IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cybersecurity Challenges in Telehealth Services: Addressing the security vulnerabilities and solutions in the expanding field of telehealth

VENKATESWARANAIDU KOLLURI

Sr. Software Engineer, Department of Information Technology

ABSTRACT—This paper explores the current types of telehealth systems in use, the unique security challenges faced, the impacts of security breaches, and methods to mitigate security threats in order to provide greater patient safety and data integrity. Despite being around for three decades, telehealth has recently gained considerable popularity and acceptance due to the rising cost of healthcare and the increasing demand for home-based care. However, the rapid advancement of technology has outpaced the development of necessary policies and standards to ensure the utmost security and privacy of both patients and providers [1]. Thus, the healthcare reform implemented is expected to further drive the significant growth of telehealth in the coming years.The analysis unequivocally highlights the groundbreaking and transformative potential of telehealth in enhancing access to care and improving patient outcomes. The immense value that telehealth brings to the table cannot be overstated. By addressing the existing challenges, capitalizing on emerging opportunities, and adopting a patient-centered approach, telehealth has the power to revolutionize the field of healthcare on a global scale. Therefore, all stakeholders, including healthcare providers, policymakers, researchers, and technology developers, are strongly encouraged to remain adaptable, innovative, and proactive[1]. It is only through their collective efforts that the full potential of telehealth can be unlocked, leading to a future where accessible and high-quality healthcare is available to all individuals, regardless of their geographical location or socio-economic status. The advancement of technology in this sector has further enhanced the capabilities of remote healthcare services but has also increased security risks due to the large amount of personal and health information stored on electronic systems. Adherence to system safety, security, integrity, confidentiality, and patient safety is a crucial goal and challenge in this rapidly evolving field.

Keywords— Telehealth, telemedicine, cyber security, challenges, Healthcare, vulnerabilities, innovation, technology, automation, clinicians, analytics, HIPAA.

I. INTRODUCTION

With the advancement of technology in the contemporary world, it has become so convenient for individuals across the globe to go online to communicate with others, manage bank accounts, pay bills, purchase items, and perform countless other tasks. Although the ability to perform these tasks virtually has made things much more convenient, it has also opened a window of opportunities for malicious computer hackers to employ a series of technologically advanced methods to access personal data recorded within organizational databases. This, in turn, has created an increased threat to information security[3,4]. Telemedicine is the application of electronic communication between a patient and a doctor, by doing this they could get care and consultation without visiting a health-care facility. One of the services of telemedicine is tele-psychiatry, a form of telemedicine which guarantees a consultation for psychiatric needs of a person by using several forms of communication such as phone, text, video call and others. The spread of the pandemic forces psychiatrists to avoid face-to-face consultation, this makes the demand for telepsychiatry keep growing. Although tele-psychiatry is an effective way to prevent and have a consultation, it could not be separated from a cyber-security threat [4]. Tele-psychiatry service usually uses a messaging or video call app, this messaging or video call has a possibility to be intercepted by irresponsible parties. These intercepted conversations could be used in an irresponsible way and it could harm the patient and the psychiatrist.

Telemedicine or remote healthcare is the provision of clinical health services and education by means of electronic information and telecommunications technologies from a distance. It covers a wide variety of areas such as telemedicine where patients can go to their doctor online, monitoring their health remotely, tele-consults, etc. Telehealth has significantly changed the shape of healthcare by increasing access to care, enhancing patient outcomes, and increasing efficiency in healthcare supply. Telehealth implementation did indeed revolutionize the way patients are treated by healthcare providers. The use of most advanced technologies, including cloud data storage and advanced software systems, can facilitate in providing quality healthcare services even at remote areas. On the one hand, these technologies are both very beneficial to us, however, online security risks are also the price of usage of the systems. Security breaches over cyberspace pose a great danger to telehealth services and may cause more damages than physical attacks. The weaknesses of cloud data storage and software systems make them an attractive target for cyber criminals who wish to steal sensitive patient information. These consequences can be serious, ranging from legal repercussions, identity thefts, to loss of intellectual property. Moreover, data of telehealth patients can

be easily exposed to unauthorized users if service providers don't take proper measures to protect them.

