Telemedicine: Regulation and Protection of Healthcare's Newest Innovation

Introduction

Through telemedicine a new and innovative way for patients to receive the health care they need using technology is becoming more common. With increased amounts of technology and digitalization a space for maleficent actants has been created where cyber-attacks and cyber-security have become prevalent in the healthcare industry. This exponential growth of technological care in the medical field has created new concerns for the safety of digital records. Typically, most clients are unaware that there is a connection between the culmination of medical documents and financial health insurance documents into a more integrated system. When cyber-attacks occur, information such as social security numbers, addresses, confidential, and health information can be taken advantage of. These ideas pose the question, how safe is your data? McGee and Ross (n.d.) state in February of 2015 Anthem Inc., a health insurance company revealed that they had become the victim of a large-scale cyberattack. The authors continue to say the attack led to the leaking of names, birthdays, medical IDs, social security numbers, addresses, emails, as well as employment information affecting approximately 78.8 million people. Given the shear magnitude of critical information one would think that Anthem would have rock solid cybersecurity protocols. However, the perpetrators used phishing emails, a tactic that sends an infected email that looks normal but contains malware that affords the hacker access to company information by creating a backdoor to the network. In the same article, it was found that Anthem had to spend approximately $260 million in efforts surrounding the cyberattack. The money went towards actions such as implementing new and improved security measures as well as notifying and protecting those affected by the security breach.

This thesis aims to explore the efficacy of the current regulators of telemedicine. Additionally, the effects of cybersecurity on the future of the healthcare industry are examined. First, the STS framework contextualizes how telemedicine works within the healthcare industry. The literature review of the paper is divided into three parts: part one will define what telemedicine is and the kinds of products it can become. Part two will address the prominent regulators of telemedicine and what forms of regulation are in place for telemedicine. Part three explores the effect that cybersecurity has on the atmosphere of telemedicine and the healthcare industry.

STS Framework

This project takes the framework of the social construction of technology (SCOT, Figure 1) to investigate the interests and roles of the telemedicine constructors. I used SCOT as a system for evaluating the emergence and existing flexibility over different technological innovations within telemedicine's sector of healthcare. The main components of SCOT include interpretative flexibility, relevant social groups, design flexibility, problems and conflicts, and closure. Interpretative flexibility is the idea that technological artifacts can change over time and between relevant social groups. Relevant social groups are a composition of "all members of a certain social group that share the same set of meanings, attached to a specific artifact" (p. 30) (Bijker, Hughes, & Pinch, 2012). Closure happens when interpretative and design flexibility collapse for a technological artifact. Linderoth and Pellegrino (2005) explain that technological frames are defined as "the understanding that members of a social group come to have of particular technological artifacts and they include not only knowledge about the particular technology but also local understanding of specific uses in a given setting". The authors continue to describe how an application of SCOT analysis was applied to IT-dependent change projects and one of the projects was based in telemedicine. They break the technological frame up into three stages of project development: project startup, project in action, and project rebirth. The telemedicine case study utilized a video conferencing system within a health care setting. The technologies included optical medical equipment connected to a system that would transmit live or frozen images of various body parts for further information that a physician needed. Furthermore, the technology was used for conferences, medical rounds, and education activities. The case study investigated two health centers, three specialist clinics in two county hospitals, and four specialist clinics in one university hospital. In the project start-up phase the consensus among the physicians was to use telemedicine as a way of reducing distances in time and space among different health care units. The expectations were to increase access to knowledge of medical specialists to improve service to patients and development of general practitioners' capabilities. The next relevant stage to my research was the project rebirth. The authors state in order for an actor to re-shape elements of the technology the actor must be able to: have an ability to align themselves with project sponsors that can influence the process, identify tasks that can be appropriately solved by the new technology, and acquire resources in order to create a context specific usefulness for the technology.

