https://doi.org/10.48009/2_iis_2020_102-111

Issues in Information Systems

Volume 21, Issue 2, pp. 102-111, 2020

A SIX-DIMENSIONAL FRAMEWORK FOR TELEHEALTH DELIVERY

Ganesh Vaidyanathan, Roosevelt University, gvaidyanathan@roosevelt.edu
Mark Fox, Indiana University South Bend, mfox1@iusb.edu

ABSTRACT

Telehealth is one of the most influential emerging technologies in healthcare. Traditionally, failure in the successful introduction of an information system is correlated with its delivery model. The delivery of telehealth depends heavily on the mitigation of its project risks. Apart from the usual project management risks, the idiosyncratic risks of telehealth implementation are identified in this paper. We have identified several factors that constitute six dimensions for successful telehealth implementation. The six dimensions include the risks associated with new business models, legal and ethics, patient privacy and data security, new technologies, fulfillment, and socioeconomics. We use those six dimensions to formulate a framework for telehealth delivery.

Keywords: Telehealth, Telemedicine, Telecare, Mobile Health, Healthcare, Framework

INTRODUCTION

The Internet-of-Things (IoT) has been heavily employed in our personal and industrial environments. However, telehealth and its related smart devices have not been accepted or deployed widely. Healthcare spending in the U.S. continues to grow. The Centers for Medicare and Medicaid Services (CMS) forecasts national health spending will grow at an average rate of 5.5% per year through 2027. Moreover, the current COVID-19 pandemic has created widespread concern about healthcare spending. This concern accumulated with social distancing norms has prompted many healthcare professionals to take a serious look at telehealth and telemedicine (Fonda, 2020). The first uses of medicine using telephones dates back to the 1920s and employed for ship to land consultations (Pereira, 2017). While the terms telehealth, telecare, telemedicine, and mobile health are often used interchangeably, there are important differences between these medical terminologies. Figure 1 illustrates the differences between these terms based on definitions articulated by the Federal Communications Commission (2020) and Kizilova (2018).

	Telehealth is similar to telemedicine but includes a wider variety of remote healthcare services beyond the doctor-patient relationship. Telehealth includes services provided by nurses, pharmacists, or social workers, patient health education, social support and medication adherence, and troubleshooting health issues for patients and their caregivers. (Federal Communications Commission, 2020).
	Telemedicine uses telecommunications technologies to support the delivery of all kinds of medical, diagnostic, and treatment-related services usually by doctors. Telemedicine includes conducting diagnostic tests, closely monitoring a patient's progress after treatment or therapy and facilitating access to specialists that are not located in the same place as the patient. (Federal Communications Commission, 2020).
	Telecare technology allows consumers to stay safe and independent in their own homes. Telecare may include health and fitness apps, sensors and tools to connect consumers with family members or other caregivers, exercise tracking tools, digital medication reminder systems or early warning and detection technologies. (Federal Communications Commission, 2020).
	Mobile health is a newer concept that describes services supported by mobile communication devices--such as wireless patient monitoring devices, smartphones, personal digital assistants, and tablet computers. (Kizola, 2018).

Figure 1. Differences Between Telehealth, Telemedicine, Telecare, and Mobile Health

The key feature of telehealth is that it involves a broader range of remote healthcare services being provided to patients that extend beyond the doctor-patient relationship. Put concisely, telehealth involves a physician in one location using telecommunications infrastructure to deliver care to a patient located at a distant site (American Academy of Family Physicians, 2020). Telehealth use increased substantially between 2005 and 2015, but its use was still uncommon by 2016 (Pittman, 2016). While the use of tele-mental health grew steadily over this period, there was a rapid increase in growth for primary care telemedicine in 2015 and 2016, after coverage for direct-to-consumer telemedicine expanded (Pittman, 2016). Telehealth is convenient for both patients and physicians as it reduces travel and waiting times, while allowing convenient treatment and monitoring chronic conditions in patients.

