# Telehealth Security from a Patient's Perspective: A Study of Cyber Hygiene in a Health-Specific Context

**Early stage paper**

**Gargi Nandy**
University of Nebraska,
Omaha
gnandy@unomaha.edu

**Dr. Deanna House**
University of Nebraska,
Omaha
deannahouse@unomaha.edu

## ABSTRACT

The move to telehealth during the COVID-19 pandemic provided a needed platform with innumerable benefits in terms of safe delivery and continuity of care for patients. This necessity fueled the rapid growth of telehealth-related technology and its use in the healthcare sector. During this expedited move, considerations related to cybersecurity were not prioritized. This introduced additional vulnerabilities to be exploited by malicious actors. This research focuses on the traditionally un-protected and vulnerable end-user: the patient. Telehealth security and privacy research from the perspective of the patient has been relatively unexplored, as the majority of the research has focused on the providers and regulatory requirements for security and privacy that fall under the protection of HIPAA. Patient personal devices are frequently vulnerable to threats due to a lack of cyber-hygiene on the part of the user. This early stage research will provide insights related to telehealth security and privacy challenges faced by patients, protective mechanisms for personal devices, and recommended protective practices that can be utilized by patients.

## *Keywords*

Telehealth, patient, information security, personal devices, TTAT.

## INTRODUCTION

At the onset and throughout the COVID-19 pandemic, telehealth has seen a sharp rise in usage (Koonin, et al., 2020)(HHS.gov, 2021) across the US. The necessity for continuity of care paired with the health, safety, and reduced risk to patients and providers were huge drivers for the push to telehealth. As mentioned by (Benziger et al, 2020), telehealth can help balance the need for outpatient care with consideration for both individual and public health risks. Facilities were shut down for routine care and elective surgeries, which prompted a change in healthcare delivery methods. As mentioned by Marx & Padmanabhan (2020), two of the greatest barriers to telehealth advancement were lifted – reimbursement for telehealth visits that are now similar to those of in-person and the requirement for clinician licensing for every state that they were seeing patients. However, the relaxed regulatory requirements also opened up the potential for security debt (Defcon, 2021). Around 76% of US hospitals are currently using this mode of communication to connect with patients through video conferencing or remote monitoring (American Hospital Association (AHA), 2019).

With the rapid increase in usage of telehealth, the healthcare sector has become an attractive and easy target for hackers. According to a report published by the Health Sector Cybersecurity Coordination Center (HC3), cyber-attacks in health care rank first among the other industries in United states due to the sensitive nature of the health-related data (IBM Security, 2021; HHS Cybersecurity Program, 2020). Protection against these cyberthreats is very important as it may result in loss of lives when health care facilities are targeted. While at the present time this is not a common occurrence, a landmark 2020 ransomware attack on Dusseldorf University Hospital caused patients to be relocated and resulted in one death (HHS Cybersecurity Program, 2022).

The healthcare industry is unique in that there are regulatory requirements that fall under the realm of cybersecurity and privacy specific requirements for protecting health-related data (such as HIPAA). These requirements provide a minimum standard for protecting private health information from the providers' perspective. However, telehealth introduces another potential attack vector, the patient. Due to its nature, patients are frequently using personal devices and home networks when communicating with providers during telehealth visits (Defcon, 2021). This is concerning as many cyber-attacks are related to the inability of an individual in understanding and maintaining cyber-hygiene (Gately, 2019). The rush to move towards telehealth during the COVID-19 pandemic has undoubtedly increased challenges related to security and privacy (such as discussed by Plachkinova et al, 2015; Patel et al., 2021; Willis et al. 2021).

This research focuses primarily on telehealth in the United States and attempts to understand and evaluate security and privacy risks associated with personal devices (including mobile, desktop, tablets, and laptop) on home networks when used by patients for telehealth visits. As mentioned by (Xu, Wang, & Jia, 2016) devices that are connected to routers with poorly maintained security standards can be exploited easily by cyber attackers.

Hence, we hope to gain insight on aspects that can influence patients' behavior when utilizing telehealth and the influences that cyber hygiene and apathy can have on behavior. This study will provide useful perspectives on patients' cyber awareness and determine mechanisms to improve behavior in order to mitigate cyber intrusions/attacks. A review of the literature surrounding telehealth and security follows.

# LITERATURE REVIEW

Research surrounding telehealth has been sporadic at best, with a vast majority housed within medical journals and written from the perspective of medical practitioners. While there is prior telehealth research within the information systems discipline, the research specific to security from a patient's perspective has been lacking. Additionally, a variety of terms have been utilized under the umbrella of telehealth.

## Variations of Telehealth

Telehealth can be considered a very broad area of healthcare. According to the Health Resource Services Administration (HRSA), telehealth uses digital technologies to deliver cost effective medical care, health education, and public health services to the wide variety of populations anytime (HealthIT, 2019). While this term has been used in research to include a number of different meanings, it is important to first understand the various terms used in telehealth and telemedicine.

The term telehealth is often used interchangeably with telemedicine but in reality, it is much broader in concept than other terms like telemedicine, m-health, remote-health, and e-health. Telehealth is an umbrella term that comprises of all the above listed terms (CDC, 2019; Rutledge et al. 2017). The Health Resources and Services Administration (HRSA) defines telehealth as "the use of electronic information and telecommunication technologies to support long-distance clinical health care, patient and professional health-related education, health administration, and public health" (Health Resources & Services Adminsitration, 2021).

The section below will attempt to explore the different terms so that a clearly defined term for telehealth can be defined. There are many terms in this area which are interlinked to each other but hardly any clear definition exists. Figure 1 below shows a detailed outline of telehealth and its variations.

### Telemedicine

The history of telemedicine goes back to 1950s and early 1960s when closed-circuit television link was used to for psychiatric consultations between the Nebraska Psychiatric Institute and Norfolk State Hospital (NCBI, 2012). Telemedicine is the subset of telehealth which can be defined as the use of digital technologies used by the doctors to provide preventive treatment and care to the patients at a distance to improve their health condition (Haleem, Javaid, Singh, & Suman, 2021). In fact, delivering health care services through telemedicine helps the patients save an average travel of 145 miles and 142 minutes per visit (Russo, McCool, & Davies, 2016). The overall aim of telemedicine is to improve patient care by providing health-care services to a wide variety of population (irrespective of sex, race, ethnicity, and financial status) from a distance with reduced health-care costs (Moghadas, Jamshidi, & Shaderam, 2008). Ancillary telemedicine services include 1) remote patient monitoring, 2) consultative visits, and 3) facilitated virtual visits (Baker & Stanley, 2018).