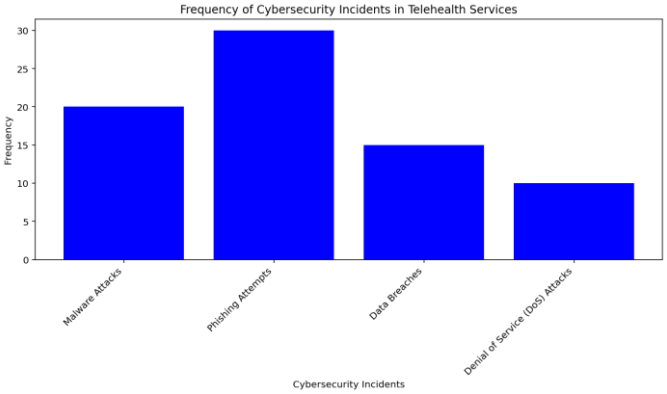

Fig. 1 Cybersecurity Incidents in Telehealth Services

Implementing a comprehensive cybersecurity strategy is crucial to safeguarding telehealth services and protecting patient data. It is not enough to simply install a firewall and consider the job done. Cybersecurity is an ongoing operation that requires constant vigilance and maintenance. Regular preventive measures must be taken to identify and address vulnerabilities before they are exploited by malicious actors. It is essential to stay updated with the latest cybersecurity practices and technologies to effectively safeguard telehealth systems[7]. Furthermore, data backups play a crucial role in ensuring the integrity and availability of patient data. Regular backups should be performed to mitigate the potential damage of data corruption or loss. By having up-to-date copies of patient data, healthcare providers can quickly recover and restore information in the event of an unforeseen incident. This significantly reduces the risk of incorrect treatment due to compromised or missing data.

Investing in the right people and providing adequate training for cybersecurity is of paramount importance. Skilled security staff who possess an intricate understanding of telehealth systems are essential in identifying and mitigating risks effectively. In some cases, security consultants may need to be employed to provide specialized expertise. Furthermore, the adoption of security software and practices such as regular data encryption is vital to ensuring data protection[1]. Encryption serves as a safeguard during the transmission of patient data between telehealth systems. By converting plaintext data into ciphertext using complex algorithms and encryption keys, the information becomes unreadable to unauthorized individuals. This is particularly important when patient data is transmitted over open networks, minimizing the risk of interception and unauthorized access.

II. RESEARCH PROBLEM

The main research problem addressed in this review is the issue of information security which must be considered in the implementation of telehealth services. While cybersecurity may appear daunting, the consequences of failing to protect patient data can be severe. A data breach not only compromises the privacy and well-being of patients but also poses a considerable financial and reputational risk to healthcare providers. It is critical that telehealth accommodate the degree of confidentiality of the patient's data by taking full measures to prevent breaches and online security challenges[7]. Telehealth is the application of telecommunications and information technology for the delivery of healthcare services remotely. This involves the exchange of medical information from one site to another through electronic communications to improve patients' health status. The exchange can occur in real-time, such as with a phone call or computer online chat, or through a delayed way, such as email between provider and patient.Regular audits and risk assessments of telehealth systems are crucial measures in identifying potential vulnerabilities and enhancing cybersecurity measures. By proactively evaluating the security gaps within the system, healthcare providers can implement appropriate controls and safeguards to prevent cybersecurity breaches. With telehealth, a medical professional can evaluate, diagnose, and treat patients without the need for an in-person visit[8]. This is quite useful in providing convenience for both the patient and the healthcare provider. Due to the nature of telehealth, it generally involves transmitting sensitive medical information and is often meant to reach patients located in rural areas or those who are in underprivileged communities. Given the nature of cyber attacks and the increased vulnerability of data traveling through cyberspace, telehealth services open an increased window for potential cybersecurity breaches. This will be a serious issue if telehealth is to be implemented to improve and provide the best possible healthcare on a global scale.

III. LITERATURE REVIEW

A. TELEHEALTH

It is evident that healthcare provision is reliant on the management and processing of information, and thus there is a need to safeguard the confidentiality and integrity of patient information. The most direct and significant threat to the privacy of a patient's personal health information is unauthorized access or disclosure. Movement of health data between stakeholders, whether it be at a local, national, or global level, increases the risk of privacy violations and requires effective security measures to reduce such risks. Data privacy concerns are one of the more prominent deterrents within the healthcare industry in adopting telehealth services.