However, while direct-to-consumer telemedicine and telehealth may increase access by making healthcare more convenient for patients it may also increase utilization and healthcare spending (Ashwood et al., 2017). There are many other issues regarding telehealth. Yang (2016) points out that although telehealth has a wide range of potential benefits, the delivery of health care via telecommunications technologies presents risks and challenges for healthcare providers. Typical concerns include health professional and patient relationships; quality of health information; infrastructure planning and development problems; lack of uniformity in parity laws; physician licensure requirements; and patient privacy and malpractice liability in different states. Such concerns--and other issues that we discuss in this paper--will constrain the implementation and growth of telehealth services.

The objective of this paper is to identify those concerns, formulate key dimensions of telehealth, and develop a framework of telehealth implementation using those dimensions. The contribution of this paper is a new framework of telehealth delivery. In this paper we have included six major dimensions, including: confidentiality risks; business model risks; ethical risks; technology risks; fulfillment and socioeconomic risks. The structure of this paper is as follows: In the next section, we discuss the details of how telehealth can play an important role in the society. We then identify the dimensions of telehealth to develop a framework that can be used by healthcare professionals and healthcare industry. The final section includes the conclusion and suggestions for future research.

KEY DIMENSIONS OF TELEHEALTH AND FRAMWORK FOR TELEHEALTH DELIVERY

There is growing concern on various issues relating to telehealth. However, the healthcare industry has begun to realize the benefits of telehealth. These concerns and benefits need to be considered in implementing telehealth systems. Vaidyanathan and Devaraj (2003) developed a five-factor framework for analyzing online risks attributable to new services, new business models, new processes, new technologies, and new fulfillment needs. Subsequently, Vaidyanathan (2007) expanded that study to summarize all the possible risks in online business. The inherent risks of online business have been a significant factor for new businesses to be cautious in embracing technologies. The perceived risks include: security and privacy (Mercuri, 2005); privacy assurance (Moores, 2005); credibility and information asymmetry (Ba & Paulou, 2002); reliability, damage and loss of systems (Dillon & Pate-Cornell, 2005; Straub & Welke, 1998); decision-making processes (Pathak, 2004); poor business models (Grover & Saeed, 2004); and online services (Lange et al., 2000; Orr, 2005).

In this paper, we consider various risks associated with telehealth to establish a framework for further evaluation of telehealth. Specifically, we demonstrate that telehealth risks can be categorized into the following six dimensions:

1. New business model risks
2. Legal and ethical risks
3. Patient privacy and data security risks
4. New technologies risks
5. Fulfillment risks
6. Socio-economic risks

These risks are represented in Figure 2 as a framework for telehealth delivery. One example of a telehealth delivery process has been proposed by Cox, Plavnick, and Boradhed (2020). Their paper focuses on the telehealth delivery process for risk mitigation. In that study, due to the ongoing Coronavirus pandemic, the authors argue that providers who serve individuals with autism spectrum disorder (ASD) should be able deliver healthcare through telehealth for

patients. The telehealth delivery technology exists in the current timeframe in the form of audio (e.g., phone) and video (e.g., FaceTime, Zoom). Such technologies should be conducive to telehealth delivery and order fulfillment.

To begin, insurance companies strictly require HIPAA-compliant platforms in their documents approving the use of telehealth services. If a noncompliant platform is used, the insurance companies demand that the platform should be clearly stated as a risk and the providers should enforce informed-consent documents before the provision of telehealth services to maintain confidentiality. The authors propose that, since telehealth services require unique skills, the Board-Certified Behavior Analysts (BCBA) should be trained well in technology and practice only within their scope of competence. The process should include a public repository with resources for delivering the services to ASD patients via telehealth and telephonic media. This example illustrates the risks that are involved in telehealth delivery including confidentiality risks, business model risks, ethical risks, technology risks, fulfillment and socioeconomic risks. We now explore these risks one by one and discuss their impact on telehealth delivery.