### E-Health and M-Health

The terms electronic health and mobile health have gained popularity in the health care sector. Although both e-health and m-health fall under the digital health category, there is a significant difference between them. Generally, e-health refers to the use of ICT (Information and Communication Technology) to maintain health records and healthcare which may involve the use of desktops and laptops while m-health refers to the use of mobile wireless technologies to maintain and monitor health and health records (Leung & Chen, 2019); (Agarwal et al. 2016). The global size of m-health is expected to reach 247 billion dollars by 2025 (Statista, 2018).

### Remote Patient Monitoring (RPM)

RPM (Remote Patient Monitoring), also referred to as physiologic monitoring, can be defined as the use of modern technologies to monitor health conditions of the patients remotely. Constantly capturing and monitoring the patient's health data helps the health care professionals to better assess the current health condition of the patients (National Institute of Standards and Technology: US Department of Commerce, 2022). To prevent serious health complications, healthcare providers recommend the use of RPM. Some examples of health conditions that could necessitate RPM are – high blood pressure, weight management, diabetes, heart conditions, and many other chronic illnesses such as chronic obstructive pulmonary disease or coronary heart disease which require regular monitoring (TELEHEALTH.HHS.GOV, 2022). The use of RPM is very convenient and cost-effective.

### Facilitated Virtual Visits (FVV)

Another variation of a "live synchronous telemedicine visit" is referred to as Facilitated Virtual Visit (FVV). In this form of visit, the patient is located at an access site which may be a clinic which is well equipped with diagnostic tools whereas the medical provider examining the patient is located at a distance (Mechanic, Persaud, & Kimball, 2017).

### Consultative Visits

There is thin line that differentiates consultative visits from facilitated visits. In case of consultative visits, there are no diagnostic tools involved during the visit and instead synchronous conversation takes place via a video conferencing platform (Baker & Stanley, 2018). These are easy to carry out as no compliant medical devices are involved and patient can avail the health-care services and health assessments by their health care providers from their home premises. Consultative visits can be further classified into two sub-categories 1) teleconsultation 2) direct to consumer.

### Teleconsultation and Direct to Consumer

Teleconsultation and direct to consumer are often confused to be same but a significant difference exists between them. Teleconsultation is a type of visit where health care providers located at different sites interact with each other regarding the patient. On the other hand, in the case of direct to consumer, the interaction happens between the health care provider and the patient seeking medical advice (Baker & Stanley, 2018). Direct to consumer is often referred to as "at home" telehealth service where patient can use their personal devices for consultation and has two modes of delivery 1) synchronous - where the patient uses phone or video consultation to interact with the provider and 2) asynchronous – where the patient and the provider interact initially using form or pre-recorded information. The provider can look at the submitted information to diagnose and prescribe medications later/after submitted/recorded. This type of health care delivery is also known as "store-and-forward" (Telehealth.hhs.gov, n.d.).

## PRIVACY AND SECURITY REVIEW

### HIPAA Review

HIPAA (Healthcare Insurance Portability and Accountability Act) is a governing body, established in 1996, that is responsible for creating national standards for protecting and preventing PHI (Protected Health Information) of patients from being disclosed without patients' consent . The HIPAA security rule is responsible for protecting the confidentiality, integrity, and security of ePHI (electronic Protected Health Information) of the patients. Specifically, protecting the PHI that is in electronic format (Center for Disease Control and Prevention, 2018). Figure 2. shows the entities that fall under HIPAA jurisdiction. The definitions of the entities are listed in table 1. As mentioned by (Bassan, 2020), the scope of HIPAA is limited to the covered entities (that includes health plans, healthcare clearinghouses and health care providers) and the business associates (that includes third party vendors) that deal with the PHI of the patients. However, when personal devices and home networks of the patients are involved to store or process PHI, they are not covered under HIPAA. Hence the specifics surrounding patient data from home networks/the patient side may be less regulated and are subject to relaxed standards.

During the pandemic there were and are ongoing travel restrictions and instances of lockdowns in many places in the world. These issues have created challenges related to available healthcare options and have led to people opting to use virtual care options. To ease technology challenges in the US, The Department of Health and Human Services Office for Civil Rights (HHS OCR) lifted some restrictions on the current HIPAA-compliant technologies to be used for communications. The reduced restrictions were necessary for continuity of care which increased the dependency on telehealth. According to the "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency", health care providers are free to use video chat applications like Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, and Skype and text-based applications like Signal, Jabber, Facebook Messenger, Google Hangouts, WhatsApp, and IMessage. No penalties will be imposed as long as it is conducted under "good faith provision" (HHS.gov, 2021). These relaxations have indeed helped both the patient/user and the providers to a great extent but have raised questions on the security and privacy risk. For example, if a doctor conducts a video conferencing with a patient using Facebook messenger video chat, the health information exchanged during the conversation will not be regulated under HIPAA and instead will fall under Facebook's privacy and security policy. Additionally, technologies are being used in a multi-purpose context to include business, personal, and healthcare specific. Cybersecurity requirements vary greatly in these contexts.

### Threat Landscape

There has been a recent rise in cyber-attacks in the healthcare industry more significant than in any other industry. The average cost of a data breach in the healthcare industry in 2021 in the US is close to $9.23 million with $4.62 million dollars alone as the average cost of ransomware breach (IBM Security, 2021). A key reason the health care industry is a prime target is due to the monetary value, up to $250 per health record (Taylor, 2022). They are ten times more valuable than credit card information and can be used to create a new bank account, obtain credit card, passports or it may also be used to steal the identity of the person. In many cases health records can be used for political purposes to cause collateral damages. For instance, the database of the World Anti-Doping Agency was compromised, and sensitive data of athletes were made public (Coventry & Branley, 2018).

