Analyzing Various Security Threats to Healthcare Professionals

Jacylan Doering
Graduate Student, Master of Business Administration
Graduate Assistant, NCITE Center of Excellence

I. Project Description

1. Project Background

Technology has become a heavily used resource in healthcare. The Digital Health Market Size, Share, & Trends Report states, "The global digital health market size was estimated at USD 240.9 billion in 2023 and is projected to grow at a compound annual growth (CAGR) of 21.9% from 2024 to 2030" (2023, as cited in Kasoju et al., 2023). Technology can be used for advancing patient care, efficiency of health care practices, and expanding the potential of modern medicine (Harvard Medical School, 2023). Technology advances healthcare, however, increasing technology use increases security threats, therefore changing familiarity and ease for practicing healthcare professionals. Thus, the ceiling on technological evolution of healthcare is left to the healthcare professionals and their perspectives on implementing the internet of things into medicine (Jennett et al., 2003; Muigg et al., 2019; Pecina et al., 2012). The assimilation of technology in healthcare is ultimately a summation of the perspectives and intentions of healthcare professionals, highlighting the crucial role human factors play in the adoption of modern solutions.

Technology in healthcare provides endless resources to improve the methodology of caregiving. Three main ways technology is seen to be used are electronic health records (EHRs), telemedicine, and mobile health (mHealth) (Ahmad et al., 2022; Rampton, Böhmer, & Winkler 2022). Technology use is subjective to patients' circumstances and provider preference. The scholarly literature has stated providers are seen daily interacting with these technologies to record patient data in patient accessible medical records, provide virtual consultations and appointments, and utilize apps and wearable devices to monitor patient health and wellness (Heath & Porter, 2019; Zobair, Sanzogni, & Sandhu, 2020).

With providers' use of technology comes a wide span of security risks. Relying on EHRs, telemedicine, and mHealth practices expands security threats to cyberattacks, phishing, data breaches, and insider threats (Argaw et al., 2020). The patient's health, patient-to-provider trust, provider licensing, and institutional repercussions are affected depending on the severity level of the breach. For example, Richard Klein performed a study on patients' trust and acceptance of technology-based methods used by physicians to treat and communicate. Klein's study had results showing that trust in healthcare providers positively influenced patients' willingness to adapt to electronic health records and mobile health methods (Klein, 2006 as cited in Van Velsen, Flierman, & Tabak, 2021). When a patient's health and medical information is breached, trust is lost and negatively affects the patient-to-provider relationship, sometimes to the point of discontinued care. Knowledge on proper security protocol is not always proportional to the amount of technology use. Healthcare providers may heavily rely on technology in their caregiving, however, their efforts to minimize security risks often stem from their preexisting knowledge or training provided by the healthcare institution (Argaw et al., 2020).

This study will examine the perceptions of healthcare providers of the security risks they experience while providing care. Insight will be gathered on their training experiences related to security. To understand these perceptions, I will leverage insights from the theory of planned behavior (TPB), which proposes that individual decision-making is motivated by intent to engage in specific behavior

(Ajzen, 1985). The more intent an individual has towards executing certain behaviors, the more likely he or she is to complete that behavior, influenced by attitudes, subjective norms, and behavioral constraints (Alexandrou & Chen, 2019). Studying planned behavior is crucial because it gives healthcare professionals and institutions an understanding of motivations and intentions behind actions of their employed personnel. Policies are developed from insights gathered and then implemented as protocol for specific actions in the work environment to offer patients the highest quality care. By studying influences such as attitudes, subjective norms, and perceived behavioral constraints, institutions can be more successful in the implementation of technological innovations. These social components that formulate intent to act affect the individual's perspective. Perspective directly affects policy implementation and execution. For example, the perceived ease of use (PEU) of telehealth devices is the perspectives healthcare providers may hold toward the implementation and evolution of technology (Alexandrou & Chen, 2019).

