INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Impact of Cyberethics on Healthcare and Public Health Sector

Institute for Homeland Security

Sam Houston State University

Arabella Moore

Zhou Bing

Abstract. Ethics are evident in all aspects of society, including the technology industry. This leads to the term cyberethics, which includes a special focus on moral dilemmas faced by professionals and society in their interaction with technology. This includes concerns such as data privacy, copyright, freedom of speech versus internet censorship among others. In this paper, we explore three main perspectives of the relationships between cyberethics and the healthcare and public health sector, namely, privacy of health information, usage of social media in the medical filed, and risks of mobile health apps. We will delve into the different aspects of cyberethics within each section and examine how they intersect with the health sector in both positive and negative interactions. Lastly, we will explore various solutions to counteract the negative effects identified. Through this exploration, we aim to contribute to a deeper understanding of the ethical considerations inherent in the intersection of technology and healthcare.

Keywords: Cyberethics, data privacy, healthcare, public health.

1 Introduction and Overview

"Is this morally right?" This kind of question often plagues the minds of many professionals as they integrate their skills and knowledge into society. This is no different for the world of computer science where it is now connected in all society's aspects from the information technologies, the internet and the health systems along with many others. As society becomes more dependent on technology, it becomes easier than ever for society to lose their privacy and security to those with the ability. As a result, many people's personal information and privacy are often compromised, as many professions or industries have the ability depending on their policies and restrictions. This is where ethics comes into play, specifically cyberethics, as it is the key component that forces individuals to review their actions to ensure they are in the public interest, safety, and privacy. Cyberethics is essentially about social responsibility in cyberspace, where there are standards that prescribe morality and immorality in cyberspace, signifying the preservation of freedom of expression, intellectual property, and privacy [1]. While this might sound overwhelming, it simply means that in the world of digital space, there are morals and obligations that those in power within computing science must follow before acting [2].

Cyberethics is a broad term where it can be intertwined with just about anything if it pertains to the digital world. Some of the main principles appearing within this paper are data privacy and security, transparency and accountability, and the ethical use of technology. Within the healthcare and public health sector, many professionals reside and often have a large amount of sensitive information about patients in their computer systems. Information that could be compromised with a single click, either from intruders or from the professionals themselves. Not only this, with society's ability in being able to connect with anyone through various digital platforms, it also raises the questions of ethics in whether this should be allowed. Especially when these facts could be false or could lead to potential harm to oblivious listener. Lastly, one of the fastest growing trends among society is their desire to achieve optimal health which can be done through the help of mobile health apps. However, many of users' personal data recorded by the app are often used without their notice or consent which leads to the ethics of whether it should be allowed.

The main problems this paper presents is the following

1. Security of Patient's Privacy.
2. Usage of Social Media.
3. Mobile Health Apps.

The rest of the paper is organized as follows. Section 2 goes into the problem statement of the three main issues addressed. Section 3 gives in-depth review of the cyberethics challenges in patient's right of privacy and security. Section 4 discusses the possible solutions through supporting cases. Lastly, Section 5 concludes the research with future works provided.

2 Problem Statement

2.1 Importance of Patient's Health Information

Technology has always progressed with the aim of assisting society and professions in completing tasks more effectively. In the healthcare system, technology has been utilized across various domains, including the transition from patients' paper records to digital formats. Patient

medical records hold immense importance as they provide doctors and healthcare sectors with crucial insights into patients' medical history, particularly as patients transition between health professions throughout their lifetime [3]. For instance, doctors frequently refer to patients' medical records when diagnosing illnesses and determining appropriate treatments. Each patient's unique body and illness necessitate careful consideration, especially regarding medication reactions and medical history. Healthcare professionals must ensure that administered medications do not contain ingredients to which patients react poorly. Additionally, updating patients' medical records, whether for vaccinations, heart medications, diabetes treatments, or other updates, is crucial for future healthcare professionals to remain informed about patients' statuses [4]. Given the significance of this information, it's imperative that these records are retrieved and stored properly.

The emergence of EHR in the 1990s revolutionized record-keeping by streamlining retrieval and storage processes. The transition to electronic records was driven by various factors, including the excessive time spent by healthcare professionals searching through millions of paper records, misplacement of key medical information, incomplete records, expensive maintenance, and illegible handwriting, all of which led to incorrect tests and medication administration [5]. Moreover, paper records were time-consuming to update, potentially compromising patient care during future health visits [6]. Consequently, the adoption of EHR became widespread in the healthcare sector, ensuring up to date, reducing medical errors, decreasing cost of records, and readily accessible medical care for patients. Government initiatives, such as the American Recovery and Reinvestment Act of 2009, which allocated over $20 billion to promote electronic medical records, further fueled this transition [7].

However, alongside these changes, policies and principles regarding patient privacy underwent significant transformations. Electronic records, while enhancing accessibility, also heightened concerns about data security and patient privacy. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was one of the pivotal changes enacted in response to this shift [8]. Additionally, the widespread adoption of EHR necessitated the implementation of robust security measures to safeguard patient data from unauthorized access or breaches.

Despite these advancements, concerns surrounding cyberethics have emerged, raising questions about the ethical implications of storing sensitive medical information in digital formats. As technology continues to evolve, it becomes imperative for healthcare institutions to address these ethical considerations and implement comprehensive strategies to protect patient privacy and maintain the integrity of EHR.

