dHealth 2024
D. Hayn et al. (Eds.)

doi:10.3233/SHTI240013

Unpacking Sociotechnical Discourses on Telehealth Use and Data Protection: A Path Towards Digital Health Value Creation

Javad POOL[a,1], Farhad FATEHI[a], Salma SHARIFI[a], Morteza NAMVAR[a] and Saeed AKHLAGHPOUR[a]

[a] *The University of Queensland, Brisbane, Australia*

Abstract. Background: Telehealth uptake will remain sub-optimal without consumer trust. Safeguarding the security and privacy of health information plays an important role in building trust and acceptance of telehealth. Objectives: This study seeks to unpack the sociotechnical discourses on the use of telehealth with a focus on privacy and security in the context of United States health services. Methods: A search of the media outlets facilitated via the Factiva database was conducted. Using a qualitative method, thematic analysis was performed on the news texts to identify the key themes and provide contextual explanations. Results: The analysis led to the identification of three key themes: 'data protection practice', 'clinical resilience', and 'digital health business value' perspectives. These themes focus on various concepts of telehealth use including data privacy, security, public health emergency, compliance activities in the use of telehealth, meeting stakeholders' needs, reducing costs of service delivery, the potential of telehealth for informed action, and improving users' experience. Among these themes, 'data protection practice' was directly associated with privacy compliance and telehealth use. Other thematic discourses have provided an indirect reflection on the role of privacy compliance, with a greater emphasis placed on health service delivery and market dynamics rather than compliance in practice. Conclusion: Our study revealed the importance of the COVID-19 pandemic in telehealth use, highlighting the move towards 'good faith' and responsible use of telehealth.

Keywords. Telehealth, digital health, data protection, privacy, security

1. Introduction

Telehealth is considered a key solution for improving access to healthcare services in public health emergencies and beyond [1]. The COVID-19 pandemic has catalyzed the use of telehealth and the actualization of its benefits for informed health delivery in a time of crisis [2]. This pandemic crisis, however, presented unique challenges and tensions between public health interests and privacy protection against improper health data use. While telehealth applications have the potential to generate beneficial outcomes for public health, there is also the risk of their misuse in bad faith, leading to privacy violations. Ensuring telehealth data protection is challenging due to the escalating threat of cybercriminals exploiting vulnerabilities in health systems, aiming to gain

[1] Corresponding Author: Javad Pool, The University of Queensland, Brisbane, Australia, E-Mail: j.pool@uq.net.au

unauthorized access to valuable health data. These data protection concerns have adversely affected telehealth use among clinicians and patients. Furthermore, a survey on telehealth use found that health professionals frequently expressed concerns regarding privacy [3]. In achieving the goal of health service delivery and effective use of telehealth, compliance with health data protection laws and regulations is an essential requirement. This study places its emphasis on the US Health Insurance Portability and Accountability Act (HIPAA), serving as a prominent example of data protection regulations in the health services context. HIPAA and its privacy and security rules provide a rich context for our study of telehealth use. To contribute to telehealth literature, our paper takes a holistic and multidisciplinary approach by analyzing multiple aspects of telehealth use and data protection practices. This research also aims to inform public health policy debates and health informatics research, enabling a deeper understanding of the complexity and logic of telehealth data protection, responsible use, and HIPAA compliance.

2. Methods

This research applied an inductive qualitative methodology to offer insights into the regulatory landscape encompassing telehealth use. This particular methodology holds considerable prominence in the contexts of digital health, telehealth, and health services. We used the Factiva database to identify pertinent sociotechnical discourses on HIPAA and the use of telehealth. Factiva is a global news database with a broad collection of sources that reach across disciplines from business, health, communications, and technology to political science. The search was conducted between January 1990 and June 2023 , using search terms related to telehealth and HIPAA (see Appendix, Tabel A1 for search strategy). We identified 105 records by employing the search strategy. After removing duplicates (29 records) and excluding irrelevant news content (14 records) through screening and eligibility steps, 62 news articles were included for qualitative analysis.

The qualitative analysis was conducted employing an inductive approach for contextual investigation and conceptualization. The analysis was performed by the guidance offered by the "Gioia Methodology" for inductive research [4]. We followed the steps of this methodology for constructing a data structure that is composed of '*first-order concepts'*, '*second-order themes'*, and '*aggregate dimensions'*. First-order concepts emerge from the news text. To begin, the first author open-coded the news text to identify perspectives on the use of telehealth. We then categorized the emerging concepts into second-order themes and a theoretical dimension.