According to the U.S. Department of Health and Human Services Office for Civil Rights (HHS OCR), there have been many reported cyber-attacks throughout the COVID-19 pandemic and many of them are related to phishing, ransomware attacks, and unauthorized disclosure of data (Services, 2021).

As mentioned by (Hall & Deven, 2014), telehealth services can be viewed as a bidirectional road where one has lack of control and visibility. Healthcare practitioners maintain EHR (Electronic Health Records) of their patients to provide telehealth visit facilities when needed (Carlson &

Goldstien, 2020). These records are very sensitive as they contain patient SSN (Social Security Number) patient demographics, lab results, insurance details, medical histories, diagnosis, medication record, immunization dates and any allergies (HealthIT, 2019; Coventry & Branley, 2018). This health information can be exploited by the threat attackers to conduct fraudulent activities like insurance fraud, identity theft, or extortion (NIST SPECIAL PUBLICATION 1800-30, 2022).

Telehealth being a bidirectional workflow, empowers the healthcare provider by enabling them to treat patients faster, operating within a secured perimeter. However, once outside of the secured perimeter/network this can increase the risk of a security threat to the patient's information in the use of personal devices and networks (with potential low security standards) for telehealth visits. Hence it is important to be mindful of the fact that we must be extremely careful when dealing sensitive health-related information.

### Use of Unsecured Network & Devices

Unsecured remote environments (such as those that are utilized by patients during telehealth visits) play a significant role in allowing cyber-attacks to occur. They are the most attractive target for hackers. Many home users are negligent of the fact that their home network is susceptible to attack. They believe that either they have a secure home network, or it is too small to be at risk (Cybersecurity & Infrastructure Security Agency, 2020). This is concerning for the patient, as mobile and home devices are frequently unpatched and susceptible to malware and other exploits (Hall & Deven, 2014; Dempsey, et al, 2018). People living in remote areas have very limited knowledge on maintaining cyber-hygiene, which leads to less secured home networks (including weak/no WIFI password) (Wang & Alexander, 2021).

Often people use the same passwords repeatedly to avoid the complexity of keeping track of multiple passwords and hence open up an area of vulnerability for the hackers (Esparza, Walters, & Caporusso, 2020). Having poor cyber-hygiene and a lack of security increases the chances of cyberattacks like ARP spoofing, IP spoofing, MAC spoofing, Cache spoofing and DDoS attacks. Some of the attacks like Cache spoofing are easily spread through a network connection and can disrupt the entire system (Mandal & Khan, 2020). As mentioned by Thompson, McGill, & Wang (2017), personal devices pose a greater threat as the users either have limited technology knowledge or lack of self-awareness on security risk. Once the end user's device is involved there are grey areas related to data and device that are still being sorted out.

Mobile devices, while convenient, can be just as vulnerable as a computer or laptop. Cyber-criminals can use sophisticated software tools to gain access to user's cell phone and compromise data (United States Government Accountability Office: GAO-12-757, 2012). As mentioned by (Friedman & Hoffman, 2008), mobile devices can be at risk of loss/theft, they utilize wireless communications, operating system are not frequently updated, and they operate outside of normal protective perimeters. Research by Thompson, McGill, & Wang (2017) found that mobile users' perceived severity of an attack or damage to their device had a significant relationship with the inability of the individual to protect their device.

Android and iOS mobile operating systems are both under attack. iOS and Apple zero-day vulnerabilities have been more frequently happening, with several in 2021 (Naraine, 2021). A zero-day vulnerability can be defined as the security flaw in the given hardware, software or firmware without the vendor knowing about it (NIST, n.d.). Several critical Google Chrome browser vulnerabilities, tracked as CVE-2022-1096 and CVE-2022-1232 hit the news headlines recently. These kinds of flaws can easily be exploited by threat actors and could give easy access to victim devices (Avertium, 2022). As mentioned by Roumani (2021), a zero-day vulnerability increases the exploitability risk by the attackers as there is frequently a slight delay in releasing the patch which can cost more than expected.

### Technology Threat Avoidance Theory (TTAT)

Understanding the human elements that impact cyber hygiene is very important and critical. Studies from prior studies suggested that technology alone can't fight against cyber-attacks and emphasized the importance of evaluating the human aspect of security (Woon, Tan, & Low, 2008; Workman, Straub, & Bommer, 2008).

We derive our research model from the Technology Threat Avoidance Theory (TTAT). The theory states that the individuals' understanding regarding possible technology threats is directly proportional to their awareness of the threats, which, in turn, impacts their motivation and behavior to avoid them (Liang & Xue, 2010). The original model proposed by (Liang & Xue, 2010) included the following constructs- perceived susceptibility, perceived severity, perceived threat, safeguard cost, self-efficacy and their overall impact on avoidance motivation and avoidance behavior from the context of user's security behavior. While TTAT is an important theory, this research aims to extend the framework to address important key areas of motivation that can have an effect on behavior and explore the unique context of telehealth.

The following subsections provide more detail related to the constructs from TTAT along with other important areas that can affect human motivation.

### Perceived Vulnerability

Perceived vulnerability can be defined as the individual's belief on the likelihood of any IT threat happening. Research by Sheppard et al. (2013) emphasized that 'cyber-hygiene mentality' depends on an individual's perception towards it.

### Safeguard cost

Safeguard cost can be defined as the efforts required (including time and money) to implement safeguarding measures. Users tend to follow safer practices only when benefits associated with it are more and overall maintenance cost is less (Fagan & Khan, 2016). Often this creates a barrier which reduces the overall motivation to act against any IT threats. People tend to perform cost-benefit analysis before they tend to take any actions. As mentioned by Woon et al. (2008), if the cost associated with network security is too high, there is a greater likelihood that users will opt out of it.

### Self-efficacy

In the security context, self-efficacy can be referred as the individual's confidence in their ability to apply necessary preventive measures to protect from being victimized to cyber-attacks (Liang & Xue, 2010). Often self-efficacy is considered as one of the most important outcomes of security education that is likely to influence an individual's confidence level (Verkijika, 2021).