2.2 Health Influence within Social Media

Social media refers to the "Internet-based tools that allow individuals and communities to gather and communicate, to share information, ideas, and other content" [19]. According to statista.com, some of the most popular social media platforms of 2024 include Facebook, YouTube, WhatsApp, Instagram, and TikTok. In 2024, there were about 5.04 billion active social media users [20]. With such a broad audience, the sheer number of posts is significant, creating a new way of informing and influencing users. One significant area is the health sector, where individuals with knowledge of health and nutrition can educate others about the importance of health and how to modify their lifestyle for better health. It also provides a platform for people to learn about healthcare or advocate for healthcare agendas [19]. This can be extremely useful for society as it raises awareness of the importance of health and fosters learning from one another, thereby creating a stronger community that encourages others to take control of their health [21]. This trend is evident in the statistics that "in the US, eight in ten internet users search for health information online, and 74% of these people use social media" [19]. Social media enables consumers to access a wealth of resources and knowledge with the tap of a button and at no cost for transportation or medical visits to physicians. Various individuals, such as fitness instructors, healthcare professionals, and average users, utilize social media to inform and influence their community on matters of health. With this new platform, knowledge about health and better ways of living can be easily shared.

Social media platforms can provide “valuable peer, social and emotional support for the general public and patients” as it allows people with similar situations or difficulties to be able to connect with one another [22]. For example, on Facebook, there are many channels where people with diabetes wish to connect with other people who might have tips and

advice on better managing their health. Some of the most popular health influencers active on various platforms include Doctor Mike [23], with over 11 million followers on YouTube, and FootDocDana [24], with nearly 4 million followers on YouTube. Each of these doctors has their own field of interest, with Doctor Mike mainly focusing on daily life and general health, while FootDocDana primarily focuses on Podiatric Medicine (DPM). What they both have in common is a mass following that place invaluable trust in them due to their status as doctors on social media, giving them significant influence over the daily average user and their perception of health. However, they also bear a larger responsibility due to their potential influence. Influencers like these two can share a wealth of useful medical information that could potentially save lives or improve daily life. Nonetheless, despite its positive aspects, social media also has its negatives, such as influencers who may sell fake medicine to desperate users or spread false information about certain aspects of health [25]. While many healthcare workers spread the truth, there are also many spreading false health facts. This sharing of fake health statistics may be harmful to users who trust them for accurate information and guidance on health.

2.3 Problems associated with Mobile Health Apps

Healthcare access, affordability, and quality are issues that many face around the world when it comes to their health and the health care system. To combat this in the modern world, mobile technology serves as a powerful tool with versatile solutions. This is most prevalent in mobile heath apps which are becoming more available each year with more than 5.35 billion mobile users connecting to the internet in a population of 8.08 billion population worldwide in 2024 [38]. As of 2024, roughly 1.98 billion people use their devices for health and care, 1.06 billion users for digital fitness services, and more than 350,000 health available apps with about 250 new apps released daily [38, 39]. With phones being more adapted to the world's daily technology, mobile health apps have also become more popular as its users can now access tools and resources that were unseen before. Various types of health apps can be installed on various devices such as mobile phones or tablets, but they all have the same main function: to allow patients to keep track of their conditions, whether they are physical or mental health-related [40]. With ease and affordability, the use of these health apps has increased

dramatically with millions of downloads of health apps. This can be seen in 2024 with nearly 14 million downloads in January for fitness apps and about 18% of the U.S. adults using heath apps to monitor their health in 2021.

There are two main types of apps that people install for their health. One is health apps that are downloaded for their benefits and tracking of their dependent health. This can range from health apps that encourage and track their physical activities to diet apps that can help them plan their diet to stay on track for better health to apps that are meant for mental therapy. An example of this type of app would be MyFitnessPal which is a popular app on iOS and android that allows users to keep track of their diet and daily exercises in contributions to their physical health. The second main app allows patients to better connect with physicians who can track their conditions more effectively or connect with doctors more efficiently. This can be seen apps such Heal's mobile app for doctor house calls or MediSafe which ensures that patients are able to take prescribe medications in a timely manner by allowing patients the ability to monitor their health with availability and flexibility, it reduces the costs and physical and scheduling difficulties between patients and healthcare specialists [41]. Some apps include diabetes apps such as diabetes-m that help monitor glucose levels, weight, and other personal data while other apps help patients monitor their heart rate for health conditions which then can be sent to the doctors who can easily access their information such KardiaMobile. There are thousands of mobile health apps that users can connect with, and the number of apps will increase over time. With technology and the ease of the internet, people can now easily access a wealth of health resources right from the palm of their hand, empowering them to take control of their well-being like never before. Many of these health apps allow them to build connections with people around the world, encouraging them to better themselves while making them feel connected. However, while technology offers many benefits for people to take control of their health, it does have its drawbacks as personal information is now being exposed as many of these apps often require user's personal information. With this, it creates a security risk to their privacy as their privacy and security could be violated.

3 Problem Discussion

3.1 Unauthorized Access

With medical records mostly in electronic form, new problems arise when it comes to protecting patients and their data. Most of this data is stored in a single large central database that contains millions of patients' medical records, including sensitive information. Through the use of databases, it allows for a better way to collect, process, store, consult, and share health information. Data from the database can be added, updated, or moved around depending on the situation at hand. In order to make these actions, one often needs to gain access to the database and request the necessary changes. This can lead to abuse of the database if the user requesting the records does not have the authority [8].