New Business Model Risks

The complex nature of a business itself is one of the concerns of the risk industry (Kaiser, 2002). Performance risk, financial risks, and transactions risks are central to new business models (Biswas & Biswas, 2004). Performance risk is the uncertainty and consequence of a product not functioning at some expected level. Financial risks are the uncertainty and monetary loss one perceives to be incurring if a product does not function at a certain expected level. As consumers, patients have higher levels of perceived performance, financial, and transaction risks when engaging in e-business (Biswas & Biswas, 2004). Transaction risks include, but are by no means limited to, the uncertainty associated with giving information such as credit card number during a transaction.

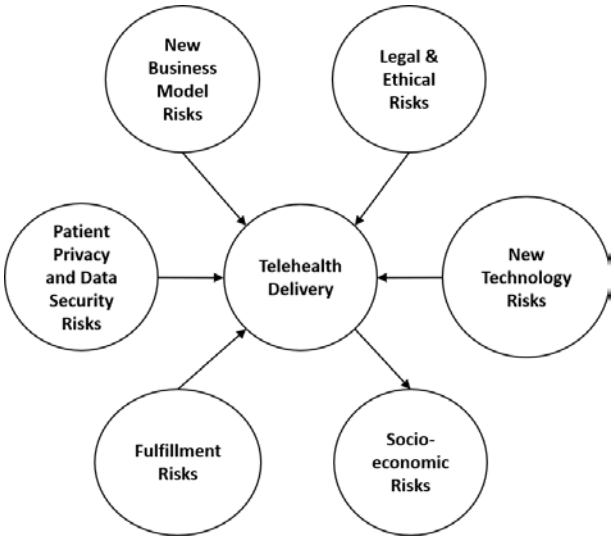

Figure 2. Framework for Telehealth Delivery

A good business model is essential to every new venture or an established organization (Magretta, 2002). Almost 75% of new e-health programs fail during the operational stage (Berg, 1999). Accordingly, the development of a comprehensive telehealth business model is important to reduce risks and ensure success (van Limburg et al., 2011). A comprehensive list of issues pertaining to business model risks is as follows:

- Lack of a robust model including appropriate pricing structures and allocation of revenues among the value chain;
- Lack of awareness of telehealth services and cost benefits;
- Exclusion of telemedicine services by employers;
- Prohibitive or high costs of telehealth to physicians, hospitals, and other healthcare providers;
- Lack of universal standards;
-

- Lack of strategy and general deployment of the system (Pereira, 2017); and
- High initial setup costs of systems (Pereira, 2017).

Legal & Ethical Risks

In 1999 the World Medical Association (WMA) promulgated a statement of ethics on telemedicine. One of the more striking recommendations of the WMA is that "Telemedicine should not be viewed as equal to face-to-face healthcare and should not be introduced solely to cut costs or as a perverse incentive to over-service and increase earnings for physicians." (World Medical Association, 2018).

Several legal issues need to be addressed if telemedicine is to grow. One such issue is the tension between state laws on medical licensure telemedicine (Uscher-Pines & Kahn, 2014). Under the present individual state licensure system physicians are required to be medically certified and licensed in each state in which they teleconsult with their patients (Pereira, 2017). Advance Practice Registered Nurses will also likely play a key role in providing clinical expertise for telehealth, as well as adopting disease prevention and health management roles (Garber & Chike-Harris, 2019). State laws differ in terms of what telemedicine activities nonphysicians can provide patients (Garber and Chike-Harris, 2019). These licensure and credentialing constraints provide both cost and access barriers to providing telehealth services (Pirtle et al., 2019). These constraints effectively limit telemedicine to the State borders and as such curbs the potential geographic benefits that mobile telehealth solutions can provide.

Two initiatives are making some inroads into providing telehealth service across states. First, in 2018 the US Department of Veterans Affairs (VA) expanded their care for veterans by allowing for telehealth to be provided irrespective of where the veteran or the provider are located. This meant that VA effectively overrode state restrictions on telehealth or practitioner licensing. In the press release, the VA said: "By enabling Veterans nationwide to receive care at home, the rule will especially benefit Veterans living in rural areas who would otherwise need to travel a considerable distance or across state lines to receive care. The rule also will expand Veterans' access to critical care that can be provided virtually — such as mental health care and suicide prevention — by allowing quicker and easier access to VA mental health providers through telehealth." (US Department of Veterans Affairs, 2018). A similar compact is available for nurses, the Nursing Licensure Compact.