Telehealth has been encouraged and facilitated as an important and feasible means to increase access to healthcare services nationwide. The potential cost savings of telehealth in terms of travel costs, time off from work, and the ability to monitor chronic conditions may be reflected in the economic viability of telehealth. Accessibility to healthcare services and record keeping are severe issues for remote or rural areas[9]. Telehealth can provide methods to improve public health by increasing the outreach to those who may otherwise not receive sufficient medical attention. Some examples of this include the widespread use of mobile phones and the internet to communicate with patients and the application of telemedicine to connect specialists with general practitioners in an effort to improve treatment.

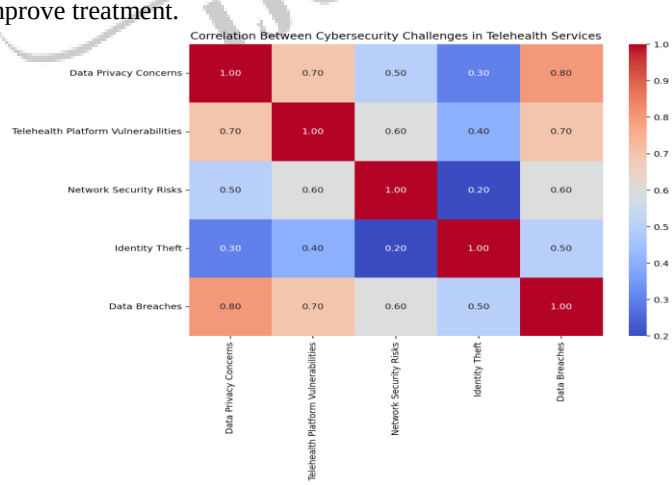

Fig. 2 Correlation Between Cybersecurity Challenges in Telehealth Services

B. TELEHEALTH ADOPTION

In the past, telehealth was utilized to connect rural individuals to healthcare services, as well as for conferencing between medical professionals. These traditional applications of telehealth were implemented through private networks for the most part. The recent emergence of the internet has led to a new generation of telehealth. New telehealth services are now interactive, involving real-time two-way communication

between patients and HCPs as well as video-conferencing between HCPs[9,10]. These services are provided by commercial vendors, but also directly to patients by healthcare providers. In the wake of the COVID-19 pandemic, there has been a large surge in direct-to-consumer telehealth services, as it complies with social distancing and reduces the risk of virus exposure. While these changes in healthcare provision have clear benefits, there are also some notable downsides, with one of the most pressing being the security of patient information. Given that telehealth is reliant on the processing and transmission of health information, often of a sensitive nature, it is crucial that we identify and mitigate the cybersecurity challenges it faces[10]. Failure to do so will compromise the privacy and integrity of patient information, and in turn, public trust in telehealth and the quality of care it provides.

C. DATA PRIVACY CONCERNS

One of the recent steps to prevent unauthorized access to PHI is a push for encryption of all data. Encryption is the process of encoding data such that only authorized parties can access it. In the case of intercepted data, encryption renders the data useless to unauthorized parties as they would be unable to decode and read the information. Encryption is currently a standard practice in e-commerce and is said to be the most effective security safeguard in all types of security. The US government has caught on to this and there is now a huge push for widespread encryption of all PHI[10]. The Health Insurance Portability and Accessibility Act (HIPAA) has deemed 2015 as the target date for all patient medical records and physician communications to be converted to the electronic format. This act has created an unprecedented demand for encryption technologies in order to secure the massive amount of electronic PHI. While encryption is a savior to data security, it is not without its own issues. The biggest concern is key management, as a loss of keys can mean a loss of access to data. This can be a major issue with older data and system upgrades. Another issue is the use of cloud storage for PHI. In this case, third-party vendors are responsible for storing the encrypted data. While it may seem safe, recent events have shown that cloud storage is a prime target for hackers. A great example is the recent breach in Apple's iCloud where unauthorized access to celebrity photos was obtained[10]. This event created skepticism over the safety of the cloud, and it is clear that rigorous encryption is only the first step in securing PHI stored with cloud third-party vendors.