The primary stakeholders that this research focused on include the FDA, pharmaceutical companies, insurance companies, and the patients. The FDA is a federal agency in the United States responsible for regulating drugs, medicines, and medical devices for the sake of promoting public safety. Pharmaceutical companies spend billions of dollars on research and development for new drugs and technologies that are capable and efficient at treating medical issues. These big pharma leaders have also begun investing into other companies that use digital technologies as a form of healthcare (Licholai, G., 2019). Insurance companies cover a variety of medical, surgical, and dental expenses for patients. Twenty-six states have “Parity” laws that require private insurers to provide reimbursement for services delivered through telemedicine (Chiron, n.d.) There are nuances within each state that may vary. Certain states require an in-person visit before a provider can be billed for telemedicine. The amount of coverage that insurers are required to pay can vary based on state law. More states are considering the adoption of these Parity laws because of the value of telemedicine. The patient is worried about getting the best healthcare possible in the most efficient and convenient way on an individual basis. The healthcare system becomes incredibly muddled because of its complex nature with so many different facets and players.

Literature Review

A Snapshot of the Current State and Potential Directions of Telemedicine

The development of telemedicine provides a perfect example of illustrating social-technical complexities. The definition of telemedicine according to the World Health Organization (WHO) is “The delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities,” (p. 9) (WHO, 2010) The WHO definition indicates that telemedicine is not a traditional medical service which requires patients’ and physicians’ physical presence. It instead fundamentally changes the interaction between healthcare provider, consumer, and government regulators.

There is a wide variety of illnesses that can be addressed by telemedicine. The Seattle Veterans Administration Medical Center employed telemedicine in order to provide follow-up care to patients with Parkinson's disease (PD) (Samii, Tsukuda, & Ryan-Dykes, 2006). These patients were anywhere from 67 to 2400 kilometers from the medical center. The results of this form of telemedicine was 1500 travel hours, 100,000 km travel distance, and 37,000 USD cost of travel and housing all saved. Studies have shown that telemedicine can be very beneficial in the treatment of chronic diseases. Hepatitis C Virus (HCV) is a liver infection that can lead to liver damage due to inflammation within the infected person. The Extension for Community Healthcare Outcomes (Project ECHO) was a program developed in order to increase accessibility to interferon-based treatment for patients with HCV in rural areas of New Mexico (Serper & Volk, 2018). They used video teleconferencing as a means to increase the expertise of health care providers and HCV treatment initiation for patients. The project also extended into Utah and Arizona showing high success rates for continual treatment of HCV and a sustained virologic response. Similarly, telemedicine was used in the treatment of Chronic Liver Disease in Mexico (Serper & Volk, 2018). The technology was used as a remote monitoring system for patients with the disease or after a liver transplant. Daily weights, blood glucose reading, and vital signs were transmitted to a transplant center that sifts through the data to decrease the amount of re-admissions to the hospital. In a study of 20 liver transplant patients using smart tablets to transmit this information, patients with 100% daily interaction were not re-admitted. This is just scratching the surface for the multitude of ways telemedicine can benefit patients and healthcare professionals.

The Role and Form of Regulations Governing Telemedicine

The FDA has had to change the way in which it views what a medical device is because of new technologies. A subsection of the FDA, the Center for Devices and Radiological Health (CDRH) created a specialized program to assess and regulate digital health technologies (Center for Devices and Radiological Health Digital Health, n.d.) The International Medical Device Regulators Forum (IMDRF) of which the FDA is a member come together in order to synchronize the standards of regulations throughout the world. They defined software as a medical device (SaMD) as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device." (Center for Devices and Radiological Health Software as a Medical Device, n.d.) SaMD presents a new issue in how to assess the safety and effectiveness of these new programs as medicine. There is a framework of criteria that a developer should aim to assess in the design of SaMD. Clinical Validity, scientific validity, clinical performance, and analytical validity are the four main aspects that need to be addressed (Whitten, Drori, Lacktman, Foley & Lardner LLP, n.d.). Clinical validity is where the developer shows that the SaMD has usefulness in terms of its patient care. Scientific validity is when the developed creates an association between the SaMD's output and the intended condition that is to be treated. Clinical performance demonstrates that the SaMD does what it is intended to do and benefits the patient. Analytical validity is the way that the developer shows that the SaMD is able to generate the expected results via proper design. This is the process that a developer should follow in order to prove to the regulating body that its SaMD can be used in the medical field.

