have to make the most of their network bandwidth and staff resources in order to guarantee a reliable quality of service, they need to choose the appropriate tools that will allow them to protect themselves from DDoS attacks and other cyber threats[15].



**2.2. Conduct Account risk assessment:**

It is an overview of the business and operations of a company; risk identification, risk assessment and the business impact analysis. It involves identification of threats, risks, vulnerabilities, controls, compliance and compliance management. Cyber attacks are increasing exponentially and have emerged as an important trend in the cybersecurity industry. Healthcare is not free of the onslaught of such attacks. Simply put, a Conduct Risk Assessment (CRA) is an assessment of the behavior and culture of an individual, group, company, or organization to identify if they may pose a security threat to the organization. A Conduct Risk Assessment helps identify potential security threats, identify and mitigate the security risk of an organization, and develop a remediation plan. Medical records, personally identifiable information (PII), and proprietary patient data are often stored in areas that may be easily accessible to malicious actors. This may be when a laptop is left unattended in a hospital or clinic waiting room, or when a medical device, such as a digital scale, printer, or electronic medical record is left on in an office[16,17].

A security breach may occur during the initial planning, design, and installation of a network, through a malicious insider, outside actor, or through a system glitch. A security breach can often occur before, during, or after a hospital project has been completed. While you may have planned out the right security measures to mitigate the risk of a security breach, hackers may still be able to breach your network with relative ease. Even with robust security measures and a secure operating system, there is always a risk of a security breach. By assessing the business model, identify the types of risks that are generated during the workflow of a healthcare organization. For example, an on-site laboratory is facing risks from data loss in case of unavailability of its IT network[18].

**2.3. Use active directory based user authentication:**

Active directory is an implementation of a Windows Server system, which keeps information about users, computers, and networks in a central place called Active Directory server. As the number of computers and users increase, so does the number of Active Directory related issues. The idea of being able to centrally manage a user accounts on Windows or Mac is awesome and this is the only way a clinician should be managing those accounts. However, it requires a little bit of effort on your part. With the emergence of the internet of things (IoT), the technology of cloud computing, and the increasing use of mobile devices such as tablets and smartphones, more than 90% of enterprises face the challenge of dealing with the security of their network systems[19]. In addition to protecting against computer viruses and ransomware, one of the most serious cyber threats that healthcare organizations must face are security incidents that compromise their network and the integrity of the data stored there[20].

Since a typical healthcare facility includes thousands of networked systems such as electronic medical records, imaging devices, patient monitoring devices, and so on, the healthcare data are vulnerable to data breaches that hackers may use for identity theft, financial fraud, and other illegal activities[18]. According to a research conducted by Trend Micro, the top three data breaches that healthcare organizations are facing are data breaches from employee error, theft, and fraud. In healthcare, the primary sources of security incidents are stolen credentials, insider threats, and improper access to the network systems. In a hospital, an average of 1 in 5 medical professionals or employees have been the source of a data breach that led to the exposure of unencrypted and private data, such as full patient records, that are vulnerable to cyberattacks[21,22].

**2.4. Catalogue the pharmacy's Automated & clinical systems:**

For several years the market has been offering new solutions for the secure communication among healthcare providers, but to be successful they must go through some essential steps: an effective infrastructure, a good relationship with the customers, a good strategy to reach their goals, etc. The success of an EHR depends on its technical features, functionalities and security. First, there are a lot of risks associated with the use of traditional means of transmission, even if the software is protected with the best methods. In fact, there is a greater risk of attack when a patient sends data to a physician that is a risk. For example, many cybercriminals create viruses that transmit from USB drives, or send personal information using emails with an attachment. In addition, it is possible that an attacker uses the security of a company to steal data[23]. Next, security breaches are frequent in electronic data. Even when it is stored and transmitted in an encrypted form, because there are various ways to bypass encryption algorithms. For example, an attacker can use software to automatically change the password used by a user to open the software. Or even if the data is transmitted using a virtual network (such as the Internet), there are risks associated with the implementation of the virtual network, as with other types of attacks. An EHR is the information record for every medical activity, thus, if a security breach occurs, the consequences can be significant. This is why it is imperative to invest in security for EHR software[24].

