"We Have No Security Concerns": Understanding the Privacy-Security Nexus in Telehealth for Audiologists and Speech-Language Pathologists: Understanding the Privacy-Security Nexus in Telehealth

Faiza Tazi
Faiza.Tazi@du.edu
University of Denver
USA

Josiah Dykstra
josiah@designersecurity.com
Designer Security, LLC
USA

Prashanth Rajivan
prajivan@uw.edu
University of Washington
USA

Sanchari Das
Sanchari.Das@du.edu
University of Denver
USA

ABSTRACT

The advent of telehealth revolutionizes healthcare by enabling remote consultations, yet poses complex security and privacy challenges. These are often acutely felt by lower-resourced, allied-healthcare practices. To address this, our study focuses on audiologists and speech-language pathologists (SLPs) in private practice settings, often characterized by limited information technology resources. Over the course of six months, we conducted semi-structured interviews with ten audiologists and ten SLPs to understand their telehealth experiences and concerns. Key findings reveal a diversity of opinions on technology trustworthiness, data security concerns, implemented security protocols, and patient behaviors. Given the nature of the medical practitioners' primary work, participants expressed varied concerns about data breaches and platform vulnerabilities, yet trusted third-party services like Zoom due to inadequate expertise and time to evaluate security protocols. This work underscores the imperative of bridging the technology-healthcare gap to foster secure, patient/provider-centered telehealth as the prevailing practice. It also emphasizes the need to synergize security, privacy, and usability to securely deliver care through telehealth.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Social aspects of security and privacy**; *Privacy protections*; *Usability in security and privacy*; Economics of security and privacy.

KEYWORDS

Telehealth, Privacy, Security, User Study, Healthcare

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642208

ACM Reference Format:
Faiza Tazi, Josiah Dykstra, Prashanth Rajivan, and Sanchari Das. 2024. "We Have No Security Concerns": Understanding the Privacy-Security Nexus in Telehealth for Audiologists and Speech-Language Pathologists: Understanding the Privacy-Security Nexus in Telehealth. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3613904.3642208

1 INTRODUCTION

Telehealth has garnered widespread acceptance among people who need healthcare and those who provide it [85, 98]. This digital transformation of healthcare, however, introduces substantial risks to patients' privacy and security [47]. While both telehealth and traditional in-person visits often utilize cloud-based services for managing patient data, telehealth introduces unique nuances to existing vulnerabilities and challenges. These include challenges related to authentication, identity verification, consent, screen sharing and recording, and regulatory compliance [36]. These may stem from specialized hardware and software needed for video communication or data collection from remote patient medical devices. Therefore, telehealth systems not only have to comply with existing legal and regulatory frameworks which may vary across jurisdictions, but they also need to account for these risks [37].

In the United States where our study was conducted, the Health Insurance Portability and Accountability Act (HIPAA) applies to all protected health information (PHI) no matter where or how it is stored [83]. HIPAA requires various "reasonable safeguards" to accommodate the varied needs and circumstances of healthcare entities and professionals [20]. A large hospital may have a substantial budget and full-time staff that manages a mature telehealth and cybersecurity program that is HIPAA compliant [5, 42], while independent providers and small private clinics may need more economical solutions due to fewer overall resources and limited expertise [27]. Allied healthcare clinics that provide speech and audiology services are one such healthcare setting that faces challenges arising from both resource limitations and technical expertise constraints [39]. Similar to other healthcare practices,

speech and audiology clinics must contend with infrastructure, personnel, and technology costs. However unlike many other areas of healthcare, audiology and speech services encounter a unique set of challenges, including limited reimbursement options and declining reimbursement rates from private and Medicaid insurances [40, 94]. Insurance reimbursements constitute the primary and often the only source of revenue for these clinics. So, many private clinics may have to rely on general-purpose video conferencing technologies such as Zoom and Google Meet to conduct telehealth sessions. Moreover, speech and audiology services involve ongoing patient engagement, as the same individuals often require regular therapy, evaluation, and coaching. The recurring nature of their services makes telehealth an attractive option, and therefore, there is an increasing demand from patients for flexible speech and audiology services [63]. Therefore, it is critical to understand the challenges, including the security and privacy challenges, that private clinics experience with telehealth technologies. Yet, resource-constrained healthcare settings remain severely understudied.

Ensuring privacy and security in telehealth is not solely a technological challenge. Humans interacting with telehealth platforms play an important role, especially the primary users of the technology - healthcare providers. It has been suggested that the behaviors and preferences of both patients and healthcare professionals must be considered in the design and implementation of telehealth platforms [92] but there is a lack of studies that discuss medical providers perspectives on telehealth security and privacy. For instance, several studies found that patients who express satisfaction with telehealth encounters are more inclined to keep utilizing telehealth services [28, 57, 66]. Furthermore, Wilowska et al. found that females and healthy adults have the most stringent security and privacy requirements for telehealth compared to males and the ailing elderly [97]. This study aims to address this research gap by investigating how audiologists and SLPs in private practice settings currently utilize telehealth services. We specifically focus on these two allied health specialties as a preliminary exploration for understanding broader concerns of data privacy and security in telehealth in low-resource medical settings. Through interviewing 20 audiologists and SLPs who actively engage in telehealth, this research provides invaluable insights into real-world practices, professional perceptions, and attitudes concerning privacy and security risks. Finally, we identify opportunities for both technological enhancements and behavior-driven solutions that can bridge the existing gaps. Our contributions are three-fold, offering a holistic understanding of privacy and security behavior in telehealth.

- Firstly, this study furnishes a comprehensive overview of the prevailing understanding and attitudes toward privacy and security among audiologists and SLPs operating in private healthcare practices. This highlights not just the level of awareness among healthcare professionals, but also reveals the nuanced complexities and considerations that inform their daily interactions with telehealth technologies.
- Secondly, we identify specific privacy and security challenges that are unique to these specialists. These challenges encompass difficulties in securely transmitting sensitive auditory and verbal patient data and assisting particularly vulnerable populations in the secure use of telehealth software. These issues aren't solely technological; they intertwine with complex HCI problems related to usability, trust, and accessibility.
- Lastly, based on our findings, we propose a set of actionable strategies for mitigating identified challenges, thereby improving the privacy and security posture of telehealth services. These recommendations aim to facilitate a more harmonious integration of technology with healthcare delivery, making it easier for healthcare professionals to comply with security protocols without sacrificing usability or patient care. The strategies touch upon the development of intuitive user interfaces and the creation of targeted training modules for healthcare providers informed by our research, thereby forming a synergistic approach that straddles the intersecting domains of security, privacy, and healthcare delivery.

2 RELATED WORKS

2.1 Telehealth Privacy and Security Concerns

The field of healthcare has observed a significant rise in privacy and security threats, particularly within the telehealth domain [32, 74, 85]. This mirrors telehealth's increasing importance in contemporary healthcare delivery [76]. Many researchers stress the essential role of protecting patient data and ensuring confidentiality within telehealth services [74, 96]. Furthermore, data breaches remain a significant concern in telehealth [15], mirroring trends seen across various industries [9]. Several factors contribute to these breaches, including employees' lack of awareness, inadequate security protocols, and a limited allocation of resources for technological solutions [19, 38]. This underscores the importance of understanding users' perspectives beyond just the patients'.

Establishing secure communication channels between healthcare practitioners and patients stands paramount in telehealth security [86]. Alarmingly, some providers use messaging software that falls short of regulatory standards for patient information exchange [1, 22, 93]. This non-compliance jeopardizes both the HIPAA requirements and patients' privacy [75]. As telehealth adoption accelerates, we must bridge knowledge gaps—especially in private and specialty practices—to ensure the safe operation of telehealth platforms [24]. Drilling deeper into specialties, fields like speech-language pathology and audiology have seen growing telehealth integration, sparking concerns over security and privacy. While much research in these areas has delved into implementation barriers and tech solutions, they often overlook the privacy and security facets [82]. Prior studies have highlighted the necessity of earmarking resources and delivering training for robust patient data protection [36]. This involves adopting data encryption techniques, rolling out rigorous privacy and security training modules, and investing in technology that protects patient data, while simultaneously elevating practice efficiency [12, 95] which may not be aligned with the resource limitations of allied healthcare practices such as that of audiologists or SLPs. Studies squarely focused on audiologists and SLPs have concentrated predominantly on telehealth implementation barriers [13, 80], increasing adoption of telehealth [16, 33] or policy considerations [43]. Nevertheless, there is a notable gap in the literature concerning the privacy perceptions

and behaviors of these professionals in relation to telehealth. A study conducted by Dykstra et al. investigated the cybersecurity behaviors of audiologists in private practices. The study revealed that audiologist possess a limited understanding of cybersecurity and do not allocate sufficient resources to protect against potential cyber threats [27]. However, it is important to note that this study did not consider the telehealth practices of the participants.

2.2 Perspectives of Allied Healthcare Professionals on Telehealth

The exponential expansion of telehealth has spurred substantial investigation into its implementation and ramifications [74, 85, 92]. Moreover, current research on telehealth security and privacy largely focuses on creating new technological solutions [82], while technology is pivotal, addressing human and organizational aspects that might lead to security risks is equally crucial [71]. Yet, perspectives from audiologists, SLPs, and similar allied healthcare professionals in private practices remain notably understudied [38, 82]. Building on the security and privacy challenges previously discussed, healthcare practitioners and patients continue to employ telehealth technologies, highlighting their indispensable value [30]. However, breaches in security can significantly erode trust in these systems, underscoring the importance of improving our understanding of healthcare security and privacy within telehealth, especially from the lens of healthcare professionals [46]. Hall and McGraw highlight that breaches in patient privacy and security lapses can both compromise care quality and weaken patients' trust in telehealth technologies [36]. Such a decline in trust might deter patients [72, 92], especially those in remote or under-served regions, from using telehealth services they heavily rely upon [89]. While we gather comprehensive insights into the general perceptions of these professionals regarding telehealth, a gap remains in research addressing their specific privacy and security apprehensions. Our study aims to bridge this, focusing on the allied healthcare practices which are severely understudied.

Among healthcare providers, attitudes and apprehensions regarding telehealth security substantially impact its acceptance and adoption [36, 48]. In their systematic study, Watzlaf et al. analyzed the existing practices regarding privacy and security in the utilization of telehealth technology by healthcare practitioners. Nevertheless, the authors failed to document any studies that take into account the viewpoints of allied health professionals such as audiologists or speech-language pathologists [96]. Similarly, Houser et al. performed a comprehensive analysis to uncover the obstacles and contributing variables concerning privacy and security in telehealth visits during the COVID-19 pandemic. They conducted a systematic evaluation of scholarly articles that examined the utilization of telehealth in the healthcare industry, encompassing both providers and consumers of healthcare using telehealth. The selected articles were published between January 2020 and February 2022. Nevertheless, the authors did not report on any papers that consider the allied health perspectives [38]. Building on the vulnerabilities associated with healthcare providers' authentication and access control techniques often raise concerns in telehealth security [27], even though experts frequently suggest them as security solutions. Previous studies have shown that providers sometimes bypass authentication steps or share login credentials [29], often driven by burdensome access control measures [79]. Research on this topic tends to focus on larger healthcare institutions, potentially overlooking challenges unique to smaller private practices with limited tech resources [96]. A related challenge lies in patient education about telehealth security [45, 78]. Patients' limited understanding can lead to unintentional breaches, like revealing personal health details in unsecured environments [35, 91]. Providers often underestimate this knowledge gap, highlighting the need to gain a deeper understanding of these issues from their perspective.

Although there is an increasing number of studies on telehealth, there are still gaps in healthcare professionals' readiness to adequately handle important privacy and security concerns in telehealth [24, 36]. Dubose-Morris et al. conducted a study on telehealth education and training during the COVID-19 pandemic. They discovered that prior to the pandemic, telehealth training, which encompassed privacy and regulatory frameworks, was not consistently provided. Approximately 30% of programs reported a lack of formal training [26]. In addition, healthcare personnel often have insufficient training and awareness of cybersecurity and data protection best practices for telehealth [99]. As such, it is essential to have a more profound understanding of perspectives surrounding healthcare security and privacy in telehealth, particularly from healthcare experts.