A subsection of the IMDRF named the Software as a Medical Device Working Group (SaMD WG) has created general policies for SaMD in order for people to globally be on the same page when it comes to the regulation for SaMD. However, these documents are only suggestions and there is no concrete regulation for software as a medical device as of yet. These documents include the definition, the clinical evaluation, the quality management system, and framework for risk categorization for SaMD. The goal of the clinical evaluation is to answer three important questions: “Is there a valid clinical association between your SaMD output and your SaMD’s targeted clinical condition? Does your SaMD correctly process input data to generate accurate, reliable, and precise output data (analytical validation)? Does use of your SaMD’s accurate, reliable, and precise output data achieve your intended purpose in your target population in the context of clinical care (clinical validation)? (Software as a Medical Device Working Group, 2017, p. 7).” The quality management system of a SaMD is a system created by the manufacturer with the intent to control quality and maintain safe and effective performance throughout the life of the SaMD (IMDRF SaMD Working Group, 2015). An effective QMS for SaMD has leadership and organizational support, life cycle support processes, and realization and use processes for the SaMD. The strong leadership and organizational support’s purpose are to effectively implement the QMS and create a strong team with the correct qualifications for doing so. The lifecycle support processes are in place in order to provide effective ways that support any SaMD through the entirety of its life. One example is the idea of a risk management system focused on patient safety. The QMS can include the identification of hazards, estimation and evaluation of associated risks, actions to control risks, and methods to monitor the effectiveness of the actions implemented to control the risks. The third component of a QMS, the realization and use processes are commonly used practices that a company that manufactures SaMD should follow. An example includes verification and validation (V&V) activities. Verification is to make sure that the SaMD follows all requirements and validation is to provide evidence that the SaMD meets its intended use and operational requirements. The SaMD WG has worked extensively to provide frameworks and suggestions for manufacturers and developers of SaMD for the future of telemedicine.

With the creation of these new telemedicine technologies in the digital era problems involving privacy arise. The means in which the sensitive health information is being transmitted needs to have a high degree of security in order for patients to trust and advocate for telemedicine. There have been arguments for a single federal organization, the Federal Trade Commission (FTC) to coordinate the creation and enforcement of extensive privacy and security standards (Hall & McGraw, 2014). While the FDA has a major regulatory presence in the healthcare industry, telemedicine changes the way privacy and security need to be handled and regulated.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a law that was passed by Congress that was intended to modernize how healthcare information was transferred and interacted with. Subpart C—Security Standards for the Protection of Electronic Protected Health Information states that covered entities and business associates must "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. They must protect against any reasonably anticipated threats or hazards to the security or integrity of such information. They must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part (Procedures for hearings). They must ensure compliance with this subpart by its workforce (U.S. Department of Health and Human Services Office for Civil Rights, 2013, p. 63). The Health Information Technology for Economic and Clinical Health (HITECH) Act is a law that was passed by Congress in 2009. Part of the HITECH Act forces entities covered by HIPAA to disclose whenever they have a breach of health information (Luna, Rhine, Myhra, Sullivan, & Kruse, 2015). These federally instituted laws are critical to telemedicine's regulation and security operating primarily through fines. If a covered entity violates an identical provision there is a maximum penalty of $1,500,000 for all violation categories including did not know, reasonable cause, willful neglect that is corrected, and willful neglect that is not corrected (HHS, 2009).

Impacts of Cybersecurity on Telemedicine and the Healthcare Industry

Cybercrime can be broken up into two types, external or internal threats. The two types of threats can then be broken up into two categories either direct or indirect forms. Examples of direct and indirect internal threats include employees, infected equipment, denial-of-service attack (direct), obsolete information security systems, and budgeting restrictions (indirect). Examples of direct and indirect external threats include data breaches, cyber terrorism, denial-of-service attack (direct), cybersquatting, and critical infrastructure failure (indirect) (Luna, Rhine, Myhra, Sullivan, & Kruse, 2015). A denial of service (DoS) attack comes in two forms, a standard form and a distributed denial of service (DDoS) attack. The criminal essentially floods the network with too many service requests and useless traffic than it can handle resulting in a crash. The DDoS attack makes it, so the requests originates from many different locations making it difficult to block. Cybersquatting is when a perpetrator registers a well-known trademark as an Internet domain name for their own financial benefit either by ransoming it back to the proper owner or keeping traffic going to their domain (Luna, Rhine, Myhra, Sullivan, & Kruse, 2015). A cybercriminal targeting companies in the healthcare industry typically does so in order to sell the information on the black market for financial gain. Cyberterrorism is another type of cybercrime that can have devastating effects including hindered care to patients that could put lives in danger. With this plethora of ways cyber criminals can take advantage of the healthcare system it is imperative that the healthcare industry bolster the cyber security that is in place.