By researching healthcare providers' perspectives, the study aims to bridge the gap between theoretical understanding and practical application in a healthcare environment. To better understand providers' perceptions of security risks and perceptions of the effectiveness of implemented training programs related to these risks, this study will conduct in-depth interviews with a diverse group of healthcare providers to gain insights on their experiences and perceptions of security protocols and education programs. New and experienced healthcare providers will be interviewed to maximize the application of gathered perspectives and experiences. In the end, the goal is to bring awareness to and pinpoint areas to improve the security measures within healthcare institutions, in turn offering a more secure physical and virtual environment for both the patients and their providers.

2. Methodology

For this research project, I completed CITI training and am working on an IRB application. This study examines the perceptions of healthcare providers of the security risks they experience while providing care. For this project, I will explore the research questions: 1) Healthcare providers' perceptions of security risks 2) Healthcare providers' perceptions of training programs to reduce these risks. Studying individual perceptions is essential for understanding and predicting an individual's behavior, as it provides insights on how they may interact with a system and its policies (Huang et al., 2011).

I will use a qualitative approach and rely on interviews to understand healthcare providers' perceptions of security issues in their work. I will focus on healthcare providers as subjects because it is the providers that implement and use the technology based on their familiarity and perception of ease of use. To identify participants, I will use my own personal network of healthcare professionals and continue my search utilizing the snowball sampling technique of asking those I interview for any additional healthcare personnel (Kirchherr & Charles, 2018). This type of sampling is the best approach because it allows me to collect data efficiently and reliably while staying within the research project's budget. For this study, I plan to interview a diverse set of healthcare providers: new and experienced nurses, med students and experienced doctors, and new and experienced nurse practitioners. A sample size of 10 would provide the minimum data needed to gather trends in perspectives. Additional interviews would allow me to compare trends seen in types of providers and trends in similar fields of care. I will use a semi-structured interview protocol (Magaldi & Berler, 2020) and conduct the interviews both in person and virtually. All interviews will be recorded and transcribed. The responses of the providers will constitute the data and enable conclusions to be drawn.

Once the data has been collected, I will use thematic analysis (Saunders et al., 2023) to identify two sets of themes. The first set will be related to healthcare providers' perceptions of security risks and the second set will be related to healthcare providers' perceptions of training programs to reduce these risks. These themes will serve as the basis for the results I will share at the Student Research and Creative Activity Fair.

3. Project Importance

The importance of this project is its contributions to maximizing the security of classified information for patients, providers, and healthcare institutions. This project's focus will bring awareness to the importance of security measures in place to combat security threats brought on by the addition of technology into healthcare. Such security threats include data breeches, cyberattacks, phishing, and HIPPA violations. *The Medical & Biological Engineering & Computing Journal* confirms the most common security breaches are found with the use of electronic health records, wireless infusion pumps, endoscopic cameras, and radiology equipment. Effects of the breach depend on the severity of information leaked; however, worst case scenario can result in direct attacks on life support equipment and implanted medical devices (Mejía-Granda et al., 2024). Analyzing professional perspectives of new and experienced providers and spreading awareness maximizes the quality and security of care available to patients. This project's efforts are result-oriented and focused on pinpointing areas lacking in existing security practices. Identifying points of vulnerability in security enables health care institutions to suggest improvements or implement needed security training, educational programs, and safety protocol. In addition to offering the highest quality of care, this is vital for establishing the patient-to-provider relationship by offering a sense of comfort and trust.

4. Project Timeline

Tentative Research Schedule	
Pre-Summer Activities	Obtain IRB approval.
May 2025	Selection of interviewees. Schedule interviews.
June 2025	Data collection. Begin analyzing data.
July 2025	Data collection continues. Data analysis.
August 2025	Complete data analysis. Begin creating poster.
September-December 2025	Review and edit poster. Prep for presentation and final submission.
Spring 2026/Post Summer Activities	Findings will be presented at the UNO Research and Creative Activity Fair.