2.3 Cybersecurity Concerns in Under-Resourced Healthcare Practices

As telehealth extends beyond traditional healthcare environments, the need to protect sensitive patient information grows even more crucial. Nevertheless, privacy and security remain insufficiently studied, especially in low-resource healthcare environments such as allied healthcare practices [90]. This gap persists despite audiologists, SLPs, and similar allied healthcare professionals in private practices facing unique challenges, particularly those contending with limited technical resources [27, 59, 62]. Because of these challenges, healthcare practitioners often struggle to implement cybersecurity measures, resorting to self-taught approaches [44, 69, 96]. Practice size and IT capabilities introduce further complexity in the telehealth landscape. As Pickering et al.'s study highlighted, small and medium enterprises in general with fewer technical resources markedly struggle to consistently uphold security protocols [64]. Prior research conducted in Indonesia [69] and Malawis [62] underscored deficiencies in cybersecurity awareness among medical professionals in lower-resourced community health clinics. However, minimal research has examined audiology and speech-language pathology practices in the US contending with similar resource limitations. Our work significantly builds on findings from these previous studies through robust sampling focused exclusively on small-scale practices within the two fields of audiology and SLP. Several studies have also underscored the role of patient demographics and accessibility barriers in shaping telehealth experiences. Wang et al. stressed the importance of optimizing telehealth platforms to serve diverse populations equitably [92]. Complementarily, Almalki et al. called attention to pronounced service access barriers frequently encountered by elderly patients in telehealth [6]. Other

works emphasized potential telehealth benefits for rural areas as well as homebound individuals facing mobility constraints [31, 89]. Such demographic considerations may disproportionately affect audiologists and SLPs, since they routinely serve patients from vulnerable or marginalized groups. Thus, our study provides crucial firsthand qualitative insights into this complex landscape from the direct lens of such healthcare professionals.

3 METHOD

This study aims to focus on the relationship between the adoption of telehealth services and the awareness of healthcare professionals—specifically audiologists and SLPs—concerning issues of privacy and security. We concentrate our investigation on professionals working in private practice settings within the allied healthcare disciplines of audiology and speech-language pathology in the United States where they have limited IT resources to support their privacy and security needs. By focusing on these specialized fields, we aim to shed light on the setting-specific implications of telehealth technologies. The overarching objective of this research is to systematically investigate the privacy and security practices, attitudes, and measures that are perceived by audiologists and SLPs to be connected with the integration and application of telehealth services in their respective fields. We seek to explore how these professionals balance challenges and risks while embracing the advantages of telehealth technology, especially with resource constraints.

3.1 Research Questions

This study aims to reveal how various factors centered on privacy and security affect the use of telehealth technologies among audiologists and SLPs in private and allied healthcare settings. To understand this multi-faceted issue, we formulate the following research questions:

- How much do audiologists and speech-language pathologists practicing in private healthcare facilities understand privacy and security issues related to telehealth?
- What strategies and practices do audiologists and speech-language pathologists employ in the realm of privacy and security when integrating telehealth technologies into their clinical workflows challenged by resource constraints? What emergent challenges related to privacy and security are perceived by these professionals?
- How do audiologists and SLPs in private healthcare settings actively institute measures to protect the privacy and security of sensitive patient data when utilizing telehealth technologies?

3.2 Recruitment Strategy

The research team adhered to institutional ethical guidelines and obtained approvals from relevant ethics review boards prior to participant recruitment. The target population comprised professionals from two allied healthcare disciplines: audiology and speech-language pathology. Utilizing a stratified purposive sampling approach [68], we aimed to recruit an equal number of audiologists and SLPs—10 from each field—to allow for a balanced exploration of professional viewpoints. Initial outreach was conducted via professional networks, academic forums, and special interest groups. To augment the study's visibility, we leveraged specialist social media groups focusing on audiology and speech-language pathology, along with other digital platforms, to disseminate information about the study's aims and participation criteria. Two authors of the manuscript had personal connections with individuals working in the field of speech and audiology services. The insights and perspectives gained from these personal connections served as the initial source of motivation for undertaking this study. These personal connections also played a pivotal role in facilitating the recruitment process.

We also enlisted the partnership of relevant professional societies to help distribute the invitation, namely the American Speech-Language-Hearing Association (ASHA) [7] and the Academy of Doctors of Audiology (ADA) [60]. Recruitment emails were disseminated to members of these organizations using their expansive membership databases. As an auxiliary strategy, we also employed snowball sampling methods to broaden the participant base. However, these inclusive recruitment methods also led to a considerable influx of 83 ineligible or false queries. Subsequently, we implemented a rigorous screening procedure involving manual evaluation to identify and exclude spam responses.

3.3 Participant Demographics

Upon concluding the recruitment phase, the study assembled a participant pool exhibiting considerable demographic and professional diversity. Participants were drawn from various geographical locations across the United States through online participation, thereby capturing perspectives influenced by different regional healthcare policies and practices. The participant composition was deliberately diverse, representing a spectrum of professional roles within the fields of audiology and speech-language pathology. Participants differed not only in their specific job responsibilities but also in their years of practice and familiarity with telehealth technologies.

The incorporation of participants with varying levels of experience and expertise in telehealth provided multifaceted insights into the challenges and opportunities linked with the adoption of telehealth services in private healthcare settings. For a detailed breakdown of the participant demographics, please refer to Table 1. This table provides a comprehensive profile, encapsulating elements such as professional designation, gender, years of experience, and platforms used for telehealth consultations. While, our sample exhibited some skewness in gender distribution (100% female SLPs and 70% female audiologists). This disproportionate gender is reasonably representative given that over 80% of audiologists [1] and over 90% of speech-language pathologists [2] are female.

3.4 Interview Process

We initiated the interview process by actively disseminating recruitment materials to our targeted audience. When potential participants contacted our research team using the provided email, we conducted preliminary screenings to determine their suitability. From 104 inquiries, we vetted and identified 21 participants who met the study's criteria, ensuring a pertinent participant pool. We then arranged virtual interviews for these 21 candidates on Zoom, a

[1] https://datausa.io/profile/soc/audiologists
[2] https://www.zippia.com/speech-language-pathologist-jobs/demographics/

ID	Role	Position	Gender	Work Exp.	Telehealth Exp.	Platform(s)
A1	AuD	Provider	M	6-10	1-5	Tuned*
A2	AuD	Owner/ Provider	M	11+	6-10	Tuned*
A3	AuD	Owner/ Provider	M	11+	1-5	Blueprint
A4	AuD	Clinic manager	F	1-5	1-5	Zoom
A5	AuD	Owner/ Provider	F	6-10	1-5	CounselEAR
A6	AuD	Provider	F	6-10	1-5	CounselEAR
A7	AuD	Owner/ Provider	F	11+	11+	CounselEAR + Epic
A8	AuD	Owner/ Provider	F	11+	1-5	Zoom + CounselEAR
A9	AuD	Partner/ Consultant	F	11+	1-5	ModMed + Athena
A10	AuD	Provider	F	6-10	6-10	Zoom
S1	SLP	Owner/ Provider	F	1-5	1-5	Google Meet
S2	SLP	Provider	F	11+	1-5	Zoom
S3	SLP	Owner/ Provider	F	11+	6-10	TheraPlatform
S4	SLP	Owner/ Provider	F	11+	1-5	TheraPlatform + Zoom
S5	SLP	Provider	F	11+	1-5	Zoom
S6	SLP	Provider	F	6-10	1-5	Zoom + Google Meet
S7	SLP	Provider	F	6-10	1-5	Zoom + Google Meet
S8	SLP	Provider	F	11+	1-5	Zoom + Google Meet + doxy.me + Blink Session
S9	SLP	Senior director of teletherapy	F	11+	1-5	Televate (proprietary platform)
S10	SLP	Provider	F	6-10	1-5	Zoom

Table 1: Demographic Profile of Study Participants with Telehealth Platform Transition Indicator. *: Denotes participants who transitioned to a new telehealth platform less than three months prior to the interview.

platform familiar to many professionals. Over a span of six months, from August 2022 to January 2023, we conducted interviews to capture their attitudes and experiences. While sessions lasted anywhere from 32 to 90 minutes, the average duration was 46 minutes, indicating deep and engaging conversations. Before each interview, we briefed participants about the study's objectives, methodologies, and ethical considerations. We obtained verbal informed consent from each participant, which included permission to record the session on Zoom Furthermore, we gave participants the option to disable their video if they felt uneasy about visual recording. However, due to unforeseen circumstances, one interview had to be canceled, leading to a final count of 20 participants.

We adopted a semi-structured interview format, crafting open-ended questions to elicit detailed responses from participants. This design fostered honest conversations, letting each session naturally adjust based on the participant's insights. The full questionnaire is provided in Appendix A. We refined these questions through 13 pilot interviews involving our research team, lab members, and external contributors from October 2021 to July 2022. To show our appreciation for the participants' input and time, we rewarded each participant with a $50 USD electronic gift card upon interview completion.

3.5 Data Analysis

After each interview, we auto-transcribed the audio recordings and verified them against the original audio to ensure accuracy. For the participant who opted out of recording, we captured their input through real-time manual notes. We then anonymized all transcripts and notes to remove identifiable details. Both the first and last authors reviewed the content to eliminate any identifiers. Subsequently, we permanently deleted the original audio recordings for confidentiality.

For our analysis, we used a thematic approach, as described by Mildner [53]. The first author generated a codebook using an inductive review of the interviews. To verify the coding's consistency, the second author recoded two random transcripts. Their inter-rater reliability (IRR) revealed a Cohen's kappa of $\kappa = 0.76$, denoting strong coder agreement. Both authors then discussed discrepancies, clarifying code definitions and merging insights to refine the codebook. With the updated codebook, Two researchers analyzed the remaining 17 transcripts and one manually noted interview through an iterative process, meeting regularly with the other authors to discuss emerging themes. We employed NVivo [49] and MAXQDA [51] for data coding and analysis. We added, merged, and split codes as new patterns emerged over three coding iterations. The first iteration focused on open coding to identify first-pass themes. The second iteration involved refining, consolidating, and organizing codes under higher-level categories. The final iteration aimed at distilling themes into a structured narrative focusing on the nuances of implementing telehealth solutions, especially regarding privacy and security. This narrative offers a deeper grasp of the practical and ethical dynamics within the audiology and speech-language pathology sectors.

4 RESULTS AND DISCUSSION

Ensuring the confidentiality and security of patient data during telehealth is crucial in audiology and speech-language pathology, as our participants have recognized. During the interviews, the healthcare providers discussed various topics related to their use of telehealth, including data collection, authentication, and security awareness in telehealth. Participants also discussed patient

attitudes towards telehealth from their perspectives. Our analysis examines participants' views on data privacy and also variations in their knowledge of telehealth security and privacy. Lastly, we highlight the distinct perceptions of audiologists and SLPs, emphasizing challenges, particularly in patients' technical proficiency, including children and older adults.

4.1 Patient Data Collection and Identity Verification Processes

In the context of audiology and SLP services, healthcare providers employ a variety of strategies to collect and protect patient data during telehealth sessions. This data includes personal information, health records, insurance data, and pertinent symptoms and concerns of patients. The primary objective of this data is to ascertain that the healthcare practitioner possesses a comprehensive understanding of the medical history of their patients and to provide them with personalized care.

4.1.1 Data Collection Strategies and Procedures. Our participants follow a variety of privacy and security strategies to collect patient data. Some of our participants (A1, A9, S2, S8) mentioned that telehealth is introduced only after the initial visit and exclusively to established patients, aligning with organizational policy compliance. This approach minimizes personal information collection during telehealth sessions, as the bulk of personal data is submitted in person. Another way of data access control our participants mentioned is avoiding use of third-party web services and instead collecting information through phone calls, preferred by their patients. For example, as A1 emphasizes that:

> "Any personal information is really limited as far as what is verbally addressed through the call." (A1)

Consequently, during telehealth sessions, limited personal information is disclosed, such as patient name and the particular health issue under discussion. The limited data interchange arises from the provider's possession of extensive medical histories and patient information, from previous encounters. Providers who accept new patients for telehealth services adhere to different protocols. Some healthcare providers utilize electronic communication to send forms to gather personal information, health records, insurance particulars, and pertinent symptoms or concerns. The primary objective of this data collection endeavor is to ascertain that the healthcare practitioner possesses a comprehensive and precise understanding of the medical history of the recently admitted patient. As A3 explains:

> "The new patient has already initiated an appointment so we then send online forms." (A3)

In a similar vein, S10 delineates their intake protocol for new patients, which entails the involvement of administrative personnel who contact these patients in order to collect the necessary information, patient concerns and the initial appointment is scheduled.