The Ponemon Institute completes an annual study on privacy and security of healthcare data. In the 2016 study they looked at 91 HIPAA covered entities and 84 business associates who perform services for the covered entities involving use or disclosure of protected health information (PHI). 89 percent of the healthcare organizations and 61 percent of business associates involved in the study suffered from at least one data breach involving the loss or theft of patient data within the past 24 months. They estimate that data breaches within the healthcare industry could be costing approximately $6.2 billion. The healthcare organizations paid on average $1.1 million a year in expenses due to data breaches. It was reported that 50 percent of the healthcare organizations said the breaches were due to a criminal attack and 13 percent report it was due to a malicious insider. On the other hand, business associates reported 41 percent of breaches were caused by a criminal attacker and nine percent report it was due to a malicious insider (Ponemon Institute, 2016).

There are different methods that healthcare providers can take in order to minimize the effects caused from cyberattacks. According to the Healthcare Provider Breaches and Risk Management Road Maps survey conducted by the SANS Institute, there are various priorities that can help to build the cybersecurity system for the healthcare industry. Quick and efficient responses are needed to address cyber threats. The implementation of breach detection technology and procedures will assist in improved response times. Patient data protection is paramount for covered entities and business associates. Internal security measures need to position technical and operational security controls close to the data. Cyber criminals can attack from multiple different entry points because the healthcare industry is multifaceted. The supporting infrastructure such as third-party networks in the supply chain must also adopt proper cybersecurity systems. Regulatory compliance standards must be followed in order to secure data and critical systems. Health data should be classified, sorted, and stored appropriately to prevent easy access by cybercriminals. Managing who is able to access the organizations network is crucial to stopping outsiders from getting in. According to the SANS Institute, "Implementing a robust role-based identity access management strategy that includes password admittance procedures, user access trackers, network segmentation, and encrypting network systems…" (p. 29) are properties of a well-crafted network management system. An essential part of developing a cybersecurity system is planning. In the event of a data breach, a plan that includes the necessary steps to minimize the threat, bring the system back online, and alert the victims must be readily available. An organization is only as good as the team that makes it up. Employing high-quality cybersecurity strategists will draft a better system and minimize vulnerabilities that the organization may face. The users of the network: employees, vendors, and patients alike need to be educated about how their actions can leave loopholes for cybercriminals to exploit. Medical devices connected to the network can also be insecure if not properly maintained. Lastly, the endpoints in an online system is the hub in which the users interact. It is the perfect landscape for cybercriminals to employ phishing emails and ransomware to infect a network. Extra security measures should be placed at these points to prevent cyberattacks from happening (Cabrera, 2016). Telemedicine cybersecurity methods can be taken from existing markets that already protect their important digital data however, within the telemedicine section of healthcare the level of protection is not where it needs to be. The healthcare industry needs to take action to implement these cybersecurity priorities so that the insurgence of digital health data is well protected.

Analysis

Telemedicine is a new innovative tool that uses information technology to facilitate healthcare services over a distance. The main function of using this method over a more traditional approach is to lower costs and time spent. There are endless possibilities of uses for telemedicine. It can make chronic disease monitoring simpler and faster without constant in-person checkups.