In cybersecurity, there is a model consisting of three main structures that embody the main principles needed in every system connected by technology called the CIA Triad [9]. The CIA Triad comprises confidentiality, integrity, and availability. This triad model has been modified over time to take into account, which in this case would be authorization and authentication [10]. It can be seen that the authorization branch of cybersecurity is breached when unauthorized users gain access to unauthorized data. For instance, this occurs when doctors or other people view the patient's personal data without proper authority. This raises another question: where does authorization come from? Authorization is derived from consent, where the owner of the specific data would give permission for accessing the data, which in this case is the patient. In the health sector, most patients are often given the right to determine who has the right to view their medical records, and the hospital is obliged to follow this in legal and moral terms [11]. By not following the patient's terms, it breaks the trust between the hospital and its patients, which could lead to a decrease in health for the patients in certain scenarios. There are also ethical boundaries that hospitals break when unauthorized individuals access patient data. Furthermore, breaches in data integrity within the healthcare sector can have profound implications, as tampering with medical records or altering information could lead to misdiagnoses, incorrect treatments, or compromised patient care [12]. Therefore, ensuring the integrity of patient data is paramount to maintaining the quality and reliability of healthcare services.

Additionally, the availability aspect of the CIA Triad is crucial for healthcare systems to provide timely access to accurate patient information for medical professionals when making critical decisions. Any disruptions or downtime in accessing these records due to security breaches can impede patient care and potentially endanger lives. Thus, a comprehensive approach to cybersecurity in healthcare must encompass not only confidentiality, integrity, and availability but also robust authorization and authentication mechanisms to safeguard patient data effectively.

Another significant challenge is the data breach that could be detrimental to the health sector and the patients within it. Since it is a large database, once hackers gain access to the database, they can obtain medical records and data which compromise patients' security and privacy. These stolen data not only contain patients' medical records and information but might also contain their personal profiles such as their gender, phone number, email address, and even social security number depending on the requirements of the health sector. This sensitive data can then be sold to other parties for wrongful usage [13]. For instance, a hacker could gain access to the system and steal a patient's social security number and sell it to third parties. This could lead to security breaches for patients if the third parties use their social security numbers to create a bank account based on their personal profile. All of this ties back to hospitals breaking cyberethics boundaries as they are not protecting patients' privacy and data. Most hospital databases are usually secure and protected as they should be, but there have been several data breaches in modern times. These breaches of a patient's privacy often led to issues with privacy protection and patients' concerns about the security of their data [5]. In a recent conducted survey where participants were asked about their concerns regarding security and privacy, with results showing that "between 54 and 59 percent of respondents expressed a high level of concern" [14]. Many participants, especially disabled or long-term patients, within the research, gave many testimonies where they felt that the hospital often knows everything about them and "has nothing to hide" with the hospital [14]. Another point is that when there is an opening in the sharing distribution system, it also allows weakness in the transition where hackers could obtain the data before it reaches the actual destination. With these main issues, it can be seen that despite the

positive effects of the usage of electronic health records, it brings new issues in patients' security.

3.2 False Information and Disruptions

According to Moorhead et. al., "the main limitation of health information found on social media and other online sources is a lack of quality and reliability" [22]. With social media being an open source for anyone with the right personality and tools, information can often be manipulated to fit the influencer's perspective [26]. Aside from skewed facts, some influencers might also display false information intentionally or unintentionally. Many of these influencers often do not have the knowledge that is on par with someone with a professional degree or years of study. Due to these issues, it can be hard to differentiate between reliable and unreliable platforms or channels. This might cause issues for professionals who encounter many false or misinterpreted pieces of information but cannot do much besides clarifying them. Even then, some people might find it hard to believe a professional if they feel their opinion is more valid based on their own beliefs and interests, even though it might be logically false [27].

There is also the idea that "social media users may also be vulnerable to both hidden and overt conflicts of interest that they may be incapable of interpreting" [19]. The amount of health-related data available is excessive, which is why many medical professionals often take years to study medicine, and some even specialize in a particular health sector. Due to this, the average user on social media may not be able to comprehend or find it difficult to discern the truth or hidden truth when influencers try to push their health agendas. This can lead to followers being loyal to their health influencers even if they are wrong, as some simply do not know the truth behind the excessive number of studies and research that goes into medicine [28]. Another way social media could be misused in the medical field is through the connections between doctors [29]. As doctors progress within their field and the medical field evolves, many medical professionals often connect with one another on social media to learn more about modern medicine or seek advice on how to approach a medical dilemma [29]. However, this could lead to issues of sharing confidential data, which in turn violates their own health ethics codes and laws [30].