**DISCUSSION:**

As technology becomes more ubiquitous, it is inevitable that attacks targeting the healthcare system will grow in scale and complexity. As the healthcare community is often the first line of defense for a wide variety of health threats, it is critical that all practitioners, from doctors to pharmacists, understand Cybersecurity and how it pertains to health and the health care system[25]. With the ever-increasing number of Internet of Things devices, Cybersecurity has become a critical component of the field. The purpose of this primer is to provide a general understanding of the concept of cyber risk, and, in particular, how cyber risk (including security, privacy, and data integrity) applies to the practice of pharmacy[26]. Information about cyber security at the pharmacy is also addressed. The purpose of this primer is to provide a general understanding of the concept of

cyber risk, and, in particular, how cyber risk (including security, privacy, and data integrity) applies to the practice of pharmacy. Information about cyber security at the pharmacy is also addressed. The world is getting increasingly connected and there are several advantages that come with that, but these are also some downsides[27]. Some users and systems might be insecure and in that way the risk can also come to the victim of the attack. A hacker who wants to break into a system has to do it in a certain way. First of all, he has to find a way of getting access to it, that's why he uses a computer. Another thing that will make this possible is the software that is used for it[28].

The software is also used to get access to other computers that he has to use to get what he wants. He will then be able to read the computer of the victim, take and change any information that he needs and use it against the victim. There is an increasing need for healthcare organizations to make their facilities and IT systems more secure, to protect patients, clinicians and the company[29]. In this case, IT security has come to be an essential part of the work of the Health-IT security, and therefore IT has also gained credibility among the medical community. The most significant role of the IT security within the healthcare sector has been to protect the patients, and also the companies. IT security plays a crucial role in making sure that the data is safe and is also used securely. As healthcare is evolving, more organizations are realizing the need to protect themselves from cyber-attacks and hacking. They do not want to be taken advantage of. The cyber-attackers can use the healthcare organizations' information to perform financial fraud, or even worse, identity theft. This has led to the creation of a new job category, the IT security manager[30].

The need for Cybersecurity in healthcares industry has been widely identified by industry, academia and security researchers. However, the extent of the problems and needs of healthcares remain unknown and unmet, and also there is lack of a common definition of Cybersecurity in the industry. The field of healthcares has been facing many threats from hackers with malicious intention. These attacks are aimed to steal health data of patients, to manipulate data, destroy devices and services, and to use such health data and manipulated data to threaten patients' health. Such malicious activities of hackers can occur via internal and external mechanisms. Internal attacks are often done through network exploits, data breaches and insider threats[31,32]. Meanwhile, external attacks are carried out on many occasions via cyber-attacks and Internet-based attacks. Healthcare professionals or researchers have defined Cybersecurity in healthcares as "the study of protecting patients' privacy, health information, and healthcare from hacking and cyberattacks". The definition of Cybersecurity in healthcares is widely accepted by industry, academia, and government agencies, and also many of them are trying to develop Cybersecurity solutions for healthcares industry[33].

## CONCLUSION:

The healthcare IT Security landscape has been changing since last decade. At the beginning of this decade, the cyber security professionals were tasked with the role of security management of the IT Infrastructure (both networks and data centers). A well-designed Cybersecurity policy within healthcare is not only essential for the safety of patients and carers, but it can also help to improve the quality of the services provided. However, to fully implement such a policy there needs to be a balance between privacy, data protection, trust and security in healthcare. The key to ensuring the right balance is to look at the security challenges facing healthcare and the technologies that are available to respond. As healthcare systems are increasingly reliant on computer technology, and are also increasingly complex and integrated, the nature of Cybersecurity risk for the industry has changed significantly. It is a multidisciplinary problem, and requires significant multi-jurisdictional collaboration.