Parity laws are important because they identify what is covered when participating in a telehealth option of treatment. Certain states may or may not require private insurers or Medicare to reimburse these services at the same rate as in-person visits. If these laws were not in place, patients who wish to use telemedicine are disincentivized from doing so because of the lack of coverage. It would be useful to have a study of a map of coverage percentage of parity laws and the amount of use of telemedicine on a state by state basis. This would assist in showing if there is a positive correlation between a patient's coverage and use of telemedicine. Because telemedicine is a novel form of treatment insurance companies may not have as much faith in it as in-person visits, thus changing the amount of coverage the patient gets. Insurance companies interpret telemedicine as an unknown that may not be as effective requiring more frequent visits and more money from them. Over time as more studies such as Project ECHO come to light their interpretation of telemedicine can change to a positive one.

Based upon the evidence presented by IMDRF SaMD WG they have created enough working frameworks to assist the current climate of SaMDs. They have taken many components from what already works in current regulations of medical devices and applied them to SaMDs. This is a form of closure over the debate according to SCOT. The IMDRF SaMD WG's framework is vetted and can be transferred to telemedicine's SaMD. No new relevant social groups need to get in the way of this innovation. The scientific validity establishment, the generation, appraisal, and analysis of analytical performance data, and the clinical performance data conformation to relevant evaluation processes were adopted into the three prong effect of establishing a valid clinical association, analytical validation, and clinical validation for SaMDs (Software as a Medical Device Working Group, 2017).

The FDA has a class system in place for the regulation of medical devices. There is Class I the lowest risk class that is exempt from any application materials. Class II is the moderate risk category where a 510(k) is needed. A 510(k) or a premarket notification (PMN) states that device manufacturers must notify the FDA in advance to market their device. The device does not require clinical trials; however, there must be substantial evidence that the device is equivalent to a device already on that market that was reviewed according to a 510(k). The highest risk, Class III requires a premarket approval (PMA) which means the device must prove safety and efficacy based upon a conducted premarket clinical trials and premarket inspection of the manufacturing facility (Ronquillo & Zuckerman, 2017). Between 2011 and 2015 the FDA recalled 627 medical devices due to software-related issues. 23 of the devices were low-risk recalls, 592 were moderate-risk recalls, and 12 were high-risk recalls. SaMD has a similar categorization system ranging from Category I to Category IV. The category is determined based on the information SaMD provides as well as the severity of the healthcare condition. The information categories include treat or diagnose, drive clinical management, and inform clinical management. The healthcare conditions vary between non-serious, serious, and critical (IMDRF Software as a Medical Device (SaMD) Working Group, 2014).

In December of 2016 the 21st Century Cures Act was passed. This law gave federal funding mostly to the National Institute of Health. The goal of the law is to accelerate medical product development and the review and regulation of medical products. The passing of this law has implications of faster approval time for medical devices however, the benchmark for the evidence provided must remain high or ineffective treatments could be approved (FDA, n.d.). HIPAA acts as a baseline for the regulation of telemedicine. Applicable covered entities and business associates must follow these rules or face legal and financial consequences. In order to build trust between the patient and healthcare organizations laws such as the HITECH act create transparency when there is a breach. With telemedicine being a newer form of treatment as it grows and develops more specific legislature may be needed for future regulation.

It is important that funds are allocated to bolstering the cybersecurity within the healthcare industry in order to combat against cyberattacks. Both external and internal threats are costing these entities millions if not billions of dollars and will continue to bleed the industry if measures are not taken. As more and more technologies are created for healthcare the digital footprint on the industry becomes larger. Both the Ponemon and SANS Institutes are in agreement that the healthcare industry is not doing enough to protect electronic health information. There is a severe lack of infrastructure in many of the healthcare industries' cybersecurity systems that needs to be fixed.

Conclusion

In order to continue this research paper, the next step would be to continue to monitor the ways in which telemedicine is being regulated. As it grows and potentially becomes ubiquitous there will be more government regulation surrounding it. Telemedicine is highly adaptable to many different situations within healthcare therefore the way in which the design flexibility effects the specifications of the regulation should be explored.

From the information gathered, there is evidence to support that there is a regulatory framework available for telemedicine. The FDA and IMDRF provide useful guidelines for the developers and manufacturers of telemedicine products to follow. One prominent issue that must be addressed within the growing healthcare industry is cybersecurity. While there are resources available, such as hiring a private cybersecurity firm such as Mandiant in the case of the Anthem breach, healthcare organization haven't been adequately budgeting for the rise of cyberattacks (McGee, M. K., & Ross, R., n.d.). The approach to cyberattacks need to be proactive and not reactive.