3.3 Freedom of Speech versus Censorship

All of this brings up one main challenge when it comes to social media and its usage in the medical field. We are faced with our freedom of speech, where a person is allowed to spread whatever information under the first Amendment, or censorship, where legal actions should be taken when the false spread of information brings harm to society [31]. This also brings into question how this tie into cyberethics. The argument between freedom of speech versus censorship also calls into question doctors' authority and their status in society. Is their opinion and knowledge worth more than an influencer on a platform? How much should they intervene when correcting people's false information? Despite its controversies, not all medical information endorsed by medical professionals is accurate. Authors of medical information found on social media sites are often unknown or identified by limited information [19]. In addition, "the medical information may be unreferenced, incomplete, or informal" [19]. Either way, both the medical and civilian sides can have false medical information, as medicine is a growing field. This then leads to the argument of freedom of speech versus censorship as a general. Since social media has such immense power over its users, "any post, tweet, or shared resource that misinterprets the knowledge of medicine accepted by experts is considered misleading health information" [32]. This misleading information could lead to potential harm to individuals on social media [25]. For example, an influencer might give misleading health advice, such as consuming wrong products, which in turn might hurt individuals. To ensure that no false information is spread, censorship could be placed on social media platforms to ensure only credible, accurate information is displayed. However, this infringes on freedom of speech, which in turn causes more legal, moral, and ethical issues [33]. By limiting freedom of speech, individuals might not be able to connect with others as they did before and share their experiences within the medical field. Additionally, the uniqueness of the human body can lead to different perceptions of the medical field and allow connections with others who have similar abnormalities. Censoring information can also be hard to approach, as it creates new standards that social media must follow. What should be considered medically inaccurate to censor and how much should be censored? This also connects with medical professionals who are connecting with others, as they are exposing sensitive information [30]. Should doctors also be censored to decrease the chance of infringing

patients' rights? However, by doing this, this can cause more dilemmas on the medical profession's side, as some information might be important to the patient's cure. Questions on freedom of speech versus censorship might sound simple, but they have many complex answers depending on the group of people you're asking. The answer to censorship versus freedom of speech is a question that can have various answers depending on the situation, which is why it must be more closely examined before any actions can be taken.

In terms of cyberethics, it ties back to the developers' power of censorship of their social media platforms on their creators. Creators on these platforms are using technology to spread their medical beliefs and therefore might cause harm to individual users [34]. It is within the realm of cyberethics for developers to consider the issues of allowing potentially harmful medical misinformation on their platforms as they must prioritize the well-being and safety of their users. However, censoring information leads to another dilemma, as silencing an individual's opinion also crosses boundaries on ethics. Ultimately, addressing these issues found within the intersection of cyberethics and medical social media platforms requires further research and a deeper understanding of the ethical complexities involved, as well as the development of transparent and inclusive policies that strive to balance the protection of public health with the preservation of freedom of expression.

3.4 Mobile Health App Security

Within most health apps, users are required to input their personal information such as their birthday, age, email, payment information and name among others sensitive data which could poses a threat to their privacy. This is especially true depending on the security of the app, as certain apps have more or less security than others. One of the key weaknesses of many health apps is the fact that many do not encrypt users' personal information, which causes a risk of data security breaches and, in turn, compromises user privacy [42]. Besides the initial login and storage of personal information, mobile health apps continue to store users' personal information as they use it to monitor their health such as their personal daily lifestyle, their medications, and others [43]. Users' personal information is also often at risk, as "sensitive data gathered by

mobile health apps is not only accessible to the patient, physicians, family, scientific research" but also to third parties "such as advertisers" [41]. This puts consumers' privacy and their information at risk, as many of these consumers are often unaware of the outside usage of their online data. Most of these problems stem from the fact that during production, many of these apps do not undergo a process of security and upholding standards to ensure their quality and security is efficient for consumers [41]. Many of these apps do not have a verification process where if the user loses their device, their privacy is now vulnerable to outsiders who may gain access to their personal information [41, 44]. When creating these apps, it is the developer's job to ensure they create a secure app, as one of the conducts of cyberethics is protecting consumers' privacy and ensuring that their products are of the highest standards, which in this regard, fails both. In addition, many health apps do not have a privacy policy, and also do not disclose it to the user upfront which often can lead to consumer confusion on the boundaries and usage of their data. It gives more power to developers on their handling of consumer's personal data.

Another significant problem with mobile health apps is the unencrypted consumer information [43]. Encryption is the process of converting readable data into ciphertext, which cannot be read or understood by a normal user or computer. However, many of these apps often leave consumer data unencrypted, which poses a threat to their security as unencrypted files are accessible by other apps or third parties services or data breaches as "unencrypted files are stored on SD card" which makes it easily accessible [43]. This problem again raises ethical questions about developers not protecting users' data, which could potentially harm them. In a world of cyberethics, creating products that can secure consumers' data and privacy is extremely important, as these data are not the developers' database to manipulate; instead, they are entrusted to keep this data safe. While many of these apps are often free, developers should place a higher standard of consumers' security and privacy risk.

The last issue is the vulnerabilities consumers face when their data is sent to a third party without their notice or consent. Many health apps often send consumers' data to third parties through unencrypted connections without the consumers' consent or notice [45]. This poses a huge security risk, as through unencrypted connections and sending data to third

parties, users' personal data is violated. With data and connections left unencrypted, almost anyone with the right tools can now access it, which violates cyber ethics, as users' information are securely protected [45]. This is turn can cause potential harm to the consumers, leaving them vulnerable to identity theft, alteration of medical, data breaches and many others [41].