3. Results

The analysis led to the identification of three major discursive themes: data protection practice, clinical resilience, and digital health business value. These themes provide a holistic perspective on the use of telehealth as a digital health artifact. Figure 1, informed by data structure (see Appendix, Figure A1) and practice lens [5], illustrates a model of telehealth data protection as practice. The following subsections explain the three perspectives of data protection, clinical resilience, and digital health business value.

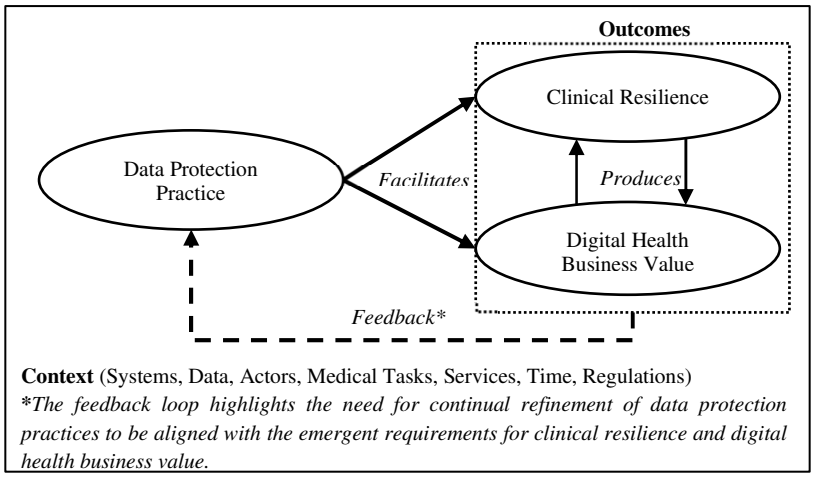

Figure 1. A model of Telehealth Data Protection as Practice (TDPP).

3.1. Data Protection Practice Perspective

The first sociotechnical theme that emerged from our analysis is *Data Protection Practice Perspective*. It consists of concepts around the protection of patient data privacy and security, and information assets. Practices related to the protection of patient data privacy and ensuring telehealth security are boldly represented in media discourses. This dominant concept reflects compliance with HIPAA rules in telehealth use, including video-based and audio-only modalities. Using telehealth technology with full HIPAA compliance in mind can help to achieve data protection [6]. For example, to avoid "bad faith" in telehealth provision and protect patient data, health professionals should not use public-facing video communication platforms, even in public health emergencies (e.g., Facebook Live) [7]. Bad faith in telehealth provision extends beyond malicious intent, covering acts like criminal behavior, privacy breaches, violations of licensing laws, and use of inappropriate communication platforms. Privacy practices such as gaining informed consent for use of telehealth are also important. Providers should inform health service customers that telehealth applications potentially introduce privacy breach risks. Beyond the informed consent, telehealth providers should enable security and privacy features of telehealth (e.g., encryption) when using third-party telehealth [8]. The success of telehealth use is associated with the security of patient data and digital assets. Data privacy and security concerns can lead to refusal of telehealth use by customers. As the number of telehealth users increases, telehealth providers must prioritize the management of emerging cyber risks associated with telehealth use [6]. They should consider effective cybersecurity practices during the high demand for telehealth. Extending encryption technology to mobile health, designing specific training programs for secure use of telehealth are examples of such cybersecurity and data protection practices [9].

3.2. Clinical Resilience Perspective

The second theme in the sociotechnical discourse on HIPAA is *Clinical Resilience Perspective*. It comprises three concepts: public health emergency as a trigger of

response and system use, providing healthcare service, and meeting stakeholders' needs. Clinical resilience perspective can be seen as beliefs and health practices that provides meaning and guides for telehealth actions in responding to public health crises. We found this salient theme on HIPAA and telehealth use are constructed during the COVID-19. While complying with HIPAA indicated in the background, our observation is that the perspective was explicit in the acknowledgment of the role of telehealth services for public health. For instance, the term "good faith" was introduced to the HIPAA discourse during COVID-19. In particular, the US Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) provided guidance on telehealth use that highlighted the good faith. Good faith implies that "*a covered entity or workforce member would exercise a degree of discretion appropriate for its role when deciding to use or disclose [Personal Health Information] PHI*" [10]. As a response to the crisis, this notification facilitated and expanded the use of telehealth platforms which were not considered fully HIPAA compliant before. During the COVID-19, OCR did not penalize service providers for using less secure telehealth platforms to provide timely and accessible care while maintaining good faith provision [8]. But to meet good faith in telehealth provision, providers were prohibited from improper data processing and misuse [11]. From a clinical resilience perspective, relaxing HIPAA restrictions derive additional benefits. This includes increased access to healthcare services via telehealth (especially for rural and underserved patients), reducing the risk of in-person visits for patients and clinicians, and helping to limit the virus spread [12].