The issue of data privacy concerns is intrinsically tied to personal health information (PHI). PHI is defined as information about health status, or healthcare that is personally identifiable. Although this may seem straightforward, the definition can be quite complex especially in telehealth and other technology-based healthcare services[12]. In order for telehealth to be a viable alternative to in-person healthcare, PHI must be recorded and stored electronically. This creates a new realm of privacy concerns, as data that was once stored in locked file cabinets now can be potentially accessed from around the world. The internet and various databases have revolutionized the availability and flow of information. While this may be seen as a benefit to accessibility to information, it poses a substantial increase in the risk of unauthorized access to PHI. In a study by Doherty and Fulcher, data security was rated as a key concern by telehealth practitioners. This concern was highlighted by an incident in the UK where a provider was ordered to stop using email to send appointment reminders to patients because it potentially violated data protection laws. This type of scenario has become all too common as hackers have shown that they can easily infiltrate standard email and obtain unencrypted PHI[13].

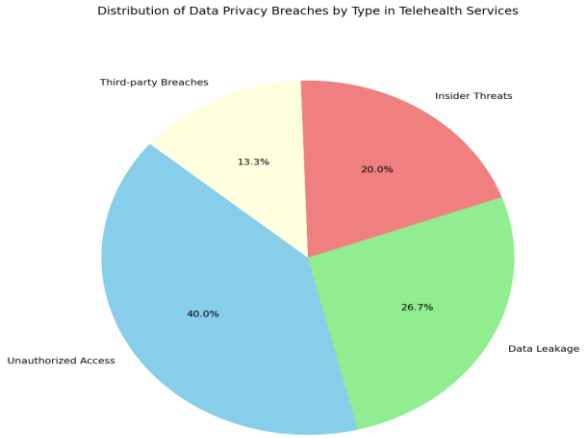

Fig. 3 Distribution of Data Privacy Breaches by Type in Telehealth Services

D. AUTHENTICATION AND ACCESS CONTROL

Authentication techniques are deemed as a first line of defense against potential security threats as it will ensure that only legitimate system users will have access to the system. It is crucial to have strict access control on healthcare information as leaking of sensitive data can damage the reputation of the patient, as well as the providers involved. The most basic form of authentication would be user IDs and passwords. However, the assumption of modern technology claims that it is unreliable as it can be easily forgotten, stolen, guessed, and can be misused by others[13,14]. A single security breach can put an organization and its clients at risk of identity theft. Hence, stronger forms of authentication such as smart cards, biometric systems and digital certificates are recommended for guaranteeing the proper identification of an individual before access to specific information is allowed. In consideration of the cost of these authentication methods, the value of the healthcare information being protected should be weighed against the cost of the authentication solution and the potential loss if the information is compromised[14]. The decision of which level of authentication is implemented will be heavily dependent on this comparison.

E. SECURE COMMUNICATION CHANNELS

Telehealth has the potential to make healthcare more convenient and efficient, especially considering the growing population of the elderly and limited healthcare workforce. However, the ability of patients to engage with the healthcare system from remote locations presents privacy concerns with respect to the transmission of personal health information over the internet. Security for telehealth systems is a critical requirement, and an area that has not received the attention it deserves. User authentication and access control mechanisms have been the focus of several studies[15]. These are important for ensuring that data is accessed only by authorized individuals. However, there are many different ways that data can be communicated between healthcare providers and the patient, and potentially between different members of the care team. Each of these communication methods has different security implications, particularly with respect to encryption, but this is an area that has received little attention in the telehealth literature to date. The wide variety of technologies and terminologies used in telehealth make understanding the security risks associated with each a difficult task[15]. An example is a recent study on the potential use of mobile phone messaging applications for telehealth. While it found that this technology has great potential in resource-poor settings, little consideration is given to the potential risks of using widely available messaging platforms that were not designed with security as a primary concern.