The second initiative, The Interstate Medical Licensure Compact (IMLC), streamlines licensure for physicians who want to be able to practice in multiple states. At present, 29 states are included in the compact, which allows physicians who are already licensed in one of the Compact states to apply to practice in other Compact states by completing a single online application (Interstate Medical Licensure Compact, 2020).

Furthermore, there remains significant ambiguity as to whether telemedicine services are covered under malpractice insurance policies (Smith, 2005). Malpractice issues and challenges are compounded when telemedicine services extend beyond individual state borders (Gagnon et al., 2005). Medical malpractice is typically included in professional liability insurance. However, such policies may not cover telehealth unless additional coverage is purchased (Balestra, 2018).

Patient Privacy and Data Security Risks

Telehealth systems require data collected through transmissions to and from remote healthcare facilities, either through live sessions or through web-based applications. Privacy, integrity, and authenticity of the collected data must be guaranteed to ensure correct diagnosis and treatment without any violation of the privacy of patient data. Incorrect and inaccurate calibrations of medical equipment, inaccurate data, non-compromised data, proper identity management of individual patients are critical and pose as risks. In general, healthcare data are sensitive and critical, and mishandling of patient information and this may pose severe risks (Pramanik et al., 2019).

Privacy is the infringement by online retailers or service providers who share, sell, or rent personal information to other companies, contacting without the consent of consumers, and tracking habits and purchases. Patient privacy risks may be greater in telehealth because of the nature of the interactions between patients and those providing care. The remote location of healthcare providers means that they will often have to share information with one another, thus giving increased potential for security risks (we discuss this further below). Patient privacy is also a

concern when patients have interactions with care providers in locations that do not have the privacy of, say, the traditional doctor's examination room, e.g., in the workplace or at telehealth locations in more public locations such

as pharmacies. Security refers to the technical safety of the network against fraud or hackers (Surjadjaja et al., 2003). Given recent data breaches in the health sector, network security has become a primary concern. Thus, a high level of security, characterized in part by encryption, authentication, and controlled access, to protect health-care data is necessary and critical for mobile telehealth (Varshney, 2007).

Remote monitoring of patients leads to a range of privacy risks, some of which are unintended. For example, sensors in a patient's home or body to detect falls may unwanted transmit information such as absence of people at home or private interactions with other household subjects (Hall, 2014). More generally, privacy concerns regarding the following need to be addressed for any remote monitoring of patients that may be part of telehealth services: recording or monitoring of patients and how those recordings and other patient information are maintained and transferred (Demiris et al., 2009). Demiris et al. (2009) propose that informed consent is one critical element for telehealth success. They propose that informed consent should be viewed as an ongoing process rather than a one-off event. Ensuring patient privacy by various stakeholders in the patient care process (not just caregivers), such as family members, is also necessary for privacy. The World Medical Association states that informed consent for telemedicine patients should cover at least the following:

- "explaining how telemedicine works,
- how to schedule appointments,
- privacy concerns,
- the possibility of technological failure including confidentiality breaches,
- protocols for contact during virtual visits,
- prescribing policies and coordinating care with other health professionals in a clear and understandable manner, without influencing the patient's choices." (Word Medical Association, 2018).

The requirements for patient privacy are the same under (Health Insurance Portability and Accountability Act of 1996), HITECH (Health Information Technology for Economic and Clinical Health), and the COPPA (Children's Online Privacy Protection Act) (Balestra, 2018). Two HIPAA rules need particular attention by telehealth providers—the Privacy Rule and the Security Rule. The Privacy Rule requires the protection of patient's medical records and related health information. Notably, entities covered by HIPAA "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." (45 CFR § 164.530c). With regard to what specific safeguards are necessary is left up to the covered entities thus providing flexibility and technological neutrality in how telehealth providers comply with the Rule.