> "The admin will reach out to the client, gather basic information concerns and they will schedule the initial appointment." (S10)

This process involves the collection of sensitive personal information, necessitating secure data handling and communication channels. Collecting patient data prior to the consultation is crucial because it helps the providers prepare for the telehealth consultation. It also prevents the need for spending valuable consultation time in trying to obtain the necessary information.

4.1.2 Patient Identity Verification Processes. The process of verifying the identity of patients participating in telehealth is critical in order to uphold ethical and legal standards, comply with healthcare regulations, and secure sensitive health information. To prevent medical errors, improve the precision of prescriptions and treatments, and foster confidence between patients and healthcare providers, precise identification is vital. Additionally, it is instrumental in secure against fraudulent activities, ensuring precise invoicing, and establishing a secure chain of accountability within the field of digital healthcare. As such identity verification measures are indispensable for ensuring the security and efficacy of telehealth services.

We asked our participants to explain their patient identity verification processes, there is variation between respondents in their procedures pertaining to the verification of patient identity prior to the start of telehealth sessions. For example, A9 finds formal validation unnecessary as they indicated their ability to recognize their patients:

> "Most of the people that I'm doing telehealth with on the audiology side…I know these patients…I know their face." (A9)

In the interview, A9 highlights their familiarity with the majority of patients in telehealth sessions, emphasizing recognition of their faces. This suggests an established relationship, from prior in-person consultations. While this familiarity can enhance the patient-provider connection and reduce the need for extensive data exchange, it raises considerations for formal identity verification and ensuring informed consent. Conversely, A2 delineated a procedure in which they authenticate the identification of patients:

> "I confirm their identity because that's always kind of a question mark when you're meeting people online, you never know who's actually signing in." (A2)

Our participant responses underline the significance of identity verification within the telehealth domain. Ensuring the authenticity of participants' identities is of utmost importance, particularly in the digital domain where it may not be feasible to authenticate using physical evidence. As such, A2 highlights the critical need for confirming patient identity in telehealth, given the inherent uncertainty of online interactions. The potential for anonymity afforded by the internet gives rise to apprehensions over the true identity of those situated behind the screen. The verification process serves the dual purpose of protecting the privacy and security of telehealth sessions and promoting trust and confidence between healthcare providers and patients. This process ensures that confidential medical information is only shared with the intended recipient, thereby improving the overall quality of care provided via telehealth.

Furthermore, telehealth provides a secure platform for confidential health consultations, protecting people' sensitive health information from public exposure. This is particularly vital for those in delicate professions. The need of this discretion is emphasized by A2, who, when questioned about their patients' apprehensions, stated that certain patients are deeply concerned about the

confidentiality of the information they provide, fearing potential repercussions on their professional careers:

> "I'm working with a patient who's a singer ... and [they] tell me I'm having trouble perceiving pitch now because of my ear injury and I don't know if I can keep singing at the level that I used to but they don't want that information getting out because that could impact their employability and their ability to continue their career."

4.2 Provider Awareness of Security and Privacy

Our participants exhibited a diverse array of perspectives coming from varied background and discuss in detail about security and privacy in telehealth, demonstrating a combination of awareness and confusion.

4.2.1 Limited Awareness and Understanding. Eight participants (A2, A4-A6, A8, A10, S1, and S8) expressed a relative lack of awareness of potential security concerns associated with telehealth. For instance, A2 displayed a sense of assurance by asserting that their actions were as safe as a confidential conversation held face-to-face in a private setting. As they state:

> "What we're doing is as secure as a phone or as a conversation in a room behind closed doors." (A2)

This attitude might stem from a generally positive experience with telehealth. This statement also conveys a high level of confidence in the security of telehealth sessions, indicating that any sensitive information exchanged during these exchanges is effectively protected. This perception that telehealth is inherently secure is due to the lack of our participants' expertise in cybersecurity which has been emphasized by multiple participants (A8-A10, S5, S7-S10), and as A10 notes when asked about the ways security and privacy of healthcare data factor into their telehealth appointments:

> "This is outside of my area of expertise." (A10)
> "I don't have like a tech background." (S5)
> "I would not consider myself an expert in computer privacy and security by any means" (S7)

Furthermore, three participants (A4, A6, A9) admitted to having a restricted understanding of privacy and security matters, which might be attributed, in certain instances, to their limited exploration of the security dimensions associated with telehealth. In fact, A4 acknowledged a lack of comprehensive examination of privacy statements from the viewpoints of both patients and providers, hence indicating a deficiency in comprehension pertaining to the implemented security measures:

> "I'm actually not sure I... you know... I'd have to go in and read their privacy statement from the patient side and from my side, which I'll be honest I have not done." (A4)

This raises apprehensions regarding our participants understanding of the data privacy and security protocols implemented during telehealth sessions. The lack of understanding regarding the platform's privacy policies may jeopardize the privacy of patient data and impede the effective communication of privacy measures to patients, which would affect trust and informed consent. However, this limited inquiry might be ascribed to the underlying premise that others bear the responsibility for guaranteeing security and privacy.

4.2.2 Recognition of Inherent Limitations. Four participants (A5, A8-A9, S1) demonstrated some level of skepticism towards the concept of information security, recognizing the significant difficulty in attaining complete security within any digital framework. A5 expressed this sentiment by observing:

> "Nothing is perfect, nothing is impenetrable if somebody really wants in, they're going to get in it." (A5)

By citing real-life instances, such as the multitude of security breaches encountered by prominent corporations such as the 2013 Target data breach, participants emphasized the alarming fact that even the most heavily fortified systems can be susceptible to persistent hackers. This acknowledgment of the inherent limitations of security measures reflects a pragmatic understanding of the complex landscape surrounding information security.

4.2.3 Variation in Security Knowledge and Implementation. The significance of security measures and the level of awareness among telehealth practitioners cannot be overstated, given the highly sensitive and confidential nature of healthcare data. During telehealth sessions, healthcare providers are entrusted with the private medical information of patients, and it is incumbent upon practitioners to fulfill their ethical and legal obligations in ensuring the security and privacy of this data. Insufficient security protocols may result in the occurrence of data breaches, thereby jeopardizing the confidentiality of patient information and potentially inflicting irreversible damage. As such, we try to understand the levels of awareness of our participants as well as the security measures they implement. Seven of our participants (A4, A6, A9, S5, S7-S9) expressed a restricted comprehension of security and privacy, as indicated by S7:

> "Maybe I should preface this by saying I would not consider myself an expert in computer privacy and security by any means so my feelings on it I guess are impacted by my lack of knowledge in the area." (S7)

The acknowledgment of a lack of expertise in computer privacy and security implies that their perceptions or attitudes regarding privacy and security in telehealth are shaped by their restricted understanding in this domain. This suggests possible difficulties in navigating the intricate field of digital security in telehealth, resulting in an increased susceptibility to overlooking crucial security measures. Nevertheless, the majority of participants (A1-A4, A6, A9, S1, S2, S4, S8-S10) recognized the significance of privacy and security. As such, many participants (A7, S7-S8, S10) reported that they rely on assistance in addressing matters pertaining to security and privacy. Both A7 and S10 indicated receiving support and guidance from their respective spouses. Nevertheless, A7 reports depending on the aid of non-experts, to navigate issues related to information technology and cybersecurity:

> "Right now, it is my husband who can help me, and he's not an IT person. He knows enough to fix things and get things done, but he's not an IT professional by trade." (A7)

This reliance on non-IT professional raises concerns regarding possible oversights in ensuring the security of the telehealth environment. underscores the prevalent issue of healthcare professionals lacking IT expertise and resources and depending on personal connections for technical assistance, emphasizing the necessity of guaranteeing sufficient IT resources to adequately handle privacy and security concerns. Furthermore, three participants (A5, S1, S6) have placed significant emphasis on their dedication to ensuring privacy and security, noting that they have implemented extensive measures to protect the confidentiality of their telehealth sessions, demonstrating a proactive stance towards ensuring security. As A5 notes:

> "We do the best and we carry policies and insurances to protect us in the event that [a cyber attack] happens…everything is protected…we do the best that we can in a way that should minimize our risks of hacking we don't open links from emails the whole team knows that, we review it every year, if I have software updates we do them physically through our software we don't do them through links so we do the best that we can." (A5)

Participants such as A5 highlighted their proactive stance towards ensuring data privacy and security in telehealth. They discuss the implementation of policies and insurance coverage as a measure to mitigate the possible impact of cyber attacks, showcasing a strategic approach to risk management. Furthermore, some of our participants emphasized the implementation of precautionary measures, such as refraining from clicking on email links and doing software upgrades manually. It also promotes the cultivation of a collective understanding of these practices across the whole team through periodic evaluations. However, not all telehealth practitioners have the same level of expertise or awareness when it comes to cybersecurity. While some take proactive measures, such as implementing two-factor authentication, access control, auto-logout features, and virtual waiting rooms, others may be less informed due to their professional background, or the resources available to them, or time constraints to acquire knowledge and expertise pertaining to privacy and security:

> "I don't have like a tech background to know like every single thing about Zoom security" (S5)
> "A lot of it in the beginning was just trying to find any resources" (S9)
> "I have to depend on other people to do this because guess what I don't have time and my job is not to do cybersecurity, my job is to take care of patients." (A9)

Our participants highlight the importance of efficient and user-friendly security solutions to overcome gaps in knowledge and time constraints as well as limited resources, in order to ensure effective protection of data in the changing field of digital healthcare. Furthermore, the observed disparity in security awareness and implementation underscores the necessity for continuous education and support in order to improve the security and privacy of telehealth services.

4.3 Data Security and Privacy Concerns

Our participants expressed varying concerns regarding the security and privacy aspects of telehealth. Certain individuals voiced substantial concerns, but others appeared to be less apprehensive or held misunderstandings regarding potential hazards.

4.3.1 Apprehension Over Data Security. Seven out of 20 participants (A9, A10, S4, S5, S7, S9-S10) expressed apprehensions over the security of patient data. Concerns were raised over the poor understanding among vulnerable populations, especially older adults and the younger population, regarding the data usage of their smartphones and the possible vulnerability of sensitive health information to penetration by malicious third parties. These healthcare practitioners have an understanding that hackers might readily exploit weaknesses. As A10 notes:

> "I often work with older adults and sometimes they just have no idea on how much data their phone has and so I try to avoid it as much as possible because all it takes is for them to download the wrong app and then all of this health information is potentially going somewhere." (A10)

This demonstrates the cognizance of our participants about the security and privacy risks linked to using smartphones, particularly for older individuals who may have little comprehension concerning the data kept on their devices. This also demonstrates that certain participants in our study are actively striving to decrease reliance on personal devices and prefer secure platforms to ensure the confidentiality of health information during telehealth sessions.

However, in contrast, eleven respondents (A1, A4-A7, S2-S4, S8-S10) had a lesser degree of concern over security issues. Some participants exhibited a certain level of naivety and indicated a lack of prior experience with any challenges. The seeming nonchalance expressed by individuals may be attributed to a perception that their telehealth platforms have robust security measures, as A6 states:

> "We have not had any security concerns with any aspects of telehealth. The third-parties we use are all healthcare entities and know the importance of security and consequences if there are issues." (A6)

This statement shows the confidence some of our participants in the security of their telehealth practices, as well as their confidence in the third-party software providers they use highlighting their apprehension towards security and the potential consequences in case of issues. It also indicates a dependence on reliable third-party services in the healthcare industry, with the anticipation that they prioritize strict security measures to protect patient data. On the other hand, this seeming nonchalance can also be due to underestimating the possible threats involved. In fact, when asked about whether they had any privacy or security concerns, S9 answers:

> "I don't, and part of that's being naive but we haven't had any issues ever." (S9)

Through this declaration, S9 acknowledges that they do not have any privacy or security concerns in telehealth. It suggests that this lack of worry may be due to a combination of inexperience and a lack of observed problems. This remark implies a possible lack of knowledge or aggressive actions regarding the protection and

confidentiality of data in their telehealth services. Although the lack of detected flaws is acknowledged, the possible consequences of ignorance are worrisome as they may lead to the oversight of vulnerabilities, hence leaving patient data susceptible to unauthorized access or breaches.