The three main topics are only fractions of the challenges constantly faced by mobile health app users. This is especially harmful to those who use health apps to connect with their healthcare providers and monitor their health, as these security risks often violate many health laws and regulations such as the HIPAA, the General Data Regulation (GDR), and the Common Rule [45]. All of these issues pose a huge threat to users' privacy and data, along with their trust in the healthcare system [41]. If users cannot trust the system that is supposed to help them in times of need, it undermines the entire purpose of the healthcare system. Furthermore, the intrusion of users' privacy and data also raises questions of cyberethics regarding the relationship between developers and users. In the digital world where information can be sent anywhere and anytime, it is imperative that there should not only be legal but also moral and ethical boundaries when creating mobile health apps. While health apps are useful in helping consumers connect with each other, reduce costs and travel for health monitoring, and stay encouraged to take control of their health, they create boundaries of unethical scenarios wen developers do not adhere to ethical standards of transparency, accountability, and security in how consumers' data are handled [46]. By not protecting users' security, privacy, and data when they are using their application, it creates an environment of distrust and skepticism among users, undermining the potential benefits of mobile health apps.

Way Forward

3.1 Possible Solutions for Protecting Patient's Privacy

Electronic health record systems (EHRs) are vulnerable to security breaches, posing significant risks to patient privacy and data security.

Robust cybersecurity measures and continuous monitoring to safeguard sensitive medical information are in high demand. Electronic Health Records are often stored in databases, resulting in dire need of security around the database unit and the patient related data. There are several coping strategies that could be used.

4.1.1 Implement Robust Encryption

In the database, the most important metadata needing protection is the patient's medical record and history, which is why robust encryption measures must be implemented to safeguard this sensitive information from unauthorized access or interception. Encryption is important as it helps protect patients' data and increase security by making it unreadable for hackers. Based on recent research, it can be concluded that many public health systems already "encrypt EHR data in order to increase security" [15]. These encryption methods can range from symmetric to public key schemes to store encrypted data. However, one issue resides in the lack of consistency in the type of encryption algorithm and key strength when encrypting the data. When it comes to hospitals and their systems, the security measures can vary as there are many different types of encryption algorithms, including AES, RSA, DES, etc. Each of them is unique in design and strength, though they all aim to provide the same security. Despite the encryption process on the EHRs, they can be broken into, especially when most EHRs are encrypted with either a symmetric key or public key. This creates a weakness as both, while providing protection, are not bulletproof. This can be due to issues in the encryption algorithm's strength, the key's length, or the protection on the key itself. To ensure proper key strength, it must be a certain length to prevent outsiders from brute-forcing or finding the key. So one way to ensure proper security and a decrease in security risk is for hospitals to implement stronger encryption algorithms and longer-length keys. When it comes to the key itself, there should also be better protection on the keys and who should be able to access those data.

Another way to implement robust encryption is by using multiple forms of encryption on the data that will require several forms of key access. One way to do this would be encrypting the patient's record in blockchain on top of the chosen algorithms. Blockchain is the process that "stores data in blocks and forms a hash chain in chronological order

through cryptography and multiparty consensus" [16]. Due to the fact that each block is hashed, it provides security to the patients' data, as with each addition of the block of data, it goes through a process of verification before implementing the encryption algorithm to the node. With this process, it becomes harder for the data to be tampered with, as the data is no longer controlled by a central network; instead, it requires agreement between several parties. Another form of multi-encryption would be having several keys for the data. For example, in order to access the data, one would need a key to access the data but would also need another key to decipher the data. By having several layers of encryption, it provides further protection for the user's data.

4.1.2 Access Control and Authentication

One of the most important aspects when it comes to the relationship of the user's medical record with those who access it would be the access right. Since the medical record belongs to the patient, they have the right to decide who is able to access it or not. Not creating some kind of consensus with the patient violates the patient rights under HIPAA, "patients are entitled to control their own data" [17]. One possible solution would be PCE, also known as patient-controlled encryption, where the patient would use their decryption key to generate subkeys which will allow their delegates to search and access only certain parts of her records [18]. With this process, it will give patients more control and security over their medical records regarding who can access them. PCE, in combination with a strong encryption algorithm, will increase the security of the patient's data.

4.1.3 Regular Security Audits and Penetration Testing

Another way to improve the EHR database is by identifying the vulnerabilities that are causing security breaches. This can be achieved through hospitals conducting self-penetration tests to identify weaknesses. By doing this, hospitals can identify and prioritize vulnerabilities within the EHR database, enabling them to implement targeted security measures and patches to mitigate potential risks and enhance the overall security posture of the system.

4.2 Possible Solutions for Social Media Censorship

In various studies conducted by researchers, the prevalence of misinformation regarding medical knowledge on social media platforms underscores the urgent need to address this pressing issue. One notable case study is the battle against COVID-19, where the influence of the medical field and social media platforms on average citizens became evident. This occurred at a time when trust between the medical field and citizens was low, given the novelty and unpredictability of the COVID-19 virus, which still required further study. However, the medical field was on time limit and therefore could do with the resources available. Consequently, many individuals on social media during this time were false [35]. False information spread rapidly, leading to the coining of the term "infodemic" during the pandemic in "regard to the poor and uncontrolled dissemination of information related to the COVID-19 pandemic" [36]. These instances of false information spreading on social media platforms and their effects demonstrate their significant influence on society if left unaddressed.