Further, under HIPAA, the Security Rule focused more specifically on patients electronically stored, protected health information by having safeguards in place. Specific measures or technologies are not mandated, thereby providing covered parties with flexibility in meeting the rule. Having said that, common security measures for protecting health information include: passwords; digital signatures; data encryption; encryption over public networks; backup systems; and disaster recovery plans (Kumekawa, 2001).

To ensure HIPAA compliance telehealth providers should ensure that their own systems are compliant, and also conduct due diligence of third party suppliers–who should ideally have undergone independent audits by cybersecurity risk management advisors American Physical Therapy Association (2019).

New Technologies Risks

The Internet of Things (IoT) uses many new, state-of-the-art technologies. Many such technology applications may not always have been tested for scalability, security, and availability. The integration with other software products, existing systems and new systems will expose the integrated system's vulnerabilities. Such vulnerabilities may highlight unique risks caused specifically by integration. increased networking, mobility, and telecommuting have introduced serious technical issues and potential security problems (Dillon & Pate-Cornell, 2005). Fundamentally,

the Internet and its infrastructure, system access, security, open standards, information access, reliance, integrity of data and information, complexity, interdependence, and interconnectivity, all lead to risks (Vaidyanathan, 2007).

In many developing countries, brick and mortar rural care centers are used as the patient-doctor interface. This is due to limited Internet access in rural areas as well as the preference of patients to interact with trained and reliable

healthcare professionals. The transformation to telehealth in such regions of the world is very attractive, yet it comes with its own risks. For example, the rapid proliferation of cellphone usage in remote parts of the world opens up tremendous opportunities for mobile health systems. The reliability of Internet as well as security of patient data are very vulnerable to hijack and denial of services.

The University of Arizona recently promulgated a few concerns of telehealth and proposed how to overcome those concerns (Varshneya, 2018). Those general concerns include:

- Reimbursement problems for healthcare professionals after providing telemedicine services,
- Lack of integration of Electronic Health Records (HER) with varied telehealth services platforms,
- Continuity problems when patients move from one healthcare provider to another,
- Lack of technology savviness of patients.

Other risks and issues of telehealth include:

- Complexity of telemedicine equipment interfaces;
- Ease of use and usability of use of telemedicine equipment;
- Prevalence of multiple technical standards;
- Interoperability of new wireless technologies and standards;
- Integration of applications with traditional workflows;
- Scalability; and
- Training in the use of existing or new technologies.

Fulfillment Risks

Fulfillment refers to the delivery of healthcare services in real time and, as specified, within a service level agreement (Surjadjaja et al., 2003). Order fulfillment risks (such as lost orders, delivery delays, and shipments of incomplete orders) can be detrimental to patient healthcare. In telehealth, the integration of front-office and back-office operations with the supply chain may pose a lack of integrated fulfillment systems and create risks. Inefficient fulfillment integration with external distribution providers such as pharmacies, test labs, and diagnostic labs may also expose risks. The internal factor that threatens the new fulfillment needs is supply-chain management while the external factor that threatens the fulfillment is the real-time demand for healthcare services.

Telehealth may result in the emergence of new fulfillment services that may disturb existing ones and involve several adjustments for healthcare organizations, such as additional investments and resources. This may lead to the risk of fragmentation of services. Telehealth implementation may lead to disruption of fulfillment services due to changes in the responsibilities of providers in the supply chain (Alami et al., 2019).

A recent trend in the pharmaceutical industry is the global sourcing of both active and inactive low-cost ingredients from developing countries. Moreover, the manufacture of generic drugs has been outsourced to companies in developing countries. In general, the supply chain that includes sourcing, manufacturing, packaging, logistics, and distribution from remote corners of the globe has increased the risks of contamination or substitution of alternative ingredients (Marucheck et al., 2011).