### Avoidance motivation and avoidance behavior

Avoidance motivation can be defined as the individual's intention to take necessary steps to protect themselves from any cyber-attacks (Liang & Xue, 2010). As mentioned by (Stanton et al., 2005) maintaining good password practices is related to an individual's security training, awareness, monitoring, and motivation.

### Apathy

Apathy has also been found to be a strong determinant influencing human behavior. Studies related to apathy such as Ang et al. (2017) have explored the role of apathy in healthy individuals; particularly its role in motivation. Apathy can be defined "as a quantitative reduction of goal-directed activity in comparison to the patient's previous level of in multiple dimensions including behavior/cognition, emotion and social interaction" (Fahed & Steffens, 2021). For instance, the practice of reading user policies is essential but sometimes users fail to do so as they either have no interest in reading them or belief that it is not applicable to them (Foltz, et al. 2008).

### Cyber Hygiene

In general, cyber hygiene is the sequence of steps or the practices that must be followed during an online activity to ensure the safety and security of users and devices. Table 2 below provides various definitions of cyber hygiene from the literature.

| Definitions of Cyber Hygiene (CH) | Source |
|---|---|
| Cyber hygiene can be defined as the knowledge of concepts, threats, and the behaviors of the users towards the topic that includes security software, authentication, phishing scams, social networking, web-browsing, WI-FI hotspot usage, and USB drive use. | Cain, Edwards, & Still, 2018 |
| Cyber hygiene are common practices that need to be undertaken by individuals when browsing the internet to protect their devices and their personal information online | Laws, Nowatkowski, Heslen, & Vericell, 2018 |

| | |
|---|---|
| Cyber hygiene can be considered as the "adaptive knowledge and behavior" that one should undertake during online activities to protect their social, financial, and personal information. | Neigel, Claypoole, Waldfogle, Acharya, & Hancock, 2020 |
| Cyber hygiene can be defined as the implementation and enforcement of the common security practices, policies , procedures, and controls that are in place to minimize the chances of getting breached by an intruder. | Kirkpatrick, 2015 |

**Table 2: Definitions of Cyber Hygiene**

Often cyber-attacks are related to the inability of an individual to understand cyber space and threats that may arise due to lack of cyber awareness (Cain et al. 2018). A well-known attack in the history of cyber breaches is the WannaCry ransomware attack. In May 2017 Microsoft Windows operating systems were targeted (including windows 8, 2003 and XP) with nearly 100,000 organizations affected around the globe. The main reason behind the attack was due the fact that individuals in organizations did not update their operating system and were using an outdated one (Thomas, 2018). Humans are the first line of defense but unfortunately remain the weakest link in the cyber space due to their behavior towards cyber hygiene (Zwilling et al. 2022; Kelley, 2018).

Research by Viswanath, et al. (2020) demonstrated that cyber hygiene is a multi-dimensional concept and is impacted by three aspects – 1) the user's self-belief about technology 2) users cognitive processing and 3) online activities. Often hackers target users from different professional backgrounds. Cain, Edwards, & Still (2018) found that the users from IT sectors are targeted more frequently. Cyber security breaches create a huge loss not only at the organization level but at the individual user level too. Thus, the increase in personal device usage in healthcare have moved the importance for research such as this, to the foreground. The use of untrusted networks and personal devices with low security standards can create a catastrophic situation for the users.

## RESEARCH QUESTIONS

Many of the research perspectives on cyber hygiene have been previously explored from a provider and facility viewpoint. There is a dire need for an information systems and cybersecurity lens to explore security and privacy risks, threats, and vulnerabilities from the patient's end when using personal devices with low security standards (i.e. following poor cyber hygiene practices). Therefore, our research questions are as follows:

RQ1: Which factors have a significant impact on a patient's motivation to avoid cyber-attacks during telehealth (direct-to-consumer) visits?

RQ2: Do age and gender of an individual affect avoidance motivation?

RQ3: Does cyber hygiene strengthen the relationship between avoidance motivation and avoidance behavior?

## RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

For our study, we have derived our model from the original TTAT model, where we are focusing on the following constructs – perceived vulnerability, safeguard cost, apathy, self-efficacy and their overall impact on the avoidance motivation, cyber hygiene practices and avoidance behavior. We have added apathy as an additional construct to the original TTAT model as studies suggest that apathy plays a significant role in driving the motivation of the people (Foltz et al. 2008). Additionally, an important facet of motivation is the impact of the above human elements on cyber hygiene and the negative impact it can have on telehealth visits (specific to direct-to-consumer) in terms of cyber threats.

Discussion of the hypotheses follows.

Previous study by (Liang & Xue, 2009) show that human perception towards perceived threat is directly influenced by two precursors: perceived vulnerability and perceived severity. Perceived vulnerability is the reflection of individual believe on the likelihood of getting negatively affected by malicious IT and perceived severity is the extent to which an individual perceives the effect of malicious IT will be severe. Research by Workman et al. (2008) found that perceived vulnerability has an impact on a user's IT behavior. Research by Liang & Xue (2010) reveals that avoidance behavior is positively affected by avoidance motivation. Hence, we propose that perceived vulnerability positively affects avoidance motivation. Thus, H1 is:

*Perceived vulnerability of being targeted by cyber-attacks positively affects avoidance motivation.*

Safeguard cost is referred to as the "physical and cognitive effort" in terms of money and time needed to implement the safeguarding measures (Liang & Xue, 2009). Studies have shown that individuals tend to avoid implementing secured network if the cost associated with it is too high (Woon, Tan, & Low, 2008). Hence, we propose that user motivation is negatively impacted by the potential cost. Thus, H2 is:

*Safeguard cost negatively impacts avoidance motivation.*

Apathy is defined as the lack of interest or motivation (Robert et al., 2002). Research by (Foltz, Schwager, & Anderson, 2008) reveal that apathy negatively influences behavioral intention and intention feeds motivation. Hence, we propose apathy negatively impacts avoidance motivation.