Furthermore, two participants (S1 and S7) displayed a conspicuous absence of concern over privacy and security in the context of telehealth. For example, the lack of concern exhibited by S1 towards parents allowing their children to conduct sessions from unsecured settings demonstrates a level of acceptance towards patient activities that might potentially jeopardize security. Moreover, this nonchalant attitude gives rise to apprehensions over possible breaches in data security and privacy. Allowing sessions in less secure contexts might potentially expose sensitive information to undesired individuals, hence increasing the risks of eavesdropping or unlawful access.

> "Parents choosing to sign on with their phone in the middle of a parking lot…if they want to do that that's fine…I don't care." (S1)

Allowing sessions in less secure contexts might potentially expose sensitive information to undesired individuals, hence increasing the risks of eavesdropping or unauthorized access. Which emphasizes the necessity for explicit protocols and instruction on secure telehealth practices to protect the privacy of healthcare interactions. Similarly, S7 minimizes the significance of eavesdropping by drawing a comparison to a group therapy session within the occupational therapy realm.

> "We also have a shared like computer space where multiple people are working at the same time and sometimes we will do a telehealth session from there, so there are times when I might be walking by and see someone else's telehealth session happening which in my mind is pretty similar to walking by a therapy room and hearing a session happen or in the occupational therapy world. A lot of times there's just a shared gym space and lots of kids are having therapy in the same space so it's all within the clinic building so I see it as confined in the same way as those other situations." (S7)

This analogy implies that the perceived level of security in telehealth is on par with that of in-person sessions conducted within the controlled environment of a clinic facility. However, this analogy is flawed as it neglects to recognize a crucial contrast between traditional treatment sessions done in person and telehealth sessions carried out via digital platforms. In the context of in-person treatment, all participants possess a broad awareness of their physical environment and the presence of others within the shared therapy space. Conversely, in the context of telehealth sessions, individuals could lack awareness of the absence of a private environment. Telehealth relies on the assumption of a private and secure digital environment, and patients expect that their conversations and sensitive information are protected from eavesdropping or unauthorized access, when in fact these conditions are not always met.

4.3.2 Concerns Over Platform Security. Two participants (A2 and S6) voiced an alternative viewpoint that centers on apprehensions over their own privacy as well as the privacy of persons unintentionally captured on camera during telehealth meetings. The participants placed significant emphasis on the possibility of patients or their parents recording or assuming control of a session, showing greater concern over these situations compared to external hackers. As S6 states,

> "A concern that the client or the parent was going to record the session or take over the session. I think I was more concerned about those people than [a] cyber hacker." (S6)

Our participants responses depict the difficulties that professionals encounter in guaranteeing the privacy of telehealth conversations. Considering data privacy and security, concern emphasizes the necessity of implementing steps to avoid unintentional disclosure of sensitive information by participants during the session.

A2 additionally brought attention to the frequently disregarded matter of privacy concerning those inadvertently present in the backdrop of telehealth meetings, encompassing both family members and unfamiliar individuals. These circumstances have the potential to cause unease for all those involved, including the service providers, since they may unintentionally bear witness to intimate moments or confidential information that was not intended for disclosure. A2 explained that:

> "Privacy is not just about the person who's on camera but also the people who are inadvertently on camera in the background. I'm sure everybody has experiences like this, but I've had siblings, spouses, children, strangers who show up in the background without knowing that they're on camera and that can lead to uncomfortable situations for them and for the providers sometimes." (A2)

The remarks made by this participant highlight the intricate aspects of privacy within the realm of telehealth, wherein the delineation of personal boundaries and inadvertent exposure emerge as noteworthy considerations, particularly in the context of utilizing video conferencing technology.

Six participants (S1-S2, S5-S6, S9-S10) conveyed apprehensions regarding security breaches, specifically citing instances such as Zoom bombing that occurred during the peak of the COVID-19 outbreak. Despite lacking personal experience with such attacks, the sheer awareness of their existence heightened their perception of vulnerability and underscored the necessity for implementing comprehensive security measures. As S6 notes,

> "I heard about [Zoom bombing] happening during our transition to telehealth, students being able to kind of take control of the screen, and then present their screen or inappropriate material to other people …that's obviously a concern and that I did hear about situations like that happening to providers and teachers during the very beginning of the pandemic." (S6)

4.4 Trust and Confidence in Telehealth Security

The study's participants demonstrated a range of trust levels about the security and privacy features of telehealth technology. At one

extreme of the continuum were those who publicly articulated a profound sense of skepticism towards many entities, encompassing software suppliers among others (A3, A10, S6, and S8). The mistrust exhibited by individuals was mostly based on apprehensions over the protection of personal data, as S8 states when asked whether they trust their software provider:

> "No, I don't really trust anybody with anything to be honest. The fact that you could say something and suddenly on Facebook there's all these ads for is scary." (S8)

This participant had an increased sense of unease over the wider security environment. This statement also demonstrates a dearth of confidence in diverse institutions, emphasizing apprehensions around internet spying and data monitoring.

4.4.1 Trust in Organizational Decision-Makers. Several participants (A4, A6, A10, S7, S10) shared a perspective influenced by their professional positions within their respective organizations. These participants hadn't been in decision-making positions and held the belief that it was not incumbent upon them to evaluate or execute security protocols. Conversely, the individuals or teams responsible for these tasks were entrusted with the responsibility, as it was believed that the encryption levels and security measures were in accordance with the requirements outlined by HIPAA. From these participants' perspective, their main responsibility was to offer therapeutic services, while they entrusted the complexities of security to individuals whom they perceived as being more capable of making well-informed judgments. S7 states that:

> "I haven't been in a decision making position in the jobs that I've had have. I'm just a therapist working at a private practice so in that way from my perspective I am putting a lot of trust in the people making the decisions…and then I just kind of do what I'm told because in my eyes it's not my job to make sure those things are done so I'm just trusting that they are done." (S7)

We notice a dependence on the decisions taken by others and view it as outside their responsibility to ensure the implementation of security and privacy measures. This position may present potential vulnerabilities, since it implies a passive attitude to privacy and security. In contrast, nine participants (A3, A5-A9, S4, S6-S8) expressed comparatively diminished apprehensions pertaining to the security and privacy aspects of telehealth technology. The rationales for this exhibited notable disparities. A certain cohort displayed a sense of assurance in the individuals responsible for decision-making within their respective organizations, who diligently scrutinized the software employed. The individuals held the belief that the provision of their tools by these entities engendered a sense of security. As S8 explains:

> "What I use is through the district so I feel like it's pretty safe it's not just like open to the public." (S8)

The demonstrated trust in decision-makers highlights the influence of different roles and organizational structures on perceptions of security in telehealth. From a perspective of data privacy, using a platform sponsored by the district indicates compliance with institutional security procedures. Nevertheless, it is crucial to acknowledge that institutional backing does not provide complete security, underscoring the continuous requirement for alertness and best practices to ensure patient data confidentiality during telehealth sessions.

4.4.2 Trust in Software Providers. Several participants expressed concerns, especially regarding the security and privacy of certain technological platforms. S6 expressed their lack of faith in the Zoom platform, particularly with regard to concerns about password encryption and stability issues, which ultimately resulted in their decision to cease using it:

> "I think I didn't trust Zoom to work with the password encryption version because it wasn't working so I stopped using it." (S6)

Similarly, A10 expressed apprehensions over the insufficiency of comprehensive details pertaining to the security protocols employed by third-party applications utilized in telehealth, even in cases when they are supported by the makers of the devices.

> "What I didn't feel comfortable with and where I had concerns is I didn't have a lot of information about the specific training companies and their apps for remote programming…[Manufacturers] have been telling that their system is secure however I just didn't have any information other than the manufacturer's word on that." (A10)

A subset of participants exhibited a significant level of trust in their software providers (A4, S1, S3-S5, S7, S9-S10). Several participants noted that they had not encountered any significant usability issues with the software provider they had adopted. Over the course of time, these participants' confidence in the technology grew stronger, especially as they encountered seamless and problem-free engagements with the platform. For these interviewees, the absence of technical malfunctions and usability issues was a testament to the software's overall reliability. This is corroborated by S5's response:

> "I really haven't had a ton of concerns especially as time has gone on. Maybe these things have just been going pretty smoothly." (S5)

S4 notes:

> "I do just trust the platform is maintaining security on their end." (S4)

The trust in the system and technology is sometimes ascribed to the company's established reputation and credibility. The platform was perceived by users as a reputable organization that placed a high emphasis on security, thereby mitigating apprehensions regarding the security and reliability of data. As A3 states:

> "You get what you pay for so we feel comfortable that Blueprint has our best interest at heart and they provide a quality service as well." (A3)

This trust our participant showed their software providers demonstrates a firm belief in their capacity to prioritize data privacy and security. The consequence is an assumption that the software providers' high-quality service includes robust measures for protecting sensitive patient information during telehealth sessions. The

existence of different degrees of trust and the various circumstances that have impacted them highlight the intricate nature of security and privacy views among the telehealth practitioner community.

4.5 Patient Attitudes Toward Security and Privacy

Participants in the interviews provided a range of perspectives on their patients' views regarding the security and privacy aspects of telehealth. Four participants (A3-A4, A8, S6) observed that the patients they encountered placed a higher emphasis on the convenience and user-friendliness of telehealth services compared to any concerns regarding security. Indeed, A8 implies an emphasis on technological disruptions above proactive efforts for data privacy and security. The potential outcome is the possibility of disruptions in telehealth sessions, which might affect the smooth provision of healthcare services.

> "As far as security, no not at all, just a couple of times where the internet has been a problem that's been a frustration on both ends." (A8)

In the case of these individuals, prioritizing the accessibility and efficacy of telehealth in meeting their healthcare requirements superseded concerns regarding security. In fact, when asked whether their patients have ever voiced any concerns over the security and privacy of telehealth, A9 answered:

> "No, they don't feel good they don't hear well that's all they care about." (A9)

This concession that patients do not voice concerns regarding the security and privacy of telehealth indicates a potential lack of patient awareness or engagement with the security aspect of telehealth, emphasizing their primary focus on health issues.

Concerns regarding data logging and the collection of information during telehealth sessions were expressed by some patients, as reported by A10. According to A10, some patients worry about the potential recording of sensitive conversations, despite the primary focus of data logging being on non-verbal information, such as usage patterns in various contexts. This concern emphasizes the delicate nature of patient anxieties regarding confidentiality. In fact, A10 reveals:

> "Patients are concerned about [data logging] on occasion. To them, it might be concerning like 'oh are you recording this information?' I mean how can you record conversations? There might be private conversation I can say with confidence that it's not recording any actual conversation but those are concerns that the patients have and so the data logging can be a super helpful tool but that's the one that patients are often concerned about." (A10)

Conversely, two participants (A2 and S4) reported cases in which patients demonstrated a pronounced inclination towards telehealth as a result of their concerns regarding privacy. S4 provided an example of a particular patient who made the decision to utilize telehealth services to obtain therapy discreetly, thereby circumventing the need for in-person appointments that might inadvertently disclose their condition to individuals within a close-knit community. Telehealth thus allowed this patient to make progress, stressing the significance of service accessibility in influencing patient decisions, stressing the necessity for more extensive telehealth options to tackle privacy apprehensions and accommodate varied healthcare requirements.