F. VULNERABILITY ASSESSMENTS

Another benefit of vulnerability assessments is that it provides an objective basis for comparing security. It is more cost-effective to test the telehealth system for vulnerabilities than it is to become aware of security problems through an actual security breach. If a vulnerability assessment is done correctly, it will save an organization money in the long run by identifying problems early on. This means that at present time, it will also heighten the protection of client data. Security breaches often occur because the security measures are able to be bypassed by hackers. The client's trust in services is thus maintained if their data is kept safe[16]. The work conducted by the assessors will result in documentation detailing issues with the telehealth system, providing guidance on how to best address the issues to increase security. There are several reasons as to why vulnerability assessments are important for telehealth services. Firstly, vulnerability assessments assess for weaknesses in the telehealth system that, if not fixed, can lead to security breaches resulting in damage to the organization. It also assists in reducing the possibility of a data breach. Data breaches can be costly and devastating to an organization. It examines security weaknesses in the information system that could be exploited to the detriment of the information resources[16]. Vulnerability assessment is an important step in ensuring that the telehealth services provided are secure from any security breaches and maintaining client trust in the services offered. It is used to identify, quantify, and prioritize the vulnerabilities in a system. The assessment provides a base on which to build a strong security program. The results of the assessment allow an organization to see the vulnerabilities in their system, and then take the proper measures to fix the vulnerabilities.

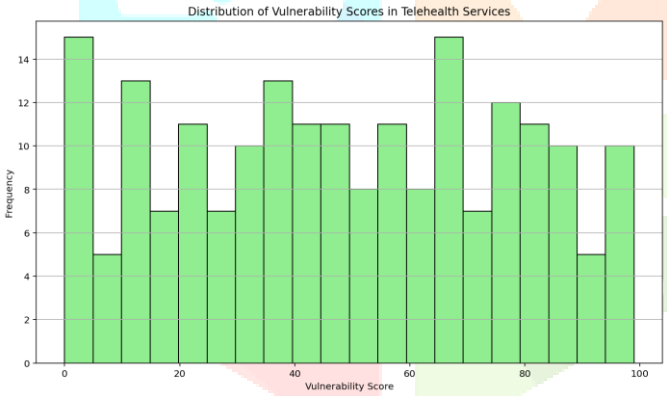

Fig. 4 Distribution of Vulnerability Scores in Telehealth Services

G. REGULATORY COMPLIANCE

Unfortunately, even with the best intentions, the laws regarding technology used in healthcare are often muddy and ill-defined, and sometimes apply only to certain states or locales. Johnstone et al. noted the significant lag time in legal and regulatory information as compared to the fast pace of technological development, and that confusion is echoed by Whitten and Price, who state that the dispersed nature of telehealth regulation could prove to be a major barrier for telehealth utilization. In a study of telepsychiatry, which has its own set of regulations apart from the general telehealth umbrella, Shore et al. found that many participants were unaware of existing regulations and instead relied on their own judgment to determine what was appropriate practice[17]. This demonstrated lack of awareness can be dangerous and potentially damaging, so it is necessary for telehealth practitioners to be proactive in seeking out up to date information on regulations and translating that into clear policies and practices for their organization. Essentially, the ideal is to have regulations that are telehealth-specific, clearly defined, and consistent across different regions and states.

Regulatory compliance involves the actions taken by an organization to abide by established laws, regulations, standards, and guidelines relevant to its operations. Those in telehealth must be aware that in addition to U.S. federal and medical regulations, they must also take into account privacy and security regulations that pertain specifically to data and technology.[17] A few examples of data privacy regulations are the EU Directive on Data Protection, and a U.S.-based Health Insurance Portability and Accountability Act. Failure to comply with HIPAA regulations can result in civil and criminal penalties, which would be counterproductive if they occurred in the midst of efforts to cut costs and expand service through telehealth.