Thus, H3 is: *Apathy negatively impacts avoidance motivation.*

Several authors have looked at the relationship between self-efficacy and intent to adopt secure IT practices. Prior research by different authors demonstrated that the user's motivation to practice IT security is positively driven by self-efficacy (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). Hence higher the user's self-efficacy, stronger is the avoidance motivation with H4 as:

*Self-efficacy positively affects avoidance motivation.*

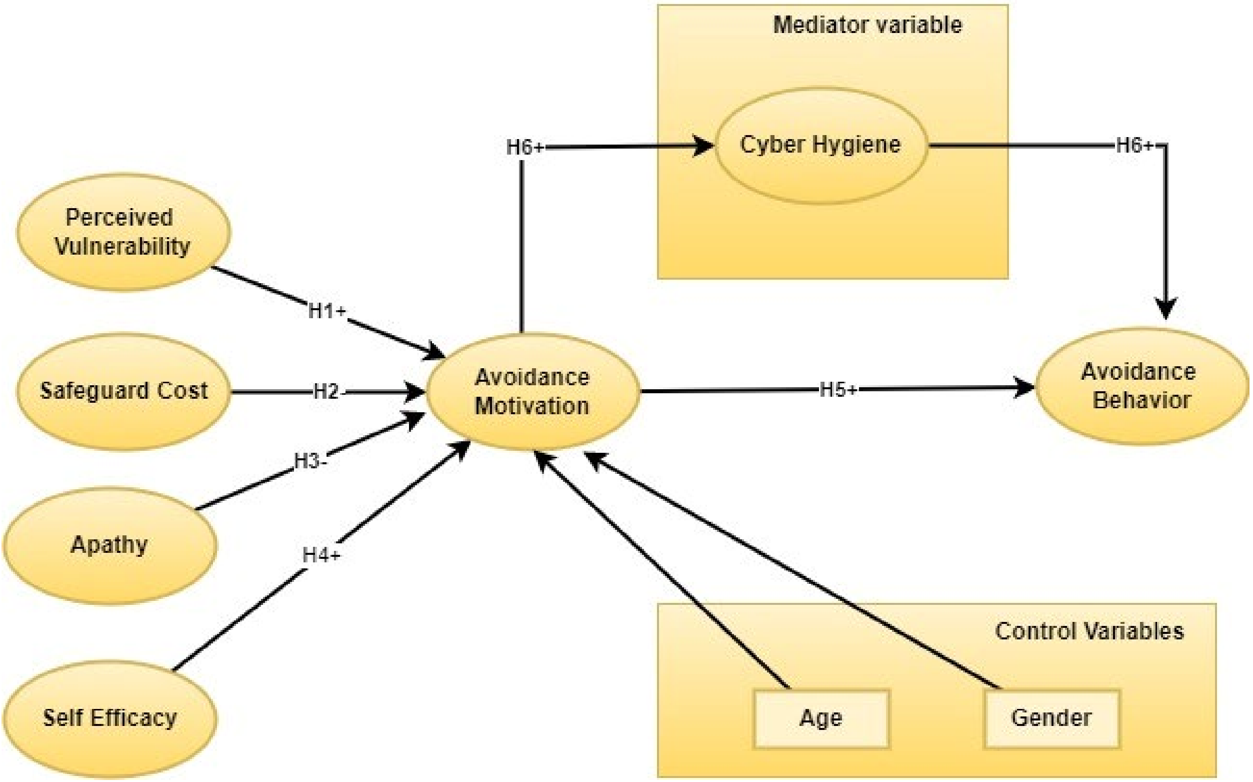
Research by (Venkatesh et al., 2003) confirmed that users having a strong motivation towards avoiding IT threats, are more drawn to engage in the avoidance behavior of implementing safeguards.

Thus, H5 is *Avoidance motivation positively affects avoidance behavior.*

Research by Esparza et al., 2020 demonstrated human behavior to be one of the key factors influencing user's motivation towards perceiving cyber threats and avoiding them. Hence, we propose that stronger avoidance motivation will also affect cyber hygiene practices, which in turn will positively impact avoidance behavior. In other words, cyber hygiene practices will have a mediating effect on the relationship between avoidance behavior and avoidance motivation. Thus, H6 is:

*The relationship between avoidance motivation and avoidance behavior will be mediated by cyber hygiene practices.*

We have identified age and gender as control variables for our research because previous research by Gratian et al. (2018) demonstrated that women tend to create weaker passwords than men. Research by Whitty et al. (2015) found that younger people follow very poor security practices. Figure 3 below represents our research model.



## PROPOSED RESEARCH METHODOLOGY

This research study will be a multi-method approach. Semi-structured interviews will be conducted with patients/users of telehealth to determine key insights that will provide information related to technologies such as hardware, software, and security that are in place during telehealth visits using personal devices. The interview subjects will be recruited by advertising via social media and on LinkedIn. The subjects will be recruited using a pre-questionnaire to determine age and prior use of telehealth. Participants will be 19+ and will need to have utilized telehealth at least one time. Approximately 5-10 interviews will be conducted in-person and/or virtually. The interviews will be transcribed, and a thematic analysis will be conducted using Atlas.ti to determine key themes related to telehealth security and privacy strengths and challenges. The findings from the qualitative data collection will provide a more insightful view from patients that have used telehealth beyond what would be collected using a survey instrument. The results from the qualitative data collection will also help the researchers determine if there are any themes or areas specific to security and privacy from a patient's perspective that are missing from the survey. This data collection will provide the authors with an enriched perspective prior to conducting the survey. The results from the qualitative data will provide answers to research question 1: Does patient cyber hygiene behavior change in the context of telehealth? The interview questions can be found in Appendix A.

The survey will be distributed via a university website and via communications among medical facilities in a Midwest metropolitan area. Participants will be 19+ and will need to have utilized telehealth at least one time. The survey for the quantitative analysis will be distributed via Qualtrics and will collect data to validate the research model and hypotheses. The survey questions will be adapted from existing instruments that test the constructs discussed in the model/hypotheses section. The constructs and instruments adapted are: Perceived Vulnerability (Kimpe, et al. 2021), Safeguard Cost (Liang & Xue, 2010; Viswanath, et al., 2020), Apathy (Viswanath, et al. 2020), Self-Efficacy **(**Kimpe, et al., 2021), Avoidance Motivation (Viswanath, et al. 2020), Avoidance

Behavior (Viswanath, et al. 2020; Liang & Xue, 2010), Cyber hygiene (Viswanath, et al., 2020), and demographic data such as age and gender.