> "[A patient] came in for the evals for [physical therapy (PT)] and [occupational therapy (OT)] and speech, but would not come back for treatment and I had suggested that we try telehealth and he was open to it. He was there twice a week did amazing…but would not come into the clinic for PT and OT and I think it was because he maybe knew it was a small community and he didn't want anyone to see him receiving therapy. Our PT and OT didn't offer telehealth at the time, so he just went without those services." (S4)

In a similar vein, A2 observed that telehealth proved to be a viable option for individuals occupying sensitive roles within their professions, as they harbored heightened apprehensions regarding their privacy and confidentiality. These individuals opted for telehealth services to protect the confidentiality of their personal and medical information. They highlighted that telehealth may be particularly suitable for specific patient demographics that place a greater emphasis on privacy sensitivity. As A2 states:

> "It's really only for specific patients who are very worried about the information that they're sharing being sensitive for their career." (A2)

4.6 Comparative Discussions for Audiologists and Speech Language Pathologists

Within our study, a significant demographic contrast arose between audiologists and SLPs regarding the patients they serve. Forty percent of the questioned audiologists (A3-A4, A6, A10) specifically said that a substantial proportion of their patients were "older adults." Conversely, a lesser percentage of SLPs indicated dealing with older adult patients, with 8 of them (S1, S3-S9) stating that they primarily focus on treating younger patients. This differentiation is essential as this patient demographic frequently face difficulties with technology, a characteristic that significantly impeded their adoption of the shift to telehealth. Several audiologists have seen a dearth of approval or enthusiasm among their primarily older patient demographic about telehealth as A3 states:

> "A lot of our population is elderly and we didn't see a real acceptance or excitement to try it [telehealth]" (A3)

Audiologists highlighted the challenges their patients had while adjusting to digital platforms, revealing a significant obstacle to the mainstream acceptance of telehealth among this particular group even during the peak of the COVID-19 outbreak, as A4 explains:

> "For most of our patient population which is older adults over the age of 65 typically they just would rather come in person to talk to someone…when we offered the telehealth appointments most of them say I'll just come in…I think our patients feel comfortable coming in despite all the precautions and the risk there was before we had [COVID-19] vaccines" (A4)

This also correlates to the overall quantity of telehealth services provided by each group. During 2021, audiologists, on average, provided less than 20% of their sessions through telehealth. Among them, only A2 conducted more telehealth sessions than in-person sessions. In contrast, 4 out of 10 SLPs almost exclusively delivered care through telehealth sessions. Furthermore, audiologists emphasized the technological literacy difficulties faced by their elderly patient demographic on many occasions as well as lack of technology in other cases, as A6 confirms:

> "Our patients really don't have the technology to actually do it [Telehealth] unless they have like a daughter or a family member that's there" (A6)

These patients who lack the necessary devices or digital skills for telehealth, may depend on technologically savvy family members for help, this dependence brings about certain security weaknesses, since family members may interact with the technological elements, putting sensitive health information at risk of unintended disclosure.

On the other end of the spectrum, SLPs emphasized the difficulties encountered in telehealth sessions, particularly with younger children. These children's parents have expressed discontent with the efficacy of telehealth sessions in the early stages of the epidemic. Several participants observed that parents often voice dissatisfaction with the progress made during telehealth sessions and express a preference for in-person therapy, as A4 explains:

> "Parents of now three or four year olds will come in and say that …during the pandemic or the early pandemic they were in therapy that was all virtual and it was very challenging and didn't seem to help at all I hear that comment a lot and then they were eventually be able to find someone providing SLP in person and then usually their parents will report that they started seeing progress once the child was in person" (S7)

This implies that the physical and interactive aspects of in-person therapy may be more advantageous for very young children. It also emphasizes the pragmatic challenges and limitations of telehealth for certain age groups. It implicitly emphasizes the significance of customizing telehealth methods to address the particular requirements and phases of growth of patients.

Our study revealed a nuanced spectrum of perceptions regarding security and privacy was observed among both SLPs and audiologists engaged in telehealth practices. While variations existed within each group, an interesting trend surfaced: a comparatively higher awareness of cybersecurity risks among audiologists. Notably, a greater number of audiologists displayed awareness of the complexities and possible dangers related to cybersecurity in the telehealth setting. The increased consciousness can be ascribed to the unique difficulties audiologists encounter, especially when working with elderly adults who are less acquainted with digital tools. Nevertheless, it is essential to recognize that there were differing perspectives within both occupations. Remarkably, two SLPs (S8, S10) and one audiologist (A8) stated that they would have greater apprehensions regarding cybersecurity if they were involved in a different profession as we can see in the following quotes:

> "[For] most of the students I work with, it's mild to moderate articulation or stuttering…I'm not doing like psychotherapy." (S10)
>
> "If I were in a different kind of healthcare then I could see maybe some concerns but the kind of stuff I deal with is out in the open, it's not things that people are trying to be quiet about or concerned that anybody's gonna find out about…and I might be less inclined to do as much telehealth as I do just because it would be more sensitive information" (A8)

This viewpoint implies that there may be a tendency to underestimate the security threats related to telehealth. It highlights the importance of being cautious in protecting even seemingly non-sensitive information in order to preserve patient privacy. Furthermore, these admission highlight the fact that cybersecurity issues are influenced by the unique professional domains within the allied healthcare industry, and that individuals' perspectives are shaped by their unique environments, which is influenced by the perceived sensitivity of the information being handled.

5 IMPLICATIONS

Telehealth, a rapidly emerging domain in the healthcare industry, offers a promise of unprecedented flexibility as reflected in its adoption trajectory. At its core, the telehealth paradigm facilitates remote health services for people in need, bridging the geographical divide, and making healthcare more accessible. Drawing from our earlier discussions, we find that audiologists and SLPs hold diverse opinions and experiences about telehealth security and privacy. Our interviews underscore a consensus that security and privacy considerations should harmoniously complement the main objective of healthcare delivery. The present insights from telehealth studies illuminate significant implications for healthcare professionals, researchers, service providers, software vendors, and policymakers.

5.1 Duality in Flexibility

As our participants discuss, the primary driver for this shift towards telehealth adoption often hinges on the flexibility it affords to both patients and practitioners. Our participants also acknowledge that unique communities, whether defined by geographical constraints or socio-cultural factors, particularly benefit from telehealth (see quote from S4 in Section 4.5). For professionals in high-profile or sensitive job roles, the benefit of telehealth lies in its promise of discretion, ensuring their health consultations remain confidential and free from public scrutiny [3] (see quote from A2 in Section 4.1.2). Similarly, for individuals who are reliant on external means of transportation—be it due to financial constraints, physical disabilities, or other reasons—telehealth provides a consistent and convenient avenue for access to healthcare without the hassles of travel [31].

However, the very flexibility that makes telehealth appealing also brings to the fore several challenges, especially in the realms of security and privacy. Our interactions with practitioners shed light on a spectrum of concerns. A recurrent theme was the potential for unauthorized recording of sessions, notably by parents or caregivers (see quotes from S6 and A2 in Section 4.3.2). Such recordings, besides infringing on patient-practitioner confidentiality, could pave

the way for unauthorized dissemination of proprietary therapy and care techniques. This could have cascading effects, from privacy violations leading to trust issues between patients and providers, to potential legal and ethical ramifications. Another emergent concern revolved around the unintended intrusion of caregivers or parents into telehealth sessions (see quote from A2 in Section 4.3.2). Such intrusions, whether inadvertent or deliberate, compromise the session's sanctity, potentially derailing the care trajectory and jeopardizing patient privacy. Adding another layer of complexity, practitioners also highlighted an emerging trend: patients attending sessions from unconventional or unsecured locations (see quote from S1 in Section 4.3.1). Such practices not only introduce additional variables into the care process but also lead to practitioners feeling undervalued or disrespected. Our findings also underscore a significant concern that often remains in the backdrop: the vulnerability of specific patient segments.

While some population groups gain accessibility with telehealth, others fall behind. For instance, elderly individuals, often not as technologically adept, may struggle with platform intricacies [6] (see quote from A10 in Section 4.3.1). Similarly, there is evidence that neurodiverse adults might find the transition to digital platforms overwhelming [88]. As the telehealth industry evolves, addressing accessibility issues of people with additional needs should be at the forefront, especially when it comes to the protection of healthcare data. The majority of past research discusses the opportunities that telehealth offers [74, 85]. This work extends this body of literature by highlighting the challenges that come with the flexibility that telehealth offers, challenges associated with ensuring the privacy of patient information, preventing unauthorized use of therapy and clinical interventions, and inclusion of people with different abilities.

5.2 Recommendations for Increasing Trust in Telehealth Technologies

Trust is fundamental to the adoption and continued use of telehealth as mentioned by our participants (see Section 4.4) and shown through prior works [84]. A synthesis of our participant feedback suggests that trust towards telehealth is multifaceted, and bears significant consequences for platform developers and healthcare providers alike. Our findings suggest that a comprehensive discussion about trust necessitates a thorough understanding of its many elements and drivers. Direct and indirect user experiences lay the foundation for trust.

People often favor technologies that have strong reputation, garnered positive feedback, or have secured commendable reviews from both their peers and industry experts [21]. This is a form of institutional trust: that learned towards a specific brand and/or institution [2]. Similarly, healthcare technology providers that have a strong reputation in a community were favored by the providers and more importantly, were trusted to prioritize security and privacy (see quote from A3 in Section 4.4). However, complete transparency regarding the collection, processing, and storage of data by telehealth providers is demanded [41] (see quote from A10 in Section 4.4). Platforms that champion this information transparency would position themselves favorably in the trust spectrum [56]. An absence of understandable and readily available information could foster mistrust, particularly if users perceive they are wading through a quagmire of technical jargon. Despite the strong reputation and transparency, some providers may be apprehensive about adopting telehealth technologies due to dispositional trust - individuals' propensity to trust technologies [34]. Participants in this work did not discuss dispositional trust as a factor but we posit that it may play a significant role in telehealth adoption.

Trust is also a dynamic construct that is established over time through individual interactions with technology [55]. Error-free interactions with emerging technologies (automated process controls, adaptive cruise controls, autonomous driving) have been shown to consistently increase trust over time [58]. Likewise, several providers in this work mentioned how error-free interactions with telehealth technologies have influenced them to perceive the system to be reliable and trustworthy (see quote from S5 in Section 4.4). However, this doesn't necessarily suggest that providers are over-trusting, but the contrary: participants understood the telehealth technologies could be vulnerable to threats (see quote from A5 in Section 4.2.2). It is expected that technologies that fail should lead to a temporary reduction in trust [50]. They typically stem from one's own firsthand experience of errors encountered while using the technology. However, providers in this study noted stories about security attacks (on healthcare systems or otherwise) as a cause for degraded trust. For example, Zoom which is one of the most prevalent videoconferencing platforms used by healthcare providers has experienced several data breaches which may contribute to trust degradation [67]. Providers also noted personal experiences as causes for trust degradation. For example, authentication errors, while they might seem minor, can have grave implications such as privacy violations, data breaches, and operational inefficiencies [54] (see quote from S6 in Section 4.4). Such issues don't just hamper the individual workflows but also cast doubts over the platform's overall reliability especially when it comes to healthcare data.

When providers aren't the main agents choosing the technology, trust is indirectly anchored on the credibility of the decision-maker(s). This is a notable dimension of trust and decision-making that emerged from interviews with the providers in this work - a form of distributed trust and decision-making (see quote from S7 in Section 4.4.1). While it reduces the burden on providers by enabling experts in information and computing technology to adopt and manage telehealth technology, it also brings unique challenges and opportunities. We characterize this as distributed trust because individuals (IT experts) who are making the adoption decisions based on initial institutional and dispositional are distinct from individuals (providers) who are learning to trust based on their interactions with telehealth technology. Such a distributed trust relationship may introduce misaligned priorities and trust levels. For instance, the technology may be trustworthy from a deployment and management perspective but unreliable from a regular interaction perspective. Likewise, there may be instance of over-trust that emerges from such distributed trust relations (see quotes from S7 and S8 in Section 4.4). Also, in scenarios where a suggested platform underperforms, who is accountable for the patient data? Establishing well-defined lines of responsibility and involving users (providers) in early phases of decision-making may preempt potential future disputes.

Finally, healthcare providers should be leveraging business associate agreements (BAAs) with telehealth technology providers including Zoom or Google, as required under HIPAA. These legal documents can help offset risk by requiring third party vendors to protect PHI. Although, all our participants emphasized their commitment to complying with HIPAA regulations in respect to the technology they use and their operational processes, only four participants mentioned having or relying upon BAAs with telehealth platform providers to protect PHI or manage security and privacy liability.

5.3 Recommendations for Training and Awareness of Security Hazards

Within the healthcare industry, it is broadly acknowledged that training is paramount for compliance efforts [4, 81]. All the participants practiced in the United States and are required by law to know and comply with HIPAA. While HIPAA provides flexibility in implementing obligatory security and compliance measures, participants often demonstrated limited awareness of these requirements (see Section 4.2). More concerning is the variation we observed in participants' awareness of threats and understanding of the necessary actions. Many were understandably anxious while few others reported to be taking actions (safe practices, investing in IT resources) to prevent a breach and buying insurance to cover losses in the event of a breach. This resulted in a deficiency in their understanding of potential security and privacy threats. Every healthcare professional—not just business owners—is accountable for HIPAA compliance.