Reference List

Bijker, Wiebe E., Thomas P. Hughes, and Trevor J. Pinch (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, 1987. Cambridge, MA: MIT Press.

Cabrera, E. (2016) Health Care: Cyberattacks and How to Fight Back. *Journal of Health Care Compliance*, *18*(5), 27–30.

Center for Devices and Radiological Health. (n.d.). Digital Health https://www.fda.gov/medical-devices/digital-health

Center for Devices and Radiological Health. (n.d.). Software as a Medical Device (SaMD). https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd

Chiron. Will My Insurance Cover Telemedicine? (n.d.). https://chironhealth.com/definitive-guide-to-telemedicine/telemedicine-info-patients/will-insurance-cover-telemedicine/

FDA (n.d.). 21st Century Cures Act. https://www.fda.gov/regulatory-information/selected-amendments-fdc-act/21st-century-cures-act

Hall, J. L., McGraw, D. (2014). For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. *Health Affairs, 33*(2), 216-221. https://www.healthaffairs.org/doi/10.1377/hlthaff.2013.0997

IMDRF SaMD Working Group. (2015). Software as a Medical Device (SaMD): Application of Quality Management System. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-151002-samd-qms.pdf

IMDRF SaMD Working Group. (2013). Software as a Medical Device (SaMD): Key Definitions. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

IMDRF Software as a Medical Device (SaMD) Working Group. (2014). "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

Licholai, G. (2019, January 07). Digital Healthcare Growth Drivers In 2019. https://www.forbes.com/sites/greglicholai/2019/01/07/digital-healthcare-growth-drivers-in-2019/#97568dc1dba3

Linderoth, H. C., & Pellegrino, G. (2005). Frames and inscriptions: tracing a way to understand IT-dependent change projects. *International Journal of Project Management*, *23*(5), 415–420. doi: 10.1016/j.ijproman.2005.01.005

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2015). *Cyber threats to health information systems: A systematic review.* Technology & Health Care, 2016, *24*(1), 1-9.

McGee, M. K., & Ross, R. (n.d.). A New In-Depth Analysis of Anthem Breach. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Ponemon Institute LLC (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data.* https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20&%20Data%20Security%20Report%20FINAL%206.pdf

Ronquillo, J. G., & Zuckerman, D. M. (2017). Software-Related Recalls of Health Information Technology and Other Medical Devices: Implications for FDA Regulation of Digital Health. *The Milbank Quarterly*, 95(3), 535–553. doi: 10.1111/1468-0009.12278

Samii, A., Tsukuda, R. A., & Ryan-Dykes, P. (2006, January). Telemedicine for delivery of health care in Parkinson's disease. *Journal of Telemedicine and Telecare. 12*(1), 16-18 https://journals.sagepub.com/doi/abs/10.1258/135763306775321371

Serper, M. & Volk, M. L., (2018). Current and Future Applications of Telemedicine to Optimize the Delivery of Care in Chronic Liver Disease. *Clinical Gastroenterology and Hepatology Journal, 16*(2),157-161 https://doi.org/10.1016/j.cgh.2017.10.004

Software as a Medical Device Working Group. (2017). Software as a Medical Device (SaMD): Clinical Evaluation https://www.fda.gov/media/100714/download

United States Department of Health and Human Services. (2009). HIPAA Administrative Simplification: Enforcement CFR 45 160 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf?language=es

U.S. Department of Health and Human Services Office for Civil Rights. (2013). HIPAA Administrative Simplification Regulation Text https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

Whitten, T., Drori, J., Lacktman, N., & Foley & Lardner LLP. (n.d.). FDA's new digital health unit and guidance for mHealth and telemedicine companies. https://www.beckershospitalreview.com/healthcare-information-technology/fda-s-new-digital-health-unit-and-guidance-for-mhealth-and-telemedicine-companies.html.