IV. SIGNIFICANCE AND BENEFITS

The importance of the cyber security challenges resolution involves competing as telehealth grows in the United States. Telemedicine guarantees many advantages among which are represented decreased healthcare costs, increased access to healthcare, and improved patient experience. At the same time, the widespread adoption of telemedicine potentially creates a vulnerability in the confidentiality of data. The platforms of telehealth can be considered the channel through which cybercriminals have access to sensitive patient information like data breaches and ransomware, creating chaos on patient confidentiality and trust in the healthcare system. What we must undertake without a doubt is to have cutting-edge cybersecurity measures and this will be instrumental to prevent these risks and protect the services of telehealth[18]. Furthermore, privacy purposes and patients' trust in healthcare professionals' competence are undermined, as it is crucial to protect the quality and constancy of healthcare services. Telehealth is an important factor in increasing the quality of health care and can help with remote monitoring of chronic diseases, timely interventions of ailments and management of illness. The fact is that without a good cybersecurity in place, these technologies might be jeopardized by data breaches and system vulnerabilities. In the age where healthcare data is a desirable target for cybercriminals, securing the privacy of patient data when using telehealth platforms through ensuring integrity and data security makes it possible to maintain the privacy and without causing disruption to patient care[19]. Although the large-scale acceptance of telehealth for the delivery of healthcare greatly relies on ensuring the patient has the trust in technology. Patients need to be guaranteed that their health information is shielded from any unauthorized access or misuse. Healthcare institutions that implement strategies to overcome cybersecurity issues show that they value protecting private information and safety of patients. It will raise the level of patient involvement and satisfaction with telehealth services. Additionally, strong cybersecurity measures can boost the image of telehealth providers and be part of the job to strengthen the health care system through resistance to cyber threats that keep changing.

.

V. FUTURE

In the future in the United States of America, telehealth is going to serve as an essential component of healthcare delivery, steering on revitalized solutions that target various concerns including accessibility and healthcare challenges like disparities. The advancement in telehealth technology, which is being incorporated into existing healthcare systems, makes the demand for a wide range of cybersecurity solutions never ending. Investments in encryption, multi-factor authentication and regular security audits are the stalwart against the boundaries of cyber-attacks and arm cyber-criminals with their growing repertoire[20]. In addition, regulations will need to evolve along with technological advancements and the changing security landscape. Preserving patient's data by enforcing stringent security norms and holding the responsible for breach to telehealth providers accountable is the need of the hour to maintain the trustworthiness of telehealth services[20].

Cybersecurity needs to be prioritized in telehealth design, but without sacrificing any amount of privacy and trust among patients. Seizing this opportunity is not only ensuring the future success of telehealth but also shows the dedication to plowing ahead with the mission to make such equitable access to quality healthcare become a reality for all Americans.

VI. CONCLUSION

The main focus of this review is the cyber security roles in telehealth and its challenges. Due to the rapid development of telemedicine, there is very sparse information on the status and types of security and confidentiality breaches in telehealth services today. Further research is required to investigate these problem areas in more detail. We believe that the current pandemic has greatly accelerated the utilization of telehealth services, and post-pandemic use will be even higher. This presents an opportunity to nip these cybersecurity-related problems in the bud, rather than attempting to fix them once they have become widespread issues.

Through telehealth services, patients can essentially bring their medical information and even the potential for diagnosis at a remote site. This makes the need for security and confidentiality all the more important. Should it become known that a particular health plan has a history of leaking information in these remote exchanges, patients will border on reluctance and refusal of participation. Although the HITECH Act has proved to be successful in improving and enforcing security and confidentiality standards in health plans today, we must ensure that any further advancement does not reverse this positive progress. It is clear that advancements in technology have influenced the healthcare industry, and telehealth services are a product of that influence. While telehealth services make it easier for patients to receive and share medical information, make appointments, and get appropriate care from the convenience of their home, there are potential cybersecurity issues related to these remote services. During the course of our presentation, we have emphasized that while IT technology, by way of electronic health records and internet use, has indeed brought about many positive changes to the healthcare industry, it has also created many security and confidentiality problems. Telehealth services are an extension of IT technology and thus have inherited these security and confidentiality problems.

REFERENCES

[1] M. F. Hogan, "New Freedom Commission Report: The President's New Freedom Commission: Recommendations to Transform Mental Health Care in America," *Psychiatric Services*, vol. 54, no. 11, pp. 1467–1474, Nov. 2003, doi: https://doi.org/10.1176/appi.ps.54.11.1467

[2] Z. A. Carter *et al.*, "Creation of an Internal Teledermatology Store-and-Forward System in an Existing Electronic Health Record," *JAMA Dermatology*, vol. 153, no. 7, p. 644, Jul. 2017, doi: https://doi.org/10.1001/jamadermatol.2017.0204

[3] K. Piwernetz, "DiabCare Quality Network in Europe-A model for quality management in chronic diseases," *International Clinical Psychopharmacology*, vol. 16, no. Supplement 3, pp. S5–S13, Apr. 2001, doi: https://doi.org/10.1097/00004850-200104003-00002

[4] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, pp. 659–676, Jan. 2018, doi: https://doi.org/10.1016/j.future.2017.04.036

[5] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, Jul. 2016, doi: https://doi.org/10.1109/mce.2016.2556879

[6] Rashid Bashshur and Gary William Shannon, *History of telemedicine : evolution, context, and transformation*. New Rochelle, Ny: Mary Ann Liebert, 2009.