This prevailing variation in awareness and responsibility about security threats amongst healthcare providers has the potential to compromise patient data, thereby undermining the efficacy of telehealth services. Comprehensive training tailored to telehealth could ameliorate these risks. Specialized telehealth awareness becomes pertinent given that the attack surface for telehealth distinctly deviates from traditional in-person information exchanges. This distinction was often misconstrued by participants (see quote from A2 in Section 4.2.1). Telehealth introduces an intermediary third-party communicator, a novel internet-based data transmission, and a unique patient connection environment. Although awareness of security and privacy threats is a prerequisite for compliance, current evidence doesn't conclusively establish that such awareness indeed minimizes data breaches or other similar incidents [10].

Current medical and state licensure processes should adopt mandates for specific knowledge in cybersecurity and privacy. This would fit within state licensure that typically necessitates a set duration of continuing education. Incorporating telehealth cybersecurity training, either as an essential prerequisite for conducting telehealth or as an elective within continuing education, seems judicious. Most private clinics have the budgets to support continuing education. Given the ceaselessly evolving cyber threat landscape, instating telehealth security training as an imperative appears indispensable. Periodic continuing education will ensure healthcare providers stay updated on emerging challenges and their countermeasures [17].

5.4 Telehealth Service Providers and Software Vendor Recommendations

Telehealth hinges not only on technological innovation but also on a symbiotic balance between usability, security, and privacy. As pivotal stakeholders, telehealth service providers and software vendors wield the unique responsibility to ensure that software architecture and deployment strategies align with the best interests of both practitioners and patients. Given the sensitive nature of healthcare data, it is imperative for vendors to build applications from the ground up with security in mind. Ensure that data, both at rest [11] and in transit [70], undergoes end-to-end encryption [52]. This diminishes the risk of unauthorized access or breaches during transmission between client and server or while stored. Undertake regular penetration testing and vulnerability assessments to identify [87] and rectify potential weak points in the system before malicious entities exploit them.

Embedding privacy controls from the onset can mitigate potential risks in data handling and processing is critical. We recommend incorporating comprehensive consent management tools that enable patients to have granular control over who accesses their data, how it's used, and for what purpose [14, 25]. Adhering to the principle of data minimization [73], such a solution could ensure that only essential data is collected and stored. This reduces the potential attack surface and exposure. Additionally, engagement with industry experts and practitioners to develop specialized guidelines tailored to address the unique challenges such as difficulties observing subtle communication cues that help SLPs assess articulation, fluency and overall communication effectiveness, or difficulties with calibration and standardization faced by audiologist, as well as limited ability to assess sound perceptions and understanding speech in noisy environments faced by both audiologists and SLPs in telehealth will be helpful. This requires collaborations with regulatory bodies, institutions, and practitioners to continuously refine and update standards, ensuring they remain relevant in the face of evolving technological landscapes. Additionally, while intuitive interfaces play a pivotal role in encouraging telehealth adoption, it is crucial to strike a harmonious balance where ease of use doesn't jeopardize security protocols. We recommend integrating adaptive authentication mechanisms, which adjust authentication challenges based on contextual factors such as user behavior or device integrity. This aligns with the experiences of certain participants who have raised concerns about the usability of certain telehealth platforms, namely for patients who struggle with account creation and session login and authentication as S6 notes:

> "there were like multiple steps for the secured Zoom... it wasn't as easy as just click on this button and you can enter my teletherapy space. It was just too many steps for the population I was working with." (S6)

Incorporate interactive training modules within the software to guide practitioners and patients on best practices to maximize security during telehealth interactions. The guidance provided by NIST 1800-30B – a US-centric standard– serves as a foundational starting point for constructing robust telehealth platforms [18].

5.5 Policy Recommendations

As the adoption of telehealth services continues to burgeon, regulatory frameworks must concurrently evolve to adequately address the nuanced challenges introduced by this digital transformation. While HIPAA has traditionally acted as a cornerstone in healthcare data protection, with technology-agnostic requirements, the advent of telehealth demands specific refinement [65, 77]. The integration of more explicit telehealth-centric clauses can elevate the overall efficacy of this regulation. Detailed guidelines are needed for delineating the recommended practices for virtual patient interaction. This can span aspects like maintaining visual privacy, ensuring session confidentiality, and utilizing secure communication channels. From our work, we see an over-reliance on systems, thus periodic security audits for telehealth platforms are needed. By ensuring they align with the stipulated security standards, it becomes possible to preemptively identify and rectify vulnerabilities. Addressing the constraints of the Office for Civil Rights (OCR) is equally paramount. As the entity tasked with overseeing compliance, fortifying its capabilities can significantly augment the enforcement landscape [61].

The initiatives such as the Audiology and Speech-Language Pathology Interstate Compact (ASLP-IC) are commendable as they foster a consistent standard of care across states [8]. Amplifying this approach can involve the creation of a unified cybersecurity and privacy standard that professionals must adhere to, regardless of the state they practice in. The development of a collaborative ecosystem could allow professionals to share their telehealth experiences, challenges, and insights. A peer review mechanism can help disseminate recommended practices and novel solutions across the community.

5.6 Patient-Related Concerns and Recommendations

As the telehealth landscape continues to evolve, a prominent issue emerges from people accessing services from unregulated or uncontrolled environments. Such scenarios inadvertently introduce a plethora of security vulnerabilities that remain challenging to circumvent. Even though consent documents can apprise them of these associated risks and furnish a legal safety mechanisms, relying solely on these documents doesn't inherently bolster security or privacy in real-world applications [23]. Providing educational resources is pivotal to navigate this quandary. But it is not merely about creating materials; it's about crafting comprehensive guidance tailored for diverse patient profiles. Let's delve deeper into the potential facets of this approach: Interactive, easy-to-follow online tutorials can be designed to guide patients through the steps of setting up a secure environment. This could range from securing their WiFi networks, such as enabling virtual private networks, to understanding the basics of end-to-end encryption.

A concise, printable checklist can ensure that people using telehealth follow a standardized protocol before initiating a telehealth session. This can include actions like finding a private location, ensuring their device's software is updated, and checking the security settings of the telehealth application. After patients undergo a telehealth session, prompt them to provide feedback regarding their security experience. This could inform areas where the educational materials might need refinement. The realm of cybersecurity is constantly evolving. Thus, it is essential to provide patients with regular updates about new threats or security measures. An automated monthly newsletter or notifications within the telehealth platform can serve this purpose effectively. Different patients may face diverse challenges based on their locations, tech-savviness, and the devices they use. Offering guidance based on specific scenarios can make the advice more actionable and relevant. By incorporating these facets, we can empower people using telehealth to take charge of their security and ensure that telehealth services remain both accessible and secure.

6 FUTURE WORK AND LIMITATIONS

Our work offers invaluable insights into the privacy and security concerns and perceptions of allied healthcare practitioners regarding telehealth. It is important to note that all participants in our study were audiologists and speech-language pathologists actively engaged in private practice settings. This deliberate selection ensured a comprehensive grasp of the distinct experiences and challenges these professionals face. Moving forward, our research will expand to include a broader spectrum of healthcare experts. Additionally, the experiences of patients remain critical. Hence, in our future research we will incorporate patients' perspectives, recognizing their essential role in shaping telehealth interactions.

While our qualitative study provides rich insights, certain inherent limitations must be acknowledged. A primary limitation stems from generalizability concerns. Our sample consisted exclusively of audiologists and speech-language pathologists in private practice, which allowed an in-depth understanding of this group's perspectives. However, the findings may not generalize to other allied healthcare professionals or those in non-private practice settings. Future studies should incorporate a wider range of participants across various allied healthcare disciplines and practice types to determine if the themes hold true more broadly. Additionally, our sample exhibited some skewness in gender distribution. This disproportionate gender distribution could introduce potential bias, although it is reasonably representative given. Still, incorporating a more balanced gender mix could reveal differing viewpoints. Furthermore, qualitative research relies heavily on participants' memories and willingness to share openly. Biases such as selective memory, recency effects, attribution errors, and social desirability biases may shape participant responses during interviews. Observations and surveys could complement interviews to mitigate some biases. Overall, our findings establish an important foundation for future research to build upon through broader, more diverse samples, mixed methods, and longitudinal tracking of telehealth privacy and security perceptions among allied healthcare professionals.

7 CONCLUSION

The telehealth paradigm in allied healthcare, particularly exemplified by audiologists and SLPs, poses intricate challenges concerning data privacy and security. We conducted an extensive qualitative analysis involving 20 healthcare professionals spanning audiologists and SLPs over six months. This study shows critical nuances in privacy and security, accentuating the exigency for bespoke solutions tailored to address its unique complexities particularly

from the providers' perspectives. Our findings shed light on a diverse spectrum of views regarding the robustness and credibility of existing technologies, trepidation surrounding privacy breaches and security, as well as the subsequent patient behaviors towards the providers. Notably, participants expressed that the pressures of their primary medical duties sometimes overshadow the imperative nature of patient data confidentiality. This often results in the inadvertent relegation of data security and patient privacy significance, constraining their ability to suitably address these issues. Based on our study, we advocate for the implementation of both secure and user-centric telehealth systems. Complementing these with rigorous training modules could potentially diminish the supplementary burdens borne by healthcare practitioners.

ACKNOWLEDGMENTS

This work was partially supported by a grant from Cisco. We thank the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Laboratory at the University of Denver. Special thanks are extended to Archana Nandakumar for her assistance in conducting the thematic analysis. We would also like to thank our participants for their valuable insights. Any opinions, results, conclusions, or recommendations stated in this material are exclusively those of the writers and may not necessarily represent the perspectives of the University of Denver, the University of Washington, and the Designer Security.

REFERENCES

[1] Alaa A Abd-alrazaq, Noor Suleiman, Khaled Baagar, Noor Jandali, Dari Alhuwail, Ibrahem Abdalhakam, Saad Shahbal, Abdul-Badi Abou-Samra, and Mowafa Househ. 2021. Patients and healthcare workers experience with a mobile application for self-management of diabetes in Qatar: A qualitative study. *Computer Methods and Programs in Biomedicine Update* 1 (2021), 100002.

[2] Afua Adjekum, Alessandro Blasimme, and Effy Vayena. 2018. Elements of trust in digital health systems: scoping review. *Journal of medical Internet research* 20, 12 (2018), e11254.

[3] Zia Agha, Ralph M Schapira, Purushottam W Laud, Gail McNutt, and Debra L Roter. 2009. Patient satisfaction with physician–patient communication during telemedicine. *Telemedicine and e-Health* 15, 9 (2009), 830–839.

[4] Julie L Agris and John M Spandorfer. 2016. HIPAA compliance and training: a perfect storm for professionalism education? *The Journal of Law, Medicine & Ethics* 44, 4 (2016), 652–656.

[5] Mohammed A Ahmed, Hatem F Sindi, and Majid Nour. 2022. Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy* 2, 4 (2022), 853–861.

[6] Manal Almalki, Majid H Alsulami, Abdulrahman A Alshdadi, Saleh N Almuayqil, Mohammed S Alsaqer, Anthony S Atkins, and Mohamed-Amine Choukou. 2022. Delivering digital healthcare for elderly: a holistic framework for the adoption of ambient assisted living. *International Journal of Environmental Research and Public Health* 19, 24 (2022), 16760.

[7] American Speech-Language-Hearing Association. 2023. https://www.asha.org/

[8] American Speech-Language-Hearing Association et al. 2021. Audiology and Speech-Language Pathology Interstate Compact (ASLP-IC).

[9] Ramakrishna Ayyagari. 2012. An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security* 8, 2 (2012), 33–56.

[10] Maria Bada, Angela Sasse, and Jason Nurse. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. In *International Conference on Cyber Security for Sustainable Society*. Coventry, United Kingdom, 118–131.

[11] Shu-Di Bao, Meng Chen, and Guang-Zhong Yang. 2017. A method of signal scrambling to secure data storage for healthcare applications. *IEEE Journal of Biomedical and Health informatics* 21, 6 (2017), 1487–1494.