4.2.1 Implement Content Moderation Tools

One of the easiest ways to prevent the false spread of health information is through the usage of content moderation tools, which can take down content that violates the guidelines set by the developers. Content Moderation Tools have always been present and became extremely popular after the development of the internet. According to MacKenzie F. Common, there are "three distinct stages: Creation, Enforcement, and Response" [37]. Creation involves the terms and conditions that content must not violate in order to be viewed. Enforcement is the decision-making section where actions are decided for violating the bylaws, and the response section deals with the aftermath of violating the bylaws. When these three phases work together, they essentially become the rule enforcer of the internet since the online world is a separate realm from the physical world and therefore requires different rules for efficiency. However, platforms such as YouTube, Twitter, and others often mainly use content moderation to block controversial topics such as suicide, graphic images like mutilated death or sex, politics, abortion, and many others. In terms of health-related content, there's not much moderation. This is especially true during this time period when there is a rise in the desire for better health, which has led to an influx of health content,

promoting various knowledge and views on the definition of optimal health, even though many are false, leading to possible negative effects. To prevent this, content moderation tools run on the flags/protocols that the developer sets to ensure that the content doesn't trigger the system.

4.2.2 Collaborate with Fact-Checking Organizations

Another way to ensure that the health data being spread is accurate is by collaborating with different well-established organizations to access the most updated and accurate knowledge on a topic. Social media encompasses various platforms with their own systems and terms and conditions that users must abide by. If they want to monitor the spread of health knowledge, then they must ensure their own knowledge is accurate. However, it takes a lot of time and resources to collect all the updated and accurate medical knowledge, especially as it continues to evolve over time. By working with a third-party organization such as the International Association for Healthcare Security & Safety, who can provide them with proper data and help them monitor content, social media platforms can ensure that users are only receiving accurate medical information and advice. With the proper content moderation tools and knowledge, developers of social media would be able to maintain the spread of medical knowledge.

4.2.3 Secure Communication Channels

Healthcare professionals are always learning, as the medical field is forever growing, making it hard for them to know everything. The medical field is a tricky one where finding the proper answer can be difficult. One of the best ways for health professionals to learn is by seeking advice from other health professionals, which is why they often communicate with each other through the internet, forums, messages, chats, and social media. However, they can often accidentally leak out their patients' private information, which can then be extracted by outsiders. Besides practicing proper withholding of information when discussing sensitive information, there should also be secure communication channels between everyone. Implementing secure communication channels is crucial to ensure that sensitive patient information remains protected during online interactions among healthcare professionals. These channels should utilize encryption

protocols to safeguard data in transit and authenticate users to prevent unauthorized access. Additionally, access controls and role-based permissions should be implemented to restrict access to sensitive information based on the user's role and level of authorization. Regular training and awareness programs should also be provided to educate healthcare professionals about the importance of using secure communication channels and best practices for protecting patient privacy online. By prioritizing the implementation of secure communication channels, healthcare organizations can facilitate effective collaboration among healthcare professionals while safeguarding patient confidentiality and complying with regulatory requirements.

4.3 Possible Solutions for Reducing Mobile Health App Risks

In a study conducted by Adhikari et. al., [41], the authors analyzed 20 mobile health apps to determine the app risk score and safe score breaking each app down to its section of registration, cloud storage, third part, authentication, update profile, complete delete, local data, security explained and privacy policy. Along with their research, they also created a visual graph, providing a better representation of the security of most health apps. Within the study, they found that most health apps pose significant risks to consumers' privacy, data, and personal information. Among the 20 mobile health apps analyzed, only 5% allowed users to delete their data completely, only two apps asked for consumers' authentication prior to log-in to the apps, and about 65% transmitted consumers' data to third parties or advertisers. All of these findings in the study emphasize the lack of security surrounding users' data and the extent to which their data is being transferred without their knowledge or consent in most cases. Through this study, it is evident that despite apps storing consumers' data, there are very few security measures in place to protect their data, leaving much of it exposed to the public. This small pool of research is an only small representation of the thousands of other mobile health apps available for download. In calculation, the number of apps that pose threats to user’s data, privacy, and security is immense as seen in this study.

4.3.1 Data Encryption

Mobile health apps are crucial and have a significant impact on those utilizing them for monitoring and improving their health. However, many of these apps often provide minimal protection to their users, especially regarding their data. One of the largest issues, as stated in Section 3, is the surprising amount of unencrypted data that puts the user's privacy and security in jeopardy. From this observation, it can be seen that encryption is heavily needed in most mobile health apps. There are many different types of encryption algorithms mobile health apps could implement, such as AES, RSA, DES, Blowfish, and many others, though AES or RSA is often recommended. By implementing robust encryption algorithms such as AES or RSA, mobile health apps can significantly reduce the risk of unauthorized access to sensitive user data and security breaches.

4.3.2 Data Minimization

Another way to prevent leakage of users' personal data would be through data minimization, where the mobile health app stores only relevant data and discards any unnecessary information. By adopting a data minimization approach, mobile health apps can significantly reduce the amount of personal data stored within their systems, thereby minimizing the risk of data leakage and unauthorized access. This involves implementing strict data retention policies and only collecting the minimum amount of information necessary for the app's functionality and user experience. For example, instead of storing an extensive amount of user data such as their name, address, or contact information, the app could focus on gathering only essential health information or specific user preferences relevant to the intended purpose of the application. Additionally, any unnecessary or outdated data should be promptly and securely discarded to further mitigate the risk of data exposure. By adhering to the principles of data minimization, mobile health apps not only enhance user privacy but also streamline data management processes and reduce potential regulatory compliance burdens. It's essential for app developers to strike a balance between data minimization and providing valuable insights and services to users, ensuring that the app remains functional and effective while respecting user privacy rights.