Counterfeiting and contamination occurs in the production of drugs for economic gain. Counterfeiters may use none or incorrect amounts of the active ingredient and then make up the drug with impurities or even harmful substances thereby creating a risk to a patient with harmful side effects or no treatment at all (Marucheck et al. 2011).

Secondary distribution channels of the supply chain may pose safety risks. During distributors, the effectiveness of drugs due to lack of proper storage and warehousing areas may pose risks to patients.

Socioeconomic Risks

The main attributes of the socioeconomic dimension of telehealth are access to services; cost of services, decreased health service use, support activities, quality of care, and quality of life. There are risks associated with the socio-economic aspects of telehealth. Generally, there is an absence of national or international e-healthcare policy and regulations and this will pose legal and economic risks to both patients and healthcare providers. A comprehensive

and national strategies regarding remote healthcare are also non-existent. The lack of insurance appears to remain a barrier even when using telehealth care. The requirements of access of patients who are in dire need for healthcare may not be addressed by telehealth (Lee et al., 2019). The other risks are contributed by factors such as diagnosing patients without physically examining them and not able to communicate effectively through an electronic medium.

The cost of implementation of telehealth seems to be prohibitive and not affordable in many under-developed countries (Meso, Mbarika, & Sood, 2008). Currently, reimbursement for telehealth is limited and healthcare organizations must develop solutions with the appropriate local, state and federal agencies (Donohue, 2016).

CONCLUSIONS

We have presented a new framework for telehealth delivery. The framework presented in this paper discusses the fundamental basic risks of telehealth. Those risks are supported by various scholars in current literature. In this paper, we have discussed six major dimensions including confidentiality risks, business model risks, ethical risks, technology risks, fulfillment and socioeconomic risks. The identified risks in this paper relates to the overall failure in an introduction of an information system which is correlated with the pattern of its implementation. Project success —which is different than project management success—depends on legal, relationships, cost, resources, politics, communications, value, and customer satisfaction (Vaidyanathan, 2013). The implementation of telehealth or any IT project depends heavily on the mitigation of its project risks (Vaidyanathan, 2013). Culture-specific beliefs and values also influence the process of implementation (Meso et al., 2008). Apart from the usual project management risks, various idiosyncratic risks are identified in this paper.

A potential advantage of telehealth is improving overall access to care and access to specialized care—particularly in countries such as the US where this access is unevenly distributed (Garcia et al., 2015). However, for this to occur, various risks in telehealth delivery need to be recognized and managed. The framework we developed in this article can help us understand the various risks involved in the delivery of telemedicine. Notably, the conceptual framework presented here examines risk from six critical dimensions: new business models; legal and ethical considers; patient privacy and data security; new technology; fulfillment; and socioeconomics.

Future research on the telehealth models may be focused on the following issues:

- How do we operationalize the measurement of telehealth delivery?
- How do we operationalize the measurement of each of the six dimensions of the telehealth model?
- How do each of the six risks identified in the telehealth model influence telehealth delivery satisfaction, both individually and in terms of how they interact with one another?

REFERENCES

American Academy of Family Physicians (2020). What's the difference between telemedicine and telehealth? Retrieved from https://www.aafp.org/media-center/kits/telemedicine-and-telehealth.html on April 3, 2020.

Alami, H., Gagnon, M. P., & Fortin, J. P. (2019). Some multidimensional unintended consequences of telehealth utilization: a multi-project evaluation synthesis. *International journal of health policy and management*, *8*(6), 337.

American Physical Therapy Association (2019). "Telehealth Ethics, Best Practice, and the Law: What You Need to Know", August 28, 2019. Retrieved from http://www.apta.org/Blogs/PTTransforms/ 2019/8/28/Telehealth/ on May 9, 2020.

Ashwood, J. S., Mehrotra, A., Cowling, D., & Uscher-Pines, L. (2017). Direct-to-consumer telehealth may increase access to care but does not decrease spending. *Health Affairs*, *36*(3), 485-491.

Ba, S., & Paulou, P. A. (2002). Evidence of the effect of trust in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, *26*(3), 243-266.