3.3. Digital Health Business Value Perspective

The final theme that emerged from our analysis is *digital health business value*. In our contextualization, three concepts represent digital health business value: reducing costs of service delivery, the affordance of IT platform for informed action, and solution view on access to care and improving users' experience. The generalized assumption about IT business value is that digital health can be used in a way that enhances organizational relationships, service operations, efficiency, and coordination [13]. In our analysis, the digital health business value for telehealth emerges as a regulatory compliant tool. From this perspective, business value is generated through various means, including cost reduction, service delivery enhancement, improved telehealth experience, and informed medical actions. However, value creation from telehealth does not take place in isolation. It occurs from a synergistic combination of organizational context, practices, policies, and business processes [14]. This theme reports that telehealth businesses promote their platforms as "HIPAA compliant" to the market, indicating the value creation from data protection. Similarly, HIPAA compliant platforms, from a telehealth designer's perspective, are intended to help providers keep technology operations costs low and in turn, through cost savings generate value for the clients [15]. Digital health business value also can be generated from actualized potentials of HIPAA compliant telehealth for health professionals and end-users. Telehealth creates value by making appointments and diagnoses of patients easier and safer for healthcare professionals, especially during the pandemics and other crises [12, 16]. A high-quality telehealth platform generates value via reducing barriers to optimal care and enabling enhanced feedback. It ultimately improves users' telehealth experiences [17]. In support of our analysis, Table A2 (see Appendix) presents inductive concepts accompanied by illustrative quotes. Overall, our theoretical perspectives on telehealth data protection, which provide research avenues for future theory elaboration and theory testing, are summarized in Table 1.

Table 1. Theoretical overview of Telehealth Data Protection as Practice (TDPP).

Proposed theoretical overview	
We proposed a theoretical model of telehealth data protection (see Figure 1) and provided a sociotechnical perspective which made contribution to digital health data protection and digital health business value literature.	
Type of theoretical perspective	Contextual explanations on Telehealth Data Protection as Practice (TDPP)
Primary constructs	*Data Protection Practice*: actions to protect patient data privacy and security involve adhering to data protection regulations, gaining informed consent, and utilizing encryption and cybersecurity measures during telehealth interactions and use. Additionally, data protection practices encompass safeguarding against malicious attacks, including those orchestrated by hackers, by implementing robust cybersecurity and continuously monitoring for potential security breaches. *Clinical Resilience*: ability to adapt and respond effectively to shocks, and public health emergencies, such as the COVID-19 crisis, by employing telehealth services in compliance with data protection regulations and maintaining good faith provision. *Digital Health Business Value*: creating digital health benefit through use of safe and trustworthy telehealth platforms, offering health service cost reduction, improved service delivery, informed medical actions, and a better telehealth user experience.
Level	Telehealth data protection practice operates on multiple levels, encompassing individual and organizational levels. It extends beyond singular efforts to collective practices, acknowledging collaborative responsibility for safeguarding health data.
Context	The context of telehealth data protection encompasses various factors and actors influencing the facilitation or limitation of data protection. It involves telehealth systems, personal health data, actors (health professionals, managers, admins, IT department, patients, compliance enforcer and data protector (e.g. OCR, privacy officers), regulators, medical tasks (e.g. diagnoses, consultations), time (e.g. public health emergency), law and regulations (e.g. HIPAA)
Overarching proposition	The extent to which telehealth users effectively practice data protection can facilitate clinical resilience and generate digital health business value.
Theoretical advancements	Providing sociotechnical perspectives and contextual explanations which contribute the theories of data protection in digital health such as "Mobile Health Data Protection (MHDP)" [18] and "Context-Privacy Concerns-Practice-Outcomes (CPCPO)" in telehealth [19].