4.3.3 User Consent & Transparency

In mobile health, user consent and transparency are extremely important, as most users often do not know what the apps keep on them and their actions when it comes to their data. This can lead to issues like selling their data to third-party organizations without their consent. However, it's the user's right to know how their data is being collected, stored, and used within the app's system. Transparency regarding data practices is essential for building trust and maintaining user confidence in the platform. Mobile health apps should provide clear and easily accessible privacy policies that outline the types of data collected, the purposes for which it is used, and any third parties with whom it may be shared. Additionally, obtaining explicit consent from users before collecting or sharing their personal data is paramount. This consent should be informed, meaning that users fully understand the implications of their data-sharing decisions. Furthermore, mobile health apps should offer users granular control over their data preferences, allowing them to opt-in or opt-out of specific data collection activities and providing mechanisms for users to review, update, or delete their data as needed. By prioritizing user consent and transparency, mobile health apps can empower users to make informed choices about their privacy and ensure that their data is handled responsibly and ethically.

5. Conclusion

In this paper, we explored the three main aspects of cyberethics within the healthcare and public health sector. From hospitals to social media influence on health, to the effects of various mobile health apps, we examined the positive and negative impacts of each. As seen through the research, it can be concluded that some of the biggest issues arising from the health sector in connection to cyberethics are patient and user data privacy and security, personal data, and potential false information through the usage of technology. By identifying these vulnerabilities, which have the potential to cause harm to average citizens and patients, we also explored various solutions to counter the negative impacts, allowing users to continue to rely on the usage of technology for the benefit of their health.

As time goes on, technology will continue to improve and become more integrated into people's daily lives. In light of this, the ethical boundaries

between users' privacy and security become more of a concern as they are now more exposed to their digital world. With technological improvements, it's crucial to conduct more studies and emphasize the importance of security and privacy knowledge among professionals, companies, and industries handling sensitive data. This is essential to prevent potential harm to users if their data is mishandled or stolen.

References

[1] H. Ki and S. Ahn, A Study on the Methodology of Information Ethics Education in Youth. International Journal of Computer Science and Network Security, vol. 6, no. 6, pp. 91-100, 2006.

[2] Ramadhan, Arief, Dana Indra Sensuse, and Aniati Murni Arymurthy. E-government ethics: a synergy of computer ethics, information ethics, and cyber ethics. International Journal of Advanced Computer Science and Applications, 2011.

[3] Mishra, A. N., Anderson, C., Angst, C. M., & Agarwal, R. (2012). Electronic health records assimilation and physician identity evolution: An identity theory perspective. Information Systems Research, 23(3-part-1), 738-760.

[4] Ayatollahi, H., Mirani, N., & Haghani, H. (2014). Electronic health records: what are the most important barriers?. Perspectives in health information management.

[5] Malhotra, N., & Lassiter, M. (2014). The coming age of electronic medical records: From paper to electronic. International Journal of Management & Information Systems (IJMIS), 18(2), 117-122.

[6] Joukes, E., Abu-Hanna, A., Cornet, R., & de Keizer, N. F. (2018). Time spent on dedicated patient care and documentation tasks before and after the introduction of a structured and standardized electronic health record. Applied clinical informatics, 9(01), 046-053.

[7] DesRoches, C. M., Campbell, E. G., Vogeli, C., Zheng, J., Rao, S. R., Shields, A. E., Jha, A. K. (2010). Electronic health records' limited successes suggest more targeted uses. Health affairs, 29(4), 639-646.

[8] Richards, M. M. (2009). Electronic medical records: Confidentiality issues in the time of HIPAA. Professional Psychology: Research and Practice, 40(6), 550.

[9] Osop, H., & Sahama, T. (2016). Quality evidence, quality decisions: ways to improve security and privacy of EHR systems. In 2016 IEEE

18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6).

[10] Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020). Executive Summary — NIST SP 1800-26 documentation. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html.

[11] Jin, J., Ahn, G. J., Hu, H., Covington, M. J., & Zhang, X. (2009). Patient-centric authorization framework for sharing electronic health records. In Proceedings of the 14th ACM symposium on Access control models and technologies (pp. 125-134).

[12] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3), 1-44.

[13] S. M. Shah and R. A. Khan, "Secondary Use of Electronic Health Record: Opportunities and Challenges," in IEEE Access, vol. 8, pp. 136947-136965, 2020, doi: 10.1109/ACCESS.2020.3011099.

[14] Lafky DB, Horan TA. Personal health records: Consumer attitudes toward privacy and security of their personal health information. Health Informatics Journal. 2011;17(1):63-71. doi:10.1177/1460458211399403.

[15] Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inform. 2013 Jun;46(3):541-62. doi: 10.1016/j.jbi.2012.12.003.

[16] Li H, Yang X, Wang H, Wei W, Xue W. A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme. J Healthc Eng. 2022 Mar 4;2022:2058497. doi: 10.1155/2022/2058497.

[17] Eom SJ, Lee J. Digital government transformation in turbulent times: Responses, challenges, and future direction. Gov Inf Q. 2022 Apr;39(2):101690. doi: 10.1016/j.giq.2022.101690.

[18] Josh Benaloh, Melissa Chase, Eric Horvitz, Kristin E. Lauter: Patient controlled encryption: ensuring privacy of electronic medical records. CCSW 2009: 103-114.