## EXPECTED CONTRIBUTIONS TO RESEARCH AND PRACTICE

While telehealth and research surrounding it have been looked at previously, the field is disjointed with a variety of terms surrounding telehealth and telemedicine. The COVID-19 pandemic has had a profound impact on the digital transformation of healthcare and the utilization of telehealth. This research provides a starting point and clear distinction between telehealth and its variations. While the TTAT is an important theory that contributes to the understanding of human motivation and behavior, there are areas that can extend and improve upon the theory to provide more insight in the context of the personal devices, home networks, and telehealth. Understanding more about this context can provide a starting point for determining if the health data can have an influence on cyber hygiene, motivation, and behavior.

The use of personal devices by patients to conduct telehealth (direct-to-consumer) related visits has opened up additional vulnerabilities that stretch beyond the coverage of HIPAA compliance requirements. This is an importance area to research considering that prior research has shown that individuals have poor cyber hygiene while using personal devices. Health care entities can use these findings to not only improve cyber hygiene practices among patients, but also for providers (which is a planned future study for the authors – focusing on provider-specific considerations for telehealth).

# Appendix A

## Qualitative Semi-Structured Interview Questions

1. Please tell me about the technology that you use for telehealth visits. Please do not provide personal details such as the type of provider, but instead use general terms such as, when I have an appointment with my provider....
2. Has COVID changed the way that you visit the doctor?
3. How do you normally perform any updates to software or systems (keeping in mind the systems that you may use for telehealth?
4. Have you received any recommendations for technology and/or security practices from your provider(s)?
5. What options do you take into consideration when planning on a telehealth visit?
    i. Also, when given a choice between telehealth and in-person visits, what are factors that are taken into consideration?
6. Please tell me your thoughts about keeping your health information secure?
7. Please tell me your thoughts about keeping your health information private?

Survey Item References:

| | |
|---|---|
| **Perceived Vulnerability** | Kimpe, et al., 2021 |
| **Safeguard Cost** | Liang & Xue, 2010; Viswanath, et al., 2020 |
| **Apathy** | Viswanath, et al., 2020 |
| **Self-Efficacy** | Kimpe, et al., 2021 |
| **Avoidance Motivation** | Viswanath, et al., 2020 |
| **Avoidance Behavior** | Viswanath, et al., 2020; Liang & Xue, 2010 |
| **Cyber hygiene** | Viswanath, et al., 2020 |

## REFERENCES

Agarwal, S., Engle, K. L., & Labrique, A. (2016, Marc 17). Guidelines for reporting of health interventions using mobile phones: mobile health (mHealth) evidence reporting and assessment (mERA) checklist. BMJ, 352. doi:https://doi.org/10.1136/bmj.i1174

American Hospital Association (AHA). (2019). Fact Sheet: Telehealth.

Avertium. (2022, Mar 29). ZERO-DAY GOOGLE CHROME TYPE CONFUSION VULNERABILITY. Retrieved from Avertium: https://www.avertium.com/blog/zero-day-google-chrome-type-confustion-vulnerability

Baker, J., & Stanley, A. (2018, Sep 26). Telemedicine Technology: a Review of Services, Equipment, and Other Aspects. 18(11), 60. doi:10.1007/s11882-018-0814-6

Bassan, S. (2020). Data privacy considerations for telehealth consumers amid COVID-19. Journal of Law and the Biosciences,, 1-12. doi:10.1093/jlb/lsaa075

Benziger, C. P., Huffman, M. D., Sweis, R. N., & Stone, N. J. (2020, July 17). The Telehealth Ten: A Guide for a Patient-Assisted Virtual Physical Examination. The american Journal Of Medicine. Retrieved from https://doi.org/10.1016/j.amjmed.2020.06.015

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36-45. doi:doi.org/10.1016/j.jisa.2018.08.002

Carlson, J. L., & Goldstien, R. (2020). Using the Electronic Health Record to Conduct Adolescent Telehealth Visits in the Time of COVID-19. Journal Of Adolescent Health, 157-158. doi:https://doi.org/10.1016/j.jadohealth.2020.05.022

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. Communications of the Association for Information Systems, 44(22). doi:DOI: 10.17705/1CAIS.04422

CDC. (2019). Telehealth and Telemedicine: A Research Anthology of Law and Policy Resources. Retrieved from Centers for Disease Control and Prevention: https://www.cdc.gov/phlp/publications/topic/anthologies/anthologies-telehealth.html#:~:text=Telemedicine%20is%20defined%20by%20the,provider.%E2%80%9D4%20The%20World%20Health

Center for Disease Control and Prevention. (2018). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved from Center for Disease Control and Prevention: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward, 113, 2-4. Retrieved from https://doi.org/10.1016/j.maturitas.2018.04.008

Cybersecurity & Infrastructure Security Agency. (2020, Nov 03). Security Tip (ST15-002) Home Network Security. Retrieved from CISA: https://www.cisa.gov/uscert/ncas/tips/ST15-002

Defcon Conference. (2021, Aug 14). Do No Harm. YouTube. https://www.youtube.com/watch?v=Pf4HJNGcMXg.

Dempsey, K., Eavy, P., Goren, N., & Moore, G. (2018). NISTIR 8011 - Automation Support for Security Control Assessments. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8011-3.pdf

Esparza, J., Walters, A., & Caporusso, N. (2020). Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. doi:10.1007/978-3-030-52581-1_12

Fagan, M., & Khan, M. M. (2016). Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. Symposium on Usable Privacy and Security, (pp. 59-75). Retrieved from https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-fagan.pdf

Fahed, M., & Steffens, D. C. (2021). Apathy: Neurobiology, Assessment and Treatment. Clinical Psychopharmacology and Neuroscience, 19(2), 181-189. Retrieved from https://doi.org/10.9758/cpn.2021.19.2.181

Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why users (fail to) read computer usage policies. Industrial Management & Data Systems, 108(6), 701-712. doi:10.1108/02635570810883969

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. Information-Knowledge-Systems, 7(1,2), 159-180. doi:https://dl.acm.org/doi/10.5555/1402701.1402714