WHO. Telemedicine: opportunities and developments in Member States. (2010). https://www.who.int/goe/publications/goe_telemedicine_2010.pdf.

Appendix

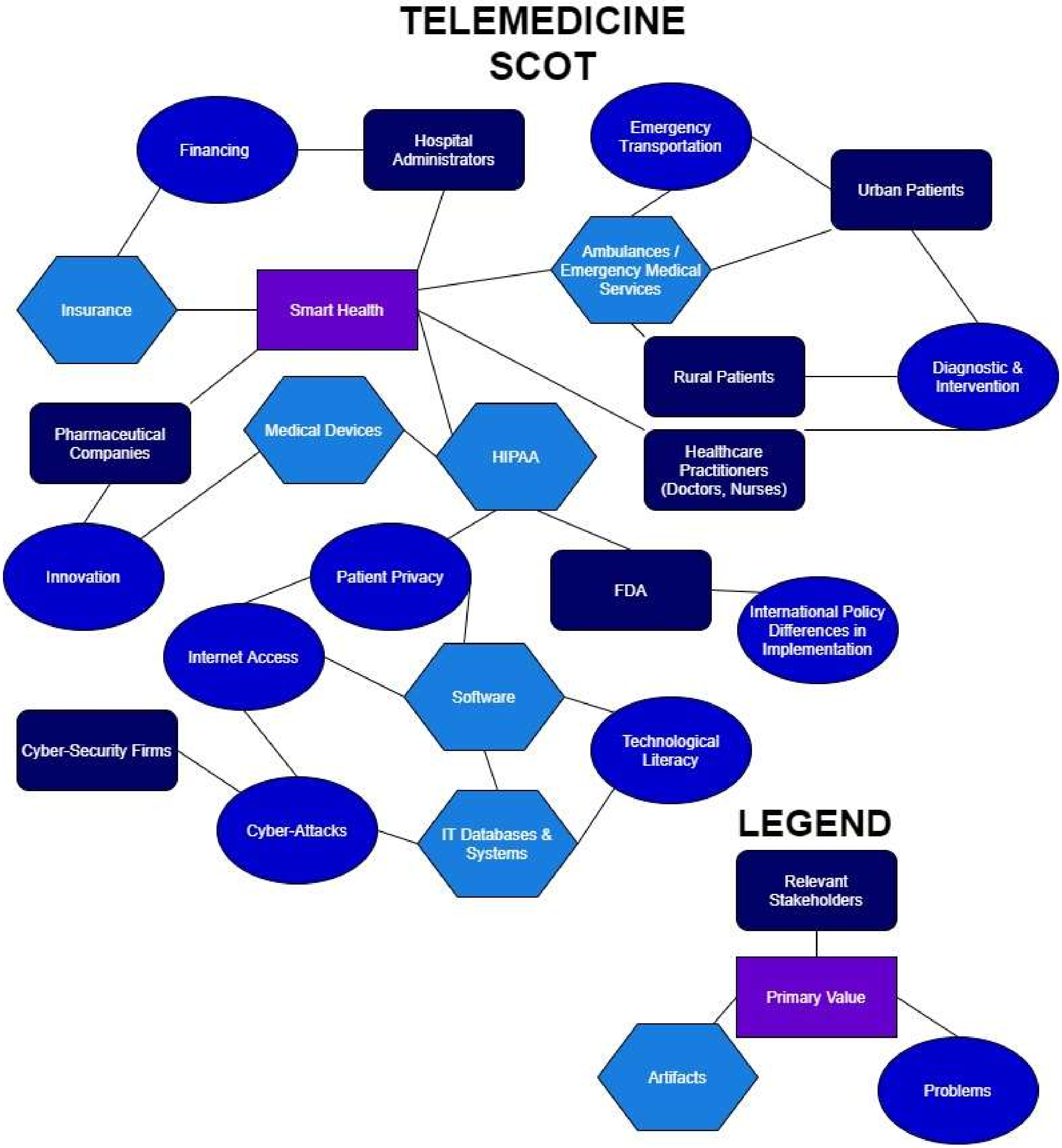

Figure 1 Social Construction of Technology Diagram for Telemedicine