[19] Ventola, C. Lee. Social media and health care professionals: benefits, risks, and best practices. Pharmacy and therapeutics 39.7 (2014): 491.

[20] http:// Dataportal.com.

[21] Lambert KM, Barry P, Stokes G. Risk management and legal issues with the use of social media in the healthcare setting. J Healthc Risk Manag. 2012;31(4):41-7. doi: 10.1002/jhrm.20103.

[22] Moorhead, S. A., Hazlett, D. E., Harrison, L., Carroll, J. K., Irwin, A., & Hoving, C. (2013). A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication. Journal of medical Internet research, 15(4), e85. https://doi.org/10.2196/jmir.1933.

[23] http://Doctormikemedia.com.

[24] http:// FoodDoctDana.com.

[25] Almomani, H., Patel, N., & Donyai, P. (2023). Reasons that lead people to end up buying fake medicines on the internet: qualitative interview study. JMIR Formative Research, 7(1), e42887.

[26] Singh, J., Crisafulli, B., & Xue, M. T. (2020). 'To trust or not to trust': The impact of social media influencers on the reputation of corporate brands in crisis. Journal of Business Research, 119, 464-480.

[27] Wei, J., & Meng, F. (2021). How opinion distortion appears in super-influencer dominated social network. Future Generation Computer Systems, 115, 542-552.

[28] Jun, S., & Yi, J. (2020). What makes followers loyal? The role of influencer interactivity in building influencer brand equity. Journal of Product & Brand Management, 29(6), 803-814.

[29] Muhlen, M., & Ohno-Machado, L. (2012). Reviewing social media use by clinicians. Journal of the American Medical Informatics Association : JAMIA, 19(5), 777–781. https://doi.org/10.1136/amiajnl-2012-000990.

[30] George, D. R., Rovniak, L. S., & Kraschnewski, J. L. (2013). Dangers and opportunities for social media in medicine. Clinical obstetrics and gynecology, 56(3), 453–462. https://doi.org/10.1097/GRF.0b013e318297dc38.

[31] Wu, T. (2019). Is the first amendment obsolete?. In The perilous public square: Structural threats to free expression today (pp. 15-61). Columbia University Press.

[32] Darwish, Omar, et al. "A survey of uncover misleading and cyberbullying on social media for public health." Cluster computing 26.3 (2023): 1709-1735.

[33] Slutskiy, P. (2020). Freedom of expression, social media censorship, and property rights. Blanquerna School of Communication and International Relations, (48), 53-67.

[34] Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic literature review on the spread of health-related misinformation on social media. Social science & medicine, 240, 112552.

[35] Khamis, R. M., & Geng, Y. (2021). Social media usage in health communication and its implications on public health security: A case study of COVID-19 in Zanzibar. Online Journal of Communication and Media Technologies, 11(1), e202101.

[36] Corinti, F., Pontillo, D., & Giansanti, D. (2022, April). COVID-19 and the infodemic: An overview of the role and impact of social media, the evolution of medical knowledge, and emerging problems. In Healthcare (Vol. 10, No. 4, p. 732). MDPI.

[37] Common, MacKenzie F. (2020) Rule of law and human rights issues in social media content moderation. PhD thesis, London School of Economics and Political Science.
[38] S. Kemp, “Digital 2024: Global overview report,” DataReportal – Global Digital Insights, Jan. 31, 2024. https://datareportal.com/reports/digital-2024-global-overview-report (accessed Mar. 11, 2024).

[39] R. Hall, “Health Apps: How Mobile Apps Are Improving Our Lives & Well Being,” MindSea Development, May 23, 2019. https://mindsea.com/health-apps/ (accessed Mar. 12, 2024).

[40] L Zhou, J Bao, IMA Setiawan, A Saptono, B Parmanto. The mHealth app usability questionnaire (MAUQ): development and validation study - JMIR mHealth and uHealth, 2019.

[41] Adhikari, R., Richards, D., & Scott, K. (2014). Security and privacy issues related to the use of mobile health apps. ACIS.

[42] McCarthy, Michael. "Experts warn on data security in health and fitness apps." BMJ: British Medical Journal (Online) 347 (2013).

[43] Sampat, B. H., & Prabhakar, B. (2017). Privacy risks and security threats in mHealth apps. Journal of International Technology and Information Management, 26(4), 126-153.

[44] Hadi Kharrazi, Robin Chisholm, Dean VanNasdale, Benjamin Thompson, ‘Mobile personal health records: An evaluation of features and functionality, International Journal of Medical Informatics’, Volume 81, Issue 9, 2012, Pages 579-593, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2012.04.007.

[45] Rezaee, R., Khashayar, M., Saeedinezhad, S., Nasiri, M., & Zare, S. (2023). Critical Criteria and Countermeasures for Mobile Health Developers to Ensure Mobile Health Privacy and Security: Mixed Methods Study. JMIR mHealth and uHealth, 11, e39055. https://doi.org/10.2196/39055.

[46] Grundy, Q. (2022). A review of the quality and impact of mobile health apps. Annual review of public health, 43, 117-134.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Moore, Arabella & Bing, Zhou (2024) The Impact of Cyberethics on Healthcare and Public Health Sector. (Report No. IHS/CR-2024-1024). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/MYPC6