5. Description of Roles

My faculty advisor is Dr. Erin Bass. I am currently a Graduate Assistant for the project she leads as the Project Investigator. I will be responsible for the project development, design, literature review, interview selection and conduction, interviewee data analyzation, interpreting and presenting results, and completion of the final product. Dr. Bass will offer her professional guidance as needed over the time of the research project. We will discuss the status of the project, and she will offer insight at scheduled meetings. Her professional guidance may extend to the analyzation of interviewee data, structure of the project report, and final review of the project and presentation prior to UNO Research and Creative Activity Fair.

6. Funding

I have not received previous funding through FUSE, GRACA, or UCRCA.

II. Budget

I am requesting a $5,000 stipend to support my graduate student research activities in the summer. The funds will cover necessary living expenses such as transportation, rent, groceries and expenses associated with the project. I intend to begin the project in May after the spring term's succession and complete most of it before the commencement of the fall semester in August. I envision the project will require 20-35 hours each week. The requested stipend would be divided over 14 weeks (about 3 months) and broken down to a pay rate of $12.50 per hour.

Budget Justification			
Budget Item	**Timeline**	**Objective**	**Justification and Amount**
Personal Salary	May 2025	Selection of healthcare providers as subjects. Research and analyze common security threats in healthcare.	- Partial stipend for living expenses - Work 20 hours per week at $12.50/hr. for 3 weeks - Stipend for Month: $750
	June 2025	Data collection process. Code interview information.	- Partial stipend for living expenses - Work 35 hours per week at $12.50/hr. for 4 weeks. - Stipend for Month: $1,750
	July 2025	Continue data collection Continue analyzing data and perceptions into trends.	- Partial stipend for living expenses - Work 35 hours per week at $12.50/hr. for 4 weeks. - Stipend for Month: $1,750
	August 2025	Complete data collection and analysis. Work on poster for presentation.	- Partial stipend for living expenses - Work 20 hours per week at $12.50/hr. for 3 weeks - Stipend for Month: $750
			Total Budget: $5,000

III. References

Ahmad, N., Atoum, I., Khan, J., Alqahhas, Y. (2022). ICT application and use in health sciences research at the global level: A scientometric study. *Healthcare*, 10, no. 9: 1701. https://doi.org/10.3390/healthcare10091701

Ajzen, I. (1985). From intention to actions: A theory of planned behavior. In *Action-control: From cognition to behavior*, ed. J. Kuhl and J. Beckman. New York: Springer.

Alexandrou, A., Chen, LC. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Secur J,* **32**, 410–434. https://doi.org/10.1057/s41284-019-00170-0

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D. *et al.* (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(146). https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7

Harvard Medical School. (2023). How digital technologies are changing health care. Retrieved from https://magazine.hms.harvard.edu/articles/how-digital-technologies-are-changing-health-care

Heath, C., & Porter, J. (2019). Digital transformation of healthcare sector: What is impeding adoption and continued usage of technology-driven innovations by end-users? *International Journal of Medical Informatics*. DOI: 10.1016/j.ijmedinf.2019.104025.

Huang, DL., Rau, P-LP., Salvendy, G., Gao, F., Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int J Hum Comput Stud*., 69(12):870–883.

Jennett, P., Yeo, M., Pauls, M., Graham, J. (2003). Organizational readiness for telemedicine: implications for success and failure. *J Telemed Telecare,* 9: S27–30. pmid:14728753

Kasoju, N., Remya, N.S., Sasi, R. *et al.* (2023). Digital health: trends, opportunities and challenges in medical devices, pharma and bio-technology. *CSIT,* **11**, 11–30. https://doi.org/10.1007/s40012-023-00380-3

Kirchherr, J., & Charles, K. (2018). Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia. *PloS one*, 13(8), e0201710. https://doi.org/10.1371/journal.pone.0201710

Magaldi, D., Berler, M. (2020). Semi-structured interviews. In: Zeigler-Hill, V., Shackelford, T.K. (eds) *Encyclopedia of Personality and Individual Differences*. Springer, Cham. https://doi.org/10.1007/978-3-319-24612-3_857

Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M. et al. (2024). Security vulnerabilities in healthcare: an analysis of medical devices and software. *Med Biol Eng Comput,* 62, 257–273. https://doi.org/10.1007/s11517-023-02912-0

Muigg, D., Kastner, P., Duftschmid, G., Modre-Osprian, R., Haluza, D. (2019). Readiness to use telemonitoring in diabetes care: a cross-sectional study among Austrian practitioners. *BMC Med Inform Decis Mak,* 19: 019–0746.