Gately, E. (2019, Apr 17). Unsecure Devices, Bad Cyber Hygiene Give Malicious Hackers a Leg Up. Retrieved from Channel Futures: https://www.channelfutures.com/mssp-insider/insecure-devices-bad-cyber-hygiene-give-malicious-hackers-a-leg-up

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers & Security, 73, 345-358. doi:https://doi.org/10.1016/j.cose.2017.11.015

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers,and applications. Sensors International, 2, 10117. Retrieved from https://doi.org/10.1016/j.sintl.2021.100117

Hall, J. L., & Deven, M. (2014, Feb). For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. 216-221. doi:https://doi.org/10.1377/hlthaff.2013.0997

Health Resources & Services Adminsitration. (2021, Sept). What is Telehealth? Retrieved from https://www.hrsa.gov/rural-health/telehealth/what-is-telehealth

HealthIT. (2019, Apr 9). https://www.healthit.gov/faq/what-information-does-electronic-health-record-ehr-contain. Retrieved from HealthIT.gov: https://www.healthit.gov/faq/what-information-does-electronic-health-record-ehr-contain

HealthIT. (2019). What is telehealth? How is telehealth different from telemedicine? Retrieved from HealthIT.gov: https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine

HHS Cybersecurity Program. (2020). 2020: A Retrospective Look at Healthcare Cybersecurity. Retrieved from https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

HHS Cybersecurity Program. (2022). Health Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead. Retrieved from https://www.aha.org/system/files/media/file/2022/03/hc3-tlp-white-health-sector-cybersecurity-2021-retrospective-2022-look-ahead-3-3-22.pdf

HHS.gov. (2013). Summary of the HIPAA Privacy Rule. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

HHS.gov. (2021, Dec 3). New HHS Study Shows 63-Fold Increase in Medicare Telehealth Utilization During the Pandemic. Retrieved from HHS.gov: https://www.hhs.gov/about/news/2021/12/03/new-hhs-study-shows-63-fold-increase-in-medicare-telehealth-utilization-during-pandemic.html#:~:text=Taken%20as%20a%20whole%2C%20the,Island%2C%20New%20Hampshire%20and%20Connecticut.

HHS.gov. (2021, Jan). Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency. Retrieved from HHS.gov: Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

HHS.gov. (2022, Mar 17). About the Affordable Care Act. Retrieved from HHS.gov: https://www.hhs.gov/healthcare/about-the-aca/index.html

HIPAA Journal. (2019, Oct 9). 68,000 Patients of Methodist Hospitals Impacted by Phishing Attack. Retrieved from 68,000 Patients of Methodist Hospitals Impacted by Phishing Attack: https://www.hipaajournal.com/68000-patients-of-methodist-hospitals-impacted-by-phishing-attack/

IBM Security. (2021). Cost of Data Breach Report 2021. Retrieved from https://www.ibm.com/downloads/cas/OJDVQGRY

Jalali, M. S., Landman, A., & Gordon, W. J. (2021). Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association, 28(3), 671-672. doi:10.1093/jamia/ocaa310

Kelley, D. (2018). Investigation of Attitudes Towards Security Behaviors. McNair Research Journal SJSU, 14(10), 125-136. Retrieved from https://doi.org/10.31979/mrj.2018.1410 https://scholarworks.sjsu.edu/mcnair/vol14/iss1/10

Kirkpatrick, K. (2015). Cyber policies on the rise. Communications, 58(10), 21-23. Retrieved from https://doi.org/10.1145/2811290

Koonin, L. M., Hoots, B., Tsang, C. A., Leroy, Z., Farris, K., Jolly, B. T., . . . Harris, A. M. (2020). Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January–March 2020.

Kumar, S., & Snooks, H. (2011). Telenursing. Springer.

Kvedar, J., Coye, M. J., & Everett, W. (2014). Connected Health: A Review Of Technologies And Strategies To Improve Patient Care With Telemedicine And Telehealth. Health Affairs, 33(2), 194-199. doi:10.1377/hlthaff.2013.0992

Laws, G., Nowatkowski, M., Heslen, J., & Vericell, S. (2018). Guidelines for Cyber Hygiene in Online Education. 93-100.

Leung, L., & Chen, C. (2019, Jan 27). E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information activities. Telecommunications Policy, 563-575. doi:https://doi.org/10.1016/j.telpol.2019.01.005

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71-90. doi:10.2307/20650279

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of Associations for Information System, 11(7), 71-90. doi:10.17705/1jais.00232

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. IEEE Xplore. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9215374

McKinsey & Company. (2021, Jul 9). Telehealth: A quarter-trillion-dollar post-COVID-19 reality? Retrieved from https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality

Mechanic, I., Persaud, Y., & Kimball, a. (2017). Telehealth Systems. StatPearls Publishing, Treasure Island (FL). Retrieved from https://europepmc.org/article/NBK/nbk459384

Moghadas, A., Jamshidi, M., & Shaderam, M. (2008). Telemedicine in healthcare system. 2008 World Automation Congress. IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4699015

Naraine, R. (2021, Oct 11). Apple Confirms iOS 15 Zero-Day Exploitation. Retrieved from Securityweek: https://www.securityweek.com/apple-confirms-ios-15-zero-day-exploitation

National Institute of Standards and Technology: US Department of Commerce. (2022). Securing Telehealth Remote Patient Monitoring Ecosystem. NIST SPECIAL PUBLICATION 1800-30A, 1-392. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-30.pdf

NCBI. (2012). The Evolution of Telehealth: Where Have We Been and Where Are We Going? In The Role of Telehealth in an Evolving Health Care Environment: Workshop Summary. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK207141/

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Computer & Security, 92, 99339-99361. Retrieved from https://doi.org/10.1016/j.cose.2020.101731

Ng, B.-Y., A. Kankanhalli, and Y. C. Xu (2009) "Studying users' computer security behavior: A health

belief perspective," Decision Support System (46) 4, pp. 815-825.