[12] Sharon Bassan. 2020. Data privacy considerations for telehealth consumers amid COVID-19. *Journal of Law and the Biosciences* 7, 1 (2020), lsaa075.

[13] Anne Brady. 2007. Moving toward the future: Providing speech-language pathology services via telehealth. *Home Healthcare Now* 25, 4 (2007), 240–244.

[14] Kelly Caine, Spencer Kohn, Carrie Lawrence, Rima Hanania, Eric M Meslin, and William M Tierney. 2015. Designing a patient-centered user interface for access decisions about EHR data: implications from patient interviews. *Journal of General Internal Medicine* 30 (2015), 7–16.

[15] Teresa M Camarines and John Christopher M Camarines. 2022. Discussing data security and telehealth during the COVID-19 pandemic. *Journal of Public Health* 44, 3 (2022), e449–e450.

[16] Deborah R Campbell and Howard Goldstein. 2021. Genesis of a new generation of telepractitioners: The COVID-19 pandemic and pediatric speech-language pathology services. *American Journal of Speech-Language Pathology* 30, 5 (2021), 2143–2154.

[17] Peter Cantillon and Roger Jones. 1999. Does continuing medical education in general practice make a difference? *BMJ* 318, 7193 (1999), 1276–1279.

[18] Jennifer Cawthra, Nakia Grayson, Ronald Pulivarti, Bronwyn Hodges, Jason Kuruvilla, Kevin Littlefield, Julie Snyder, Sue Wang, Ryan Williams, Kangmin Zheng, et al. 2022. *Securing Telehealth Remote Patient Monitoring Ecosystem.* Technical Report NIST Special Publication 1800-30. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-30

[19] Jim Q Chen and Allen Benusa. 2017. HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management* 10, 2 (2017), 135–146.

[20] I Glenn Cohen and Michelle M Mello. 2018. HIPAA and protecting health information in the 21st century. *JAMA* 320, 3 (2018), 231–232.

[21] Cynthia L Corritore, Beverly Kracher, and Susan Wiedenbeck. 2003. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies* 58, 6 (2003), 737–758.

[22] Lynne Coventry, Dawn Branley-Bell, Elizabeth Sillence, Sabina Magalini, Pasquale Mari, Aimilia Magkanaraki, and Kalliopi Anastasopoulou. 2020. Cyberrisk in healthcare: Exploring facilitators and barriers to secure behaviour. In *International Conference on Human-Computer Interaction*. Springer, Copenhagen, Denmark, 105–122.

[23] Evan H Dart, Heather M Whipple, Jamie L Pasqua, and Christopher M Furlow. 2016. Legal, regulatory, and ethical issues in telehealth technology. In *Computer-Assisted and Web-Based Innovations in Psychology, Special Education, and Health*. Elsevier, 339–363.

[24] Sanchari Das, Kapil Madathil, Josiah Dykstra, Prashanth Rajivan, Shubha Setty, James T McElligott, Jiovanne Hughart, and Daniel Votipka. 2022. Privacy and Security of Telehealth Services. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 66. SAGE Publications Sage CA: Los Angeles, CA, Atlanta, GA, 1524–1528.

[25] Yibin Dong, Seong K Mun, and Yue Wang. 2023. A blockchain-enabled sharing platform for personal health records. *Heliyon* 9, 7 (2023).

[26] Ragan DuBose-Morris, Christina Coleman, Sonja I Ziniel, Dana A Schinasi, and S David McSwain. 2022. Telehealth utilization in response to the COVID-19 pandemic: current state of medical provider training. *Telemedicine and e-Health* 28, 8 (2022), 1178–1185.

[27] Josiah Dykstra, Rohan Mathur, and Alicia Spoor. 2020. Cybersecurity in medical private practice: Results of a survey in Audiology. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, Virtual Conference, 169–176.

[28] Tania Elliott, Ian Tong, Arwen Sheridan, and Beth A Lown. 2020. Beyond convenience: patients' perceptions of physician interactional skills and compassion via telemedicine. *Mayo Clinic Proceedings: Innovations, Quality & Outcomes* 4, 3 (2020), 305–314.

[29] Ana Ferreira, Ricardo Correia, David Chadwick, Henrique MD Santos, Rui Gomes, Diogo Reis, and Luis Antunes. 2013. Password sharing and how to reduce it. In *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications*. IGI Global, 22–42.

[30] Shira H Fischer, Kristin N Ray, Ateev Mehrotra, Erika Litvin Bloom, and Lori Uscher-Pines. 2020. Prevalence and characteristics of telehealth utilization in the United States. *JAMA Network Open* 3, 10 (2020), e2022302–e2022302.

[31] Crystal L Fleischhacker. 2020. Patient satisfaction with telehealth services compared to in-office visits: A systematic literature review. (2020).

[32] Shilpa N Gajarawala and Jessica N Pelkowski. 2021. Telehealth benefits and barriers. *The Journal for Nurse Practitioners* 17, 2 (2021), 218–221.

[33] Chad Gladden, Lucille Beck, and David Chandler. 2015. Tele-audiology: Expanding access to hearing care and enhancing patient connectivity. *Journal of the American Academy of Audiology* 26, 09 (2015), 792–799.

[34] Sharon G Goto. 1996. To trust or not to trust: Situational and dispositional determinants. *Social Behavior and Personality: an international journal* 24, 2 (1996), 119–131.

[35] Roman E Gusdorf, Kaustav P Shah, Austin J Triana, Allison B McCoy, Baldeep Pabla, Elizabeth Scoville, Robin Dalal, Dawn B Beaulieu, David A Schwartz, Sara N Horst, et al. 2023. A patient education intervention improved rates of successful video visits during rapid implementation of telehealth. *Journal of Telemedicine and Telecare* 29, 8 (2023), 607–612.

[36] Joseph L Hall and Deven McGraw. 2014. For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs* 33, 2 (2014), 216–221.

[37] Colton Hood. 2021. Telehealth cybersecurity. *A Practical Guide to Emergency Telehealth, Oxford University Press, New York, NY* (2021), 81–92.

[38] Shannon H Houser, Cathy A Flite, and Susan L Foster. 2023. Privacy and Security Risk Factors Related to Telehealth Services–A Systematic Review. *Perspectives in Health Information Management* 20, 1 (2023).

[39] Melanie W Hudson and Mark DeRuiter. 2023. *Professional issues in speech-language pathology and audiology*. Plural Publishing.

[40] Shelley D Hutchins. 2021. Build an Advocacy Win for More School Resources. *Leader Live* (2021).

[41] Asif Mohammed Islam and Daniel Lederman. 2020. Data Transparency and Long-Run Growth. (2020).

[42] Mohammad S Jalali and Jessica P Kaiser. 2018. Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of medical Internet research* 20, 5 (2018), e10059.

[43] Anna Marie Jilla, Michelle L Arnold, and Erin L Miller. 2021. US Policy considerations for telehealth provision in audiology. In *Seminars in Hearing*, Vol. 42. Thieme Medical Publishers, Inc., 165–174.

[44] Reema Karasneh, Abdel-Hameed Al-Mistarehi, Sayer Al-Azzam, Sawsan Abuhammad, Suhaib M Muflih, Sahar Hawamdeh, and Karem H Alzoubi. 2021. Physicians' knowledge, perceptions, and attitudes related to patient confidentiality and data sharing. *International Journal of General Medicine* 14 (2021), 721.

[45] Ismail Keshta and Ammar Odeh. 2021. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal* 22, 2 (2021), 177–183.

[46] Clemens Kruse, Joanna Fohn, Nakia Wilson, Evangelina Nunez Patlan, Stephanie Zipp, Michael Mileski, et al. 2020. Utilization barriers and medical outcomes commensurate with the use of telehealth among older adults: systematic review. *JMIR Medical Informatics* 8, 8 (2020), e20359.

[47] Bouchra Rekia Louassef and Noureddine Chikouche. 2021. Privacy preservation in healthcare systems. In *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*. IEEE, IEEE, El Oued, Algeria, 1–6.

[48] Edimara Luciano, M Adam Mahmood, and Parand Mansouri Rad. 2020. Telemedicine adoption issues in the United States and Brazil: Perception of healthcare professionals. *Health informatics journal* 26, 4 (2020), 2344–2361.

[49] Lumivero. 2023. https://lumivero.com/products/nvivo/

[50] Poornima Madhavan and Douglas A Wiegmann. 2007. Similarities and differences between human–human and human–automation trust: an integrative review. *Theoretical Issues in Ergonomics Science* 8, 4 (2007), 277–301.

[51] MAXQDA. 2023. https://www.maxqda.com/

[52] Mohammad Mehrtak, SeyedAhmad SeyedAlinaghi, Mehrzad MohsseniPour, Tayebeh Noori, Amirali Karimi, Ahmadreza Shamsabadi, Mohammad Heydari, Alireza Barzegary, Pegah Mirzapour, Mahdi Soleymanzadeh, et al. 2021. Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life* 14, 4 (2021), 448.

[53] Thomas Mildner, Gian-Luca Savino, Philip R Doyle, Benjamin R Cowan, and Rainer Malaka. 2023. About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI, Hamburg, Germany, 1–15.

[54] Lynette I Millett and Stephen H Holden. 2003. Authentication and its privacy effects. *IEEE Internet Computing* 7, 6 (2003), 54–58.

[55] Neville Moray and Toshiyuki Inagaki. 1999. Laboratory studies of trust between humans and machines in automated systems. *Transactions of the Institute of Measurement and Control* 21, 4-5 (1999), 203–211.

[56] Timothy Morey, Theodore Forbath, and Allison Schoop. 2015. Customer data: Designing for transparency and trust. *Harvard Business Review* 93, 5 (2015), 96–105.

[57] Khadijeh Moulaei, Abbas Sheikhtaheri, Farhad Fatehi, Mostafa Shanbehzadeh, and Kambiz Bahaadinbeigy. 2023. Patients' perspectives and preferences toward telemedicine versus in-person visits: a mixed-methods study on 1226 patients. *BMC Medical Informatics and Decision Making* 23, 1 (2023), 261.

[58] Bonnie M Muir and Neville Moray. 1996. Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics* 39, 3 (1996), 429–460.

[59] Adesola Christiana Odole, Khadijah Olatoun Afolabi, Boniface Ayanbekongshie Ushie, and Nse AyoOluwa Odunaiya. 2020. Views of physiotherapists from a low resource setting about physiotherapy at a distance: a qualitative study. *European Journal of Physiotherapy* 22, 1 (2020), 14–19.

[60] Academy of Doctors of Audiology. 2023. https://www.audiologist.org/

[61] U.S. Department of Health and Office for Civil Rights Human Services. 2023. Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance. https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2021.pdf

[62] Richard Pankomera and Darelle van Greunen. 2016. Privacy and security issues for a patient-centric approach in public healthcare in a resource constrained setting. In *2016 IST-Africa Week Conference*. IEEE, 1–10.

[63] Elizabeth D Peña and Rebecca Sutherland. 2022. Can you see my screen? Virtual assessment in speech and language. *Language, Speech, and Hearing Services in Schools* 53, 2 (2022), 329–334.

[64] Brian Pickering, Costas Boletsis, Ragnhild Halvorsrud, Stephen Phillips, and Mike Surridge. 2021. It's not my problem: how healthcare models relate to SME cybersecurity awareness. In *International Conference on Human-Computer Interaction*. Springer, 337–352.

[65] Marie C Pollio. 2004. The Inadequacy of HIPAA's Privacy Rule: The Plain Language Notice of Privacy Practices and Patient Understanding. *NYU Ann. Surv. Am. L.* 60 (2004), 579.

[66] Zachary S Predmore, Elizabeth Roth, Joshua Breslau, Shira H Fischer, and Lori Uscher-Pines. 2021. Assessment of patient preferences for telehealth in post–COVID-19 pandemic health care. *JAMA Network Open* 4, 12 (2021), e2136405–e2136405.

[67] Aryn Pyke, Ericka Rovira, Savannah Murray, Joseph Pritts, Charlotte L Carp, and Robert Thomson. 2021. Predicting individual differences to cyber attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 15, 4 (2021).