Cybersecurity risks need to be identified and addressed, and the main security technologies have the ability to help with this. But there is always more to be learned, and it's important to understand how to address Cybersecurity risks. As technology within healthcare systems is developing, and becoming increasingly important, there is a need to implement policies and procedures to protect against such vulnerabilities. Within healthcare, there are a range of different stakeholders and technologies that can help to protect patient safety. In healthcare, trust is the cornerstone. Trust in healthcare systems and trust in technologies are needed to make certain processes work as intended. When developing a Cybersecurity policy for healthcare, a balance needs to be struck between protecting and maintaining this trust, and also addressing the new risks which are emerging and will become more prominent in the future.

**REFERENCES:**


1. Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. *Biomedical Instrumentation & Technology*, *51*(s6), 19-25.
2. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*(5), 1-9.
3. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52.
4. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.
5. Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4), 556-585.
6. Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, *10*(4), 48-53.
7. Murphy, S. (2015). Is cybersecurity possible in healthcare. *National Cybersecurity Institute Journal*, *1*(3), 49-63.
8. Wells, A. J. (2019). *Cyber-Security Incidents and Organizational Policies in Healthcare* (Doctoral dissertation, Northcentral University).
9. Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of Allied Health*, *48*(2), 148-156.
10. Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Information Processing & Management*, *59*(2), 102888.
11. Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018, May). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 67-73). IEEE.
12. Anastasopoulou, K., Mari, P., Magkanaraki, A., Spanakis, E. G., Merialdo, M., Sakkalis, V., & Magalini, S. (2020, September). Public and private healthcare organisations: A socio-technical model for identifying cybersecurity aspects. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 168-175).
13. Hoffman, S. A. E. (2020). Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure. *World Libraries*, *24*(1).
14. Alami, H., Gagnon, M. P., Ahmed, M. A. A., & Fortin, J. P. (2019). Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. *Health Policy and Technology*, *8*(4), 319-321.
15. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.
16. Busdicker, M., & Upendra, P. (2017). The role of healthcare technology management in facilitating medical device cybersecurity. *Biomedical Instrumentation & Technology*, *51*(s6), 19-25.
17. Caruso, R. J., & Masters, M. (2014). Applying cyber risk management to medical device design. *Biomedical Instrumentation & Technology*, *48*(s1), 32-37.
18. Sheffer, J. (2014). And the Survey Says... AAMI Members Report Top Medical Device Challenges. *Biomedical Instrumentation & Technology*, *48*(5), 341..
19. Yelton, S. J., & Schoener, B. (2020). The evolution of healthcare technology management in leading healthcare delivery organizations. *Biomedical Instrumentation & Technology*, *54*(2), 119-124.
20. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.
21. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making. 2020 Dec;20(1):1-0.
22. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: how safe are we?. Bmj. 2017 Jul 6;358.

23. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021 Jan;21(15):5119.
24. Rajamäki J, Nevmerzhitskaya J, Virág C. Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). In2018 IEEE Global Engineering Education Conference (EDUCON) 2018 Apr 17 (pp. 2042-2046). IEEE.
25. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health security. 2020 Jun 1;18(3):228-31.
26. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health. 2019 May 1;1(1):e10-2.
27. Jarrett MP. Cybersecurity—a serious patient care concern. Jama. 2017 Oct 10;318(14):1319-20.
28. Reagin MJ, Gentry MV. Enterprise cybersecurity: Building a successful defense program. Frontiers of health services management. 2018 Oct 1;35(1):13-22.
29. Williams PA, Cowley S, Bolan C, Fowle K, Staynings R. Working as a Health Cybersecurity Specialist. InThe Health Information Workforce 2021 (pp. 225-236). Springer, Cham.
30. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health. 2019 May 1;1(1):e10-2.
31. Jarrett MP. Cybersecurity—a serious patient care concern. Jama. 2017 Oct 10;318(14):1319-20.
32. Tonge AM, Kasture SS, Chaudhari SR. Cyber security: challenges for society-literature review. IOSR Journal of computer Engineering. 2013 May;2(12):67-75.
33. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices (Auckland, NZ). 2015;8:305.