[7] J. D. Sachs, G. Schmidt-Traub, M. Mazzucato, D. Messner, N. Nakicenovic, and J. Rockström, "Six Transformations to achieve the Sustainable Development Goals," *Nature Sustainability*, vol. 2, no. 9, pp. 805–814, Aug. 2019, Available: https://www.nature.com/articles/s41893-019-0352-9

[8] S. Whitmee *et al.*, "Safeguarding human health in the Anthropocene epoch: report of The Rockefeller Foundation–Lancet Commission on planetary health," *The Lancet*, vol. 386, no. 10007, pp. 1973–2028, Nov. 2015, doi: https://doi.org/10.1016/s0140-6736(15)60901-1

[9] J.-H. Wu, S.-C. Wang, and L.-M. Lin, "Mobile computing acceptance factors in the healthcare industry: A structural equation model," *International Journal of Medical Informatics*, vol. 76, no. 1, pp. 66–77, Jan. 2007, doi: https://doi.org/10.1016/j.ijmedinf.2006.06.006

[10] J. Ross, F. Stevenson, R. Lau, and E. Murray, "Factors that influence the implementation of e-health: a systematic review of systematic reviews (an update)," *Implementation Science*, vol. 11, no. 1, Oct. 2016, doi: https://doi.org/10.1186/s13012-016-0510-7

[11] M. N. Kamel Boulos, A. C. Brewer, C. Karimkhani, D. B. Buller, and R. P. Dellavalle, "Mobile medical and health apps: state of the art, concerns, regulatory control and certification," *Online Journal of Public Health Informatics*, vol. 5, no. 3, Feb. 2014, doi: https://doi.org/10.5210/ojphi.v5i3.4814. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959919/.

[12] F. S. Mair, C. May, C. O'Donnell, T. Finch, F. Sullivan, and E. Murray, "Factors that promote or inhibit the implementation of e-health systems: an explanatory systematic review," *Bulletin of the World Health Organization*, vol. 90, no. 5, pp. 357–364, May 2012, doi: https://doi.org/10.2471/blt.11.099424. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3341692/.

[13] S. Chan, J. Torous, L. Hinton, and P. Yellowlees, "Towards a Framework for Evaluating Mobile Mental Health Apps," *Telemedicine and e-Health*, vol. 21, no. 12, pp. 1038–1041, Dec. 2015, doi: https://doi.org/10.1089/tmj.2015.0002

[14] R. L. Bashshur *et al.*, "The Empirical Foundations of Telemedicine Interventions for Chronic Disease Management," *Telemedicine Journal and e-Health*, vol. 20, no. 9, pp. 769–800, Sep. 2014, doi: https://doi.org/10.1089/tmj.2014.9981. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4148063/.

[15] P. Yellowlees, J. Shore, and L. Roberts, "Practice Guidelines for Videoconferencing-Based Telemental Health – October 2009," *Telemedicine and e-Health*, vol. 16, no. 10, pp. 1074–1089, Dec. 2010, doi: https://doi.org/10.1089/tmj.2010.0148

[16] A Vaseashta, P. Susmann, and E. Braman, *Cyber security and resiliency policy framework*. Amsterdam ; Berlin ; Tokyo ; Washington, Dc: Ios Press, 2014.

[17] M. J. Alperen, *Foundations of homeland security : law and policy*. Hoboken, N.J.: John Wiley, 2011.

[18] T. G. Lewis, *Critical infrastructure protection in homeland security : defending a networked nation*. Hoboken, New Jersey: John Wiley & Sons, 2015.

[19] C. Chakraborty, *Smart Medical Data Sensing and IoT Systems Design in Healthcare*. IGI Global, 2019.

[20] M. Harwood, *Security strategies in Web applications and social networking*. Editorial: Sudbury, Mass. [U.A.] Jones & Bartlett Learning, 2011.