Pecina, J., Vickers, K., Finnie, D., Hathaway, J., Takahashi, P., Hanson, G. (2012). Health care providers' style may impact acceptance of telemonitoring. *Home Health Care Manag Pract*, 24: 276–282.

Rampton, V., Böhmer, M., & Winkler, A. (2022). Medical technologies past and present: How history helps to understand the digital era. *J Med Humanit*, **43**, 343–364. https://doi.org/10.1007/s10912-021-09699-x

Saunders, C. H., Sierpe, A., Von Plessen, C., Kennedy, A. M., Leviton, L. C., Bernstein, S. L. et al (2023). Practical thematic analysis: a guide for multidisciplinary health services research teams engaging in qualitative analysis *BMJ*, 381:e074256 doi:10.1136/bmj-2022-074256

Van Velsen, L., Flierman, I., & Tabak, M. (2021). The formation of patient trust and its transference to online health services: the case of a Dutch online patient portal for rehabilitation care. *BMC Med Inform Decis Mak*, **21**, 188. https://doi.org/10.1186/s12911-021-01552-4

Zobair, K. M., Sanzogni, L., & Sandhu, K. (2020). Health seekers’ acceptance and adoption determinants of telemedicine in emerging economies. *Journal of Telemedicine and Telecare. DOI*: 10.1177/1357633X20932456.

UNIVERSITY OF Nebraska Omaha

DEPARTMENT OF MANAGEMENT

GRACA Advisor Letter of Support for Jacylan Doering

September 13, 2024

To the GRACA Committee:

I am pleased to offer my support for Ms. Jacylan Doering's GRACA application. Ms. Doering is currently pursuing her MBA degree with a concentration in Healthcare Administration at the University of Nebraska Omaha (UNO). She also serves as a graduate assistant with the National Counterterrorism Innovation, Technology, and Education (NCITE) Center. Her role within NCITE, coupled with her academic work and prior professional experience, positions her uniquely to investigate critical issues at the intersection of technology, security, and healthcare.

Ms. Doering has been an exceptional student and graduate assistant in her short duration at UNO so far. She is highly conscientious and has demonstrated that she can complete tasks in a timely manner. She earned her undergraduate degree from the University of Nebraska Kearney where she was a student-athlete, and chose to pursue her MBA at UNO to further her education so that she can meet her professional goals. Ms. Doering has prior professional experience in healthcare, working with a cardiology clinic to maintain records and transition through a merger. Her interest in the health field paired with her MBA experience will position her well for an administrator position within a healthcare organization upon graduation in Spring 2026.

To this end, Ms. Doering is interested in advancing her knowledge of the intersection of technology, security, and healthcare in her GRACA project. Specifically, she aims to explore how healthcare providers view the security risks posed by the increasing use of technology in clinical and administrative settings. She plans to gather qualitative data through interviews with healthcare providers, analyzing their awareness of security vulnerabilities and their attitudes toward adopting new technologies. Her research will also assess how these perceptions influence decision-making processes related to technology adoption and compliance with security protocols. This study has significant implications for healthcare management, particularly in guiding strategies to improve security practices in a technology-driven environment. She will be able to use the information gleaned from her GRACA to not only inform knowledge in this field but to also put into practice the insights she gained when she eventually works as a healthcare administrator interfacing with healthcare providers.

As her advisor, I will work closely with Ms. Doering throughout the project, providing mentorship in research methodology, data collection, and analysis. She has demonstrated strong initiative and analytical skills, and I am confident in her ability to independently lead this project. With her diligent work ethic and passion for the subject matter, Ms. Doering is well-prepared to make a meaningful contribution to research in this field.

Sincerely,

Erin Bass, PhD
James R. Schumacher Chair of Ethics
Professor of Management
(402) 554-2547 | aebass@unomaha.edu