[68] Faiza Rafiq, Shafqat Hussain, and Qaisar Abbas. 2020. Analyzing students' attitude towards e-learning: A case study in higher education in Pakistan. *Pakistan Social Sciences Review* 4, 1 (2020), 367–380.

[69] Kalamullah Ramli and Hidayah. 2021. HIPAA-based Analysis on the Awareness Level of Medical Personnel in Indonesia to Secure Electronic Protected Health Information (ePHI). In *2021 IEEE International Conference on Health, Instrumentation & Measurement, and Natural Sciences (InHeNce)*. IEEE, 1–6.

[70] Fatemeh Rezaeibagha and Yi Mu. 2018. Practical and secure telemedicine systems for user mobility. *Journal of Biomedical Informatics* 78 (2018), 24–32.

[71] Andrejs Romanovs, Edgars Sultanovs, Egons Buss, Yuri Merkuryev, and Ginta Majore. 2021. Challenges and solutions for resilient telemedicine services. In *2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. IEEE, 1–7.

[72] John S Seberger and Sameer Patil. 2021. Us and them (and it): Social orientation, privacy concerns, and expected use of pandemic-tracking apps in the united states. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–19.

[73] Awanthika Senarath and Nalin Asanka Gamagedara Arachchilage. 2019. A data minimization model for embedding privacy into software systems. *Computers & Security* 87 (2019), 101605.

[74] Carmel Shachar, Jaclyn Engel, and Glyn Elwyn. 2020. Implications for telehealth in a postpandemic future: regulatory and privacy issues. *JAMA* 323, 23 (2020), 2375–2376.

[75] Lesley A Shawler, Joy C Clayborne, Brian Nasca, and Julia T O'Connor. 2021. An intensive telehealth assessment and treatment model for an adult with developmental disabilities. *Research in Developmental Disabilities* 111 (2021), 103876.

[76] Anthony C Smith, Emma Thomas, Centaine L Snoswell, Helen Haydon, Ateev Mehrotra, Jane Clemensen, and Liam J Caffery. 2020. Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19). *Journal of Telemedicine and Telecare* 26, 5 (2020), 309–313.

[77] Daniel J Solove. 2013. HIPAA mighty and flawed: regulation has wide-reaching impact on the healthcare industry. *Journal of AHIMA* 84, 4 (2013), 30–31.

[78] Timothy Stablein, Joseph Lorenzo Hall, Chauna Pervis, and Denise L Anthony. 2015. Negotiating stigma in health care: disclosure and the role of electronic health records. *Health Sociology Review* 24, 3 (2015), 227–241.

[79] Elizabeth Stobert, David Barrera, Valérie Homier, and Daniel Kollek. 2020. Understanding cybersecurity practices in emergency departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.

[80] Rebecca Sutherland, Antoinette Hodge, David Trembath, Suzi Drevensek, and Jacqueline Roberts. 2016. Overcoming barriers to using telehealth for standardized language assessments. *Perspectives of the ASHA Special Interest Groups* 1, 18 (2016), 41–50.

[81] Chris Taylor. 2005. The evolution of compliance. *Journal of Investment Compliance* 6, 4 (2005), 54–58.

[82] Faiza Tazi, Josiah Dykstra, Prashanth Rajivan, and Sanchari Das. 2022. Sok: Evaluating privacy and security vulnerabilities of patients' data in healthcare. In *International Workshop on Socio-Technical Aspects in Security*. Springer, 153–181.

[83] The Health Insurance Portability and Accountability Act of 1996 (HIPAA). 1996. 42 U.S.C. § 104-191.

[84] Chung-Hung Tsai. 2014. The adoption of a telehealth system: The integration of extended technology acceptance model and health belief model. *Journal of Medical Imaging and Health Informatics* 4, 3 (2014), 448–455.

[85] Juin-Ming Tsai, Min-Jhih Cheng, Her-Her Tsai, Shiu-Wan Hung, and Ya-Ling Chen. 2019. Acceptance and resistance of telehealth: The perspective of dual-factor concepts in technology adoption. *International Journal of Information Management* 49 (2019), 34–44.

[86] Reed V Tuckson, Margo Edmunds, and Michael L Hodgkins. 2017. Telehealth. *New England Journal of Medicine* 377, 16 (2017), 1585–1592.

[87] SACHIN Umrao, MANDEEP Kaur, and GOVIND KUMAR Gupta. 2012. Vulnerability assessment and penetration testing. *International Journal of Computer &*

Communication Technology 3, 6-8 (2012), 71–74.
[88] Martine Van Driel, John Vines, Belén Barros Pena, and Nelya Koteyko. 2023. Understanding Autistic Adults' Use of Social Media. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–23.
[89] Lex Van Velsen, Sabine Wildevuur, Ina Flierman, Boris Van Schooten, Monique Tabak, and Hermie Hermens. 2015. Trust in telemedicine portals for rehabilitation care: an exploratory focus group study with patients and healthcare professionals. *BMC Medical Informatics and Decision Making* 16, 1 (2015), 1–12.
[90] A Vithya Vijayalakshmi and L Arockiam. 2018. Hybrid security techniques to protect sensitive data in E-healthcare systems. (2018), 39–43.
[91] Elisabeth Vodicka, Roanne Mejilla, Suzanne G Leveille, James D Ralston, Jonathan D Darer, Tom Delbanco, Jan Walker, Joann G Elmore, et al. 2013. Online access to doctors' notes: patient concerns about privacy. *Journal of Medical Internet Research* 15, 9 (2013), e2670.
[92] C Jason Wang, Tiffany T Liu, Josip Car, and Barry Zuckerman. 2020. Design, adoption, implementation, scalability, and sustainability of telehealth programs. *Pediatric Clinics* 67, 4 (2020), 675–682.
[93] Ding Wang, Santosh D Kale, and Jacki O'Neill. 2020. Please call the specialism: Using WeChat to support patient care in China. (2020), 1–13.
[94] Sarah Warren. 2022. Insurance Payment Cuts Threaten Members' Jobs, Patients' Access to Care. *Leader Live* (2022).
[95] Valerie JM Watzlaf, Dilhari R Dealmeida, Leming Zhou, and Linda M Hartman. 2015. Protocol for a systematic review of telehealth privacy and security research to identify best practices. *International Journal of Telerehabilitation* 7, 2 (2015), 15.
[96] Valerie JM Watzlaf, Leming Zhou, Dilhari R DeAlmeida, and Linda M Hartman. 2017. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers. *International Journal of Telerehabilitation* 9, 2 (2017), 39.
[97] Wiktoria Wilkowska and Martina Ziefle. 2012. Privacy and data security in E-health: Requirements from the user's perspective. *Health informatics journal* 18, 3 (2012), 191–201.
[98] Jedrek Wosik, Marat Fudim, Blake Cameron, Ziad F Gellad, Alex Cho, Donna Phinney, Simon Curtis, Matthew Roman, Eric G Poon, Jeffrey Ferranti, et al. 2020. Telehealth transformation: COVID-19 and the rise of virtual care. *Journal of the American Medical Informatics Association* 27, 6 (2020), 957–962.
[99] Leming Zhou, Robert Thieret, Valerie Watzlaf, Dilhari DeAlmeida, and Bambang Parmanto. 2019. A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation. *International Journal of Telerehabilitation* 11, 1 (2019), 3.

A INTERVIEW QUESTIONS

The following is the interview script and the semi-structured interview questions asked to the participants:

Thank you for agreeing to participate in this study. We will be asking you some questions about telehealth services. We appreciate your time. We will record this conversation and please let us know if you have questions or concerns.

A.1 General Telehealth Context

- In the last year, estimate the percentage of your sessions that were done via telehealth and in-person.
- For what services do you offer telehealth?
- When did you first begin to offer telehealth? Please describe your experience in the decision and implementation of beginning to offer telehealth.
- What factors did you consider as you decided into choosing this technology(s)?
- Have you received any training regarding telehealth? If yes, who provided the training and what type of training have you received in this regard?
- What training, if any, have you received related to HIPAA security and privacy?
- In what ways, if any, does security and privacy of PHI factor into a telehealth appointment?

A.2 Telehealth Procedures & Execution

- What roles do various staff members play in a telehealth appointment?
- Do you have a specific room or location where you conduct telehealth appointments? If yes, describe the room/environment where you conduct telehealth.
- If no, where do you conduct telehealth appointments? What aspects or factors goes into to choose the location for the telehealth appointment.
- How much of it does it involve patient privacy? [Followup to the previous question]
- What technology(s) do you use during telehealth appointments?
- How reliable is the technology used during telehealth appointments?
- Describe the process involved with a telehealth appointment. Can you explain details regarding the login procedure for telehealth appointment connection.
- When you setup the appointment what information do you take from the patient and where do you save that information?
- Explain in detail how you use different features of the telehealth technology(s) during the appointment with the patient.
- Explain in detail how you maintain communication with the patient following an appointment?
- What kind of information do you exchange through these communication channels?
- For a hybrid structure, how do you navigate between the in-person and the virtual aspect of the telehealth?

A.3 Security & Privacy

- For what aspects of telehealth systems do you feel confident and secure? Do you have any privacy or security concerns about the telehealth services?
- What features would you like to see added to your telehealth systems? What concerns do you have regarding the telehealth services?
- What concerns have patients expressed to you about the telehealth systems?
- Anything else you would like to add.

A.4 Demographic Questions

- Gender
- Area of Medical Expertise
- Highest degree
- Years of Experience: Medical
- Years of Experience with Telehealth
- Current Role in Your Organization (e.g. clinician, owner, staff)
- Gross revenue of your practice in 2021 and 2022?
- Total number of full-time staff in the practice?
- How many patients are in your database?

B CODES

Table 2: A snapshot of the correlated open codes and themes generated for thematic analysis of the analyzed responses

Theme	Open Codes
Importance of telehealth	telehealth is needed, telehealth is better than patient abandonment, telehealth is better for some patients, telehealth is better for some services, telehealth in rural communities, prefer telehealth over in-person, patient choice telehealth or in-person, get caregiver to help with telehealth sessions, reasons for choosing telehealth: fulfilling a need, reasons for choosing telehealth: don't need to see patients in-person, reasons for choosing telehealth: patients' aggressiveness towards providers, reasons for choosing telehealth: prevent illness, reasons for choosing telehealth: providers personal safety, reasons for choosing telehealth: limiting the commute, reasons for choosing telehealth: cost savings, reasons for choosing telehealth: no distraction, reasons for choosing telehealth: necessity, reasons for choosing telehealth: efficient time management, reasons for choosing telehealth: convenience
Training	telehealth training, HIPAA training, educate/support patients
Limitations of telehealth	payment differences in telehealth, admin help, older adults prefer in-person, patient worries: effectiveness of telehealth, payment differences in telehealth, usability issues in telehealth, adapting in-person care to telehealth, change attitude of providers against telehealth, concerns about connectivity, difficulties of setting up telehealth, keeping attention of patients, lack of resources, patient worries: patient usability concerns, populations who had a hard time transferring to telehealth, provider concerns about telehealth, telehealth not suitable for all patients, telehealth on its own is difficult or impossible, time constraints to learn tech, vulnerable populations
HIPAA and Legal Implications	BAA, HIPAA compliance, eavesdropping in-person
Privacy and Security Considerations	as secure as in-person, data security on the internet, don't care if patient is not in private location, don't know how secure it is, don't trust anybody, don't trust tech provider, help from spouse, I do patient care not cybersecurity, I don't know whether it's two factor, I would think more about security if I were in a different field, importance of privacy, insecure behaviour, keep up with security news, No problem with tech, No/limited information taken during telehealth, Not familiar with all features of tech, Not important for patient to be in private area, Not important to be hacked, Not my area of expertise, Not saying patient names, nothing is 100% secure, past practices vs now, patient doesn't worry about telehealth, patient in private setting for telehealth, patient security behavior, patient worries/patient security concerns, patient worries/privacy, patient care more about health than privacy, positive security and privacy feeling, privacy and security assumptions, privacy and security conscious, private setting, provider security concerns, reasons behind choosing tech: security/privacy, security implemented, trust people making the decisions, there's only so much we can do about security, uncertainty about security, unconcerned about privacy and security, vetted by some department, we do the best we can to safeguard data privacy and security, We don't really talk about private information, worries about personal privacy, Zoom attacks stories