4. Conclusions

This study has unpacked sociotechnical discourses on telehealth use, data security, and privacy. Among the emerging themes, data protection practices were directly associated with HIPAA. Other concepts such as 'public health emergency', and 'reducing costs of service delivery' offered an indirect privacy perspective on the use of telehealth. In other words, HIPAA was used as background information in the discourse, but the emphasis was elsewhere such as introducing healthcare technologies. Our analyses also revealed that most of the texts on HIPAA and telehealth were produced during the COVID-19 pandemic, highlighting the impact and the momentum created by a public health emergency and the consequent move towards 'good faith' in using telehealth. As healthcare providers around the world are following the path towards the post-pandemic, compliance with data protection regulations is essential. Non-compliant behavior can adversely impact the effective use of telehealth systems for providing health services.

Also, security measures in telehealth can unintentionally deter engagement due to added complexity. This burden disproportionately affects those with low digital literacy. Stakeholders like healthcare providers and telehealth designers must prioritize user-friendly data protection solutions and offer training to alleviate this barrier. Nevertheless, this study has boundary conditions that can limit the generalizability of the findings. This research relied on the study of one major data privacy regulation in the context of the US health service. Future research can examine discourses on other regulations and privacy acts such as the EU's General Data Protection Regulation (GDPR).

Supplementary Material

Supplementary material (Appendix) is available at: https://tinyurl.com/nh9rnss7

References

[1] Hollander JE, Carr BG. Virtually perfect? Telemedicine for COVID-19. New England Journal of Medicine. 2020;382(18):1679-81.
[2] Gaitán JA, Ramírez-Correa PE. COVID-19 and telemedicine: A netnography approach. Technological Forecasting and Social Change. 2023;190:122420.
[3] Montoya MI, Kogan CS, Rebello TJ, Sadowska K, Garcia-Pacheco JA, Khoury B, et al. An international survey examining the impact of the COVID-19 pandemic on telehealth use among mental health professionals. Journal of Psychiatric Research. 2022;148:188-96.
[4] Gioia DA, Corley KG, Hamilton AL. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational research methods. 2013;16(1):15-31.
[5] Jarzabkowski P, Kaplan S, Seidl D, Whittington R. On the risk of studying practices in isolation: Linking what, who, and how in strategy research. Strategic Organization. 2016;14(3):248-59.
[6] Worth T. HIPAA Compliance: Prepare for the End of Pandemic Telehealth Waivers. Renal & Urology News. 2020.
[7] Castles C. COVID-19 Emergency Efforts: HHS To Allow Non- HIPAA Compliant Telehealth Remote Communications. Mondaq Business Briefing. 2020.
[8] Lacktman N. FAQs On Telemedicine And HIPAA During The Public Health Emergency. Mondaq Business Briefing. 2021.
[9] Hoar S. OCR Announces HIPAA Telehealth Security Waiver In Response To COVID-19 Pandemic. Mondaq Business Briefing. 2020.
[10] US Department of Health and Human Services. Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement 2021 [8.03.2022]. Available from: https://www.regulations.gov/document/HHS-OCR-2021-0006-0001.
[11] Feldman J. COVID-19: OCR HIPAA Enforcement Discretion For Telehealth Mondaq Business Briefing. 2020.
[12] Pfeffer H. HIPAA Restrictions Exist to Protect Patient Privacy. Can We Have Telehealth More Broadly and Still Comply? Risk & Insurance. 2021.
[13] Davidson E. Technology frames and framing: A socio-cognitive investigation of requirements determination. MIS Quarterly. 2002;24(6):329-58.
[14] Kohli R, Grover V. Business value of IT: An essay on expanding research directions to keep up with the times. Journal of the association for information systems. 2008;9(1):23-39.
[15] PR Newswire. DocVilla- HIPAA Compliant Telemedicine Platform to Connect Doctors and Patients through Smartphone. PR Newswire Association 2018.
[16] Nichols J. Revolve Robotics and swyMed Team to Deliver Secure, HIPAA-Compliant Robotic Telepresence for Telemedicine PRWeb. 2015.
[17] Dow Jones Institutional News. Medallia LivingLens Video Feedback Now HIPAA Compliant to Improve Telehealth Experience. 2021.
[18] Pool J, Akhlaghpour S, Fatehi F. Towards a contextual theory of Mobile Health Data Protection (MHDP): A realist perspective. International Journal of Medical Informatics. 2020;141:104229.
[19] Pool J, Akhlaghpour S, Fatehi F, Gray LC. Data privacy concerns and use of telehealth in the aged care context: an integrative review and research agenda. International Journal of Medical Informatics. 2022;160:104707.