NIST. (n.d.). COMPUTER SECURITY RESOURCE CENTER (CSRC). Retrieved from https://csrc.nist.gov/glossary/term/zero_day_attack

NIST SPECIAL PUBLICATION 1800-30. (2022). Securing Telehealth Remote Patient Monitoring Ecosystem. 11-16. doi:https://doi.org/10.6028/NIST.SP.1800-30

Patel, P., Dhindsa, D., Eapen, D.J., Khera, A., Gulati, M., Stone, N.J., Yancy, C.W., Rumsfeld, J.S. & Sperling, L.S. 2021. "Optimizing the Potential for Telehealth in Cardiovascular Care (in the Era of COVID-19): Only Time Will Tell," The American Journal of Medicine, (134:8), pp. 945-951.

Plachkinova, M., Andres, S., Chatterjee, S. 2015. "A Taxonomy of mHealth Apps – Security and Privacy Concerns," 2015 48th Hawaii International Conference on System Sciences. pp.3187-3196.

Plachkinova, M., Andres, S., & Chatterjee, S. (2015). A Taxonomy of mHealth Apps -- Security and Privacy Concerns. (pp. 3187-3196). IEEE. doi:10.1109/HICSS.2015.385

Robert, P.H., Clairet, S., Benoit, M., Koutaich, J., Bertogliati, C., Tible, O., Caci, H., Borg, M., Brocker, P. and Bedoucha, P. (2002), "The apathy inventory: assessment of apathy and awareness in Alzheimer's disease, Parkinson's disease and mild cognitive impairment", International Journal of Geriatric Psychiatry, Vol. 17 No. 12, pp. 1099-105.

Roumani, Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. Journal of Cybersecurity, 7(1), 1-13. doi:https://doi.org/10.1093/cybsec/tyab023

Russo, J. E., McCool, R. R., & Davies, L. (2016, Mar 14). VA Telemedicine: An Analysis of Cost and Time Savings. Telemedicine journal and e-health, 22(3). doi:10.1089/tmj.2015.0055

Rutledge, C. M., Kott, K., Schweickert, P. A., Poston, R., Fowler, C., & Haney, T. S. (2017, Jun 26). Telehealth and eHealth in nurse practitioner training: current perspectives. Advances in Medical Education and Practice, 399-409. doi:https://doi.org/10.2147/AMEP.S116071

Services, U. D. (2021). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved April 2021, from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=365037181A402E68E1611931BC7B016C

Sheppard, B., Crannell, M., & Moulton, J. (2013). Cyber first aid: proactive risk management and decision-making. Environ Syst Decis, 33, 530-535. doi:10.1007/s10669-013-9474-1

Stanton, J.M., Stam, K.R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & security, vol. 24, no. 2, pp.124–133.

Statista. (2018, Aug). Projected size of the global mHealth market from 2017 to 2025. Retrieved from Statista: https://www.statista.com/statistics/1014589/worldwide-mhealth-market-size/

Taylor, T. (2022, Feb 2). Hackers, Breaches, and the Value of Healthcare Data. Retrieved from SecureLink: https://www.securelink.com/blog/healthcare-data-new-prize-hackers/

TELEHEALTH.HHS.GOV. (2022, Jan 5). Telehealth and remote patient monitoring. Retrieved from TELEHEALTH.HHS.GOV: https://telehealth.hhs.gov/providers/preparing-patients-for-telehealth/telehealth-and-remote-patient-monitoring/

Telehealth.hhs.gov. (n.d.). Telehealth for direct-to-consumer care. Retrieved from Telehealth.hhs.gov: https://telehealth.hhs.gov/providers/direct-to-consumer/#:~:text=This%20type%20of%20%E2%80%9Cat%20home,device%2C%20on%20their%20own%20schedule

Telligen. (2014, Oct). Telehelath: Start-Up and Resource Guide. Retrieved from https://www.healthit.gov/sites/default/files/playbook/pdf/telehealth-startup-and-resource-guide.pdf

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. International Journal of Business and Management, 13(6), 1-2. doi:doi:10.5539/ijbm.v13n6p1

Thompson, N., McGill, T. J., & Wang, X. (2017). “Security begins at home”: Determinants of home computer and mobile device security behavior. Computers & Security, 376-391. doi:http://dx.doi.org/10.1016/j.cose.2017.07.003

United States Government Accountability Office: GAO-12-757. (2012). Better Implementation of Controls for Mobile Devices Should Be Encouraged. Retrieved from https://www.gao.gov/assets/gao-12-757.pdf

Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis (2003) "User acceptance of information

technology: toward a unified view," MIS Quarterly (27) 3, pp. 425-478.

Verkijika, S. F. (2021). Employees' Cybersecurity Behaviour in the Mobile Context: The Role of Self-Efficacy and Psychological Ownership. 2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1-5). IEEE. doi:10.1109/IMITEC50163.2020.9334097

Viswanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., & Ong, G. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113-160. Retrieved from https://doi.org/10.1016/j.dss.2019.113160

Wang, L., & Alexander, C. A. (2021, April 26). Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2), 146-157. doi:10.3934/electreng.2021008

Weinstein, R. S., Lopez, A. M., Joseph, B. A., Erps, K. A., Holcomb, M., Barker, G. P., & Krupinski, E. A. (2014). Telemedicine, Telehealth, and Mobile Health Applications That Work: Opportunities and Barriers. The american Journal of Medicine, 183-187. doi:http://dx.doi.org/10.1016/j.amjmed.2013.09.032

Whitty M, Doodson J, Creese S, Hodges D. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior and Social Networking; 2015, pp. 3–7.

Willis, J.S., Tyler, Jr., C., Schiff, G.D., & Schreiner, K. 2021. “Ensuring Primary Care Diagnostic Quality in the Era of Telemedicine,” The American Journal of Medicine, (134:9), pp. 1101-1103

Woon, I. M., Tan, G. W., & Low, R. T. (2005). A PROTECTION MOTIVATION THEORY APPROACH TO HOME WIRELESS SECURITY. Twenty-Sixth International Conference on Information Systems, (pp. 367-380).

Workman, M. D., Straub, D., & Bommer, W. H. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behaviour, 24, 2799-2816. doi:10.1016/j.chb.2008.04.005

Xu, K., Wang, F., & Jia, X. (2016, Jul 19). Secure the Internet, one home at a time. SECURITY AND COMMUNICATION NETWORKS, 3821-3832. doi:10.1002/sec.1569

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82-97. Retrieved from https://doi.org/10.1080/08874417.2020.1712269