Balestra, M. (2018). Telehealth and legal implications for nurse practitioners. *The Journal for Nurse Practitioners*, *14*(1), 33-39.

Berg, M. (1999). Patient care information systems and health care work: a sociotechnical approach. International *Journal of Medical Informatics*, *55*(2), 87-101.

Biswas, D., & Biswas, A. (2004). The diagnostic role of signals in the context of perceived risks in online shopping: Do signals matter more on the web? *Journal of Interactive Marketing*, *18*(3), 30-45.

Cox, D.J., Plavnick, J.B., & Brodhead, M.T. (2020). A Proposed Process for Risk Mitigation During the COVID-19 *Pandemic. Behavior Analysis Practice*, *13*(2), 299–305.

Demiris, G., Doorenbos, A. Z., & Towle, C. (2009). Ethical considerations regarding the use of technology for older adults: The case of telehealth. *Research in gerontological nursing*, *2*(2), 128-136.

Dillon, R. L., & Pate-Cornell, M. E. (2005). Including technical and security risks in the management of information systems: A programmatic risk management model. *Systems Engineering*, *8*(1), 15-28.

Donohue, J. (2016). Telemedicine: What the future holds. Healthcare IT News, Retrieved from https://www.healthcareitnews.com/blog/telemedicine-what-future-holds on May 8, 2020.

Federal Communications Commission (2020). Telehealth, Telemedicine and Telecare: What's What? Retrieved from https://www.fcc.gov/general/ telehealth-telemedicine-and-telecare-whats-what on May 8, 2020.

Fonda, D. (2020). Coronavirus has ushered in the digital revolution in medicine. *Barron's.* April 17, 2020.

Gagnon M, Lamothe L, Fortin JP, Cloutier A. (2005). Telehealth adoption in hospitals: an organizational perspective. *Journal of Health Organization Management*, *19*(1), 32–56.

Garber, K. M., & Chike-Harris, K. E. (2019). Nurse Practitioners and Virtual Care: A 50-State Review of APRN Telehealth Law and Policy. *Telehealth and Medicine Today*, *4*, 10-30953.

Garcia, L. R., Silva, E., & Terra, J. C. C. (2015). A comparison of telehealth programs between the USA and Brazil: a legal perspective. *Smart Homecare Technology and TeleHealth*, *3*, 139.

Grover, V., & Saeed, K. A. (2004). Strategic orientation and performance of Internet-based businesses. *Information Systems Journal*, *14*(1), 23-42.

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.

Interstate Medical Licensure Compact (2020). "General FAQs about the Compact", Retrieved from https://www.imlcc.org/a-faster-pathway-to-physician-licensure/ on May 9, 2020

Kaiser, T. (2002). The customer shall lead: E-business solutions for the new insurance industry. *The Geneva Papers on Risk and Insurance, 27*(1), 134-145.

Kizilova, N. (2018). Review of emerging methods and techniques for arterial pressure and flow waves acquisition and analyses. International Journal of Biosensors & Bioelectronics, 4(4), 179-187.

Kumekawa, J. (2001). Health information privacy protection: Crisis or common sense? *Online Journal of Issues in Nursing, 6.* Retrieved from http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ ANAPeriodicals/ OJIN/TableofContents/Volume62001/No3Sept01/PrivacyProtectionCrisis.html on May 9, 2020

Lange, S. K., Davis, J. K., Jaye, D., Erwin, D., Mullarney, J. X., Clarke, L. L., & Loesch, M. C. (2000). *E-Risk: Liabilities in a wired world.* Cincinnati: The National Underwriter Co.

Lee, S., Black, D., & Held, M. L. (2019). Factors associated with telehealth service utilization among rural populations. *Journal of health care for the poor and underserved*, *30*(4), 1259-1272.

Magretta, J. (2002). Why Business Models Matter? *Harvard Business Review,* May 2002, 1-8.

Mercuri, R. T. (2005). Trusting in transparency. *Communication of the ACM, 48*(5), 15-19.

Meso, P., Mbarika, V. W., & Sood, S. P. (2008). An overview of potential factors for effective telemedicine transfer to Sub-Saharan Africa. *IEEE Transactions on Information Technology in Biomedicine, 13*(5), 734-739.

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM,* 48(3), 86-91.

Marucheck, A., Greis, N., Mena, C., & Cai, L. (2011). Product safety and security in the global supply chain: Issues, challenges and research opportunities. *Journal of Operations Management*, *29*(7-8), 707-720.

Orr, B. (2005). Identify fraud, round two. *ABA Banking Journal,* 97(6), 64-65.

Pathak, J. (2004). A conceptual risk framework for internal auditing in e-commerce. *Management Auditing Journal, 19*(4), 556-564.

Pereira, F. (2017). Business models for Telehealth in the US: analyses and insights. *Smart Homecare Technology and Telehealth, 4*, 13-29.

Pirtle, C. J., Payne, K., & Drolet, B. C. (2019). Telehealth: Legal and Ethical Considerations for Success. *Telehealth and Medicine Today*. Retrieved from https://telehealthandmedicinetoday.com/index.php/journal/article/ download/144/174?inline=1 on May 9, 2020.

Pittman, D. (2016). Major insurer adds telemedicine in Medicare Advantage plans. Retrieved from https://www.politico.com/tipsheets/morning-ehealth/2016/01/politicos-morning-ehealth-telemedicines-use-in-medicare-advantage-biden-talks-tumor-sequencing-and-data-onc-faca-talks-ehr-tool-212103 on April 18, 2020.

Pramanik, P. K. D., Pareek, G., & Nayyar, A. (2019). Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. In *Telemedicine Technologies* (pp. 201-225). Academic Press: Cambridge, MA.

Smith D. (2005). The influence of financial factors on the deployment of telemedicine. *Journal of Health Care Finance, 32*(1), 16–27.

Straub, D., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Surjadjaja, H., Ghosh, S., & Antony, J. (2003). Determining and assessing the determinants of e-service operations. *Managing Service Quality, 13*(1), 39-53.

Uscher-Pines, L, & Kahn M. (2014). Barriers and facilitators to pediatric emergency telemedicine in the United States. *Journal of eHealth*, *20*(11), 990–996.

US Department of Veterans Affairs (2020). "VA Expands Telehealth by Allowing Health Care Providers to Treat Patients Across State Lines" Press Release, May 11, 2018, Retrieved from https://www.va.gov/opa /pressrel/ pressrelease. cfm? id=4054 on May 9, 2020.

Vaidyanathan, G. (2013). *Project Management: Process, Technology, and Practice.* Pearson: Upper Saddle River, NJ.

Vaidyanathan, G. (2007). E-Business risk management in firms. In *E-Business Processes: Technologies and Solutions.* Eds. Jayavel Sounderpandian and Tapen Sinha. IDEA Group Inc.: Hershey, PA.

Vaidyanathan, G. & Devaraj, S. (2003). A five-factor framework for analyzing online risks in E-Businesses. *Communications of the ACM, 46*(12), 354-361.

van Limburg, M., van Gemert-Pijnen, J. E., Nijland, N., Ossebaard, H. C., Hendrix, R. M., & Seydel, E. R. (2011). Why business modeling is crucial in the development of eHealth technologies. *Journal of medical Internet Research, 13*(4), 124.

Varshney, U. (2007). Pervasive healthcare and wireless health monitoring. Mobile Networking Applications. *12*, 113–127.

Varshneya, R. (2018). 7 Telemedicine Concerns and How to Overcome Them. Retrieved from https://telemedicine.arizona.edu/blog/7-telemedicine-concerns-and-how-overcome-them on April 18,2020.

Yang, T. (2016). Telehealth Parity Laws: Health Policy Brief. Retrieved from https://www.healthaffairs.org/ do/10.1377/hpb20160815.244795/full/healthpolicybrief_162.pdf on April 18, 2020.