Physician Awareness of Cybersecurity risks and the Barriers to Implementation of Cybersecurity Measures in a Private Healthcare Setting

Njideka Nto
Mediclinic
Dubai, UAE
email: Njide@doctors.org

Ejike Nwokoro
HealthNet Homecare
Derbyshire, United Kingdom
email: Ejike.nwokoro@healthnethomecare.co.uk

***Abstract*— The healthcare industry has witnessed significant advancement in recent years, with technological innovations and the application of digital health solutions that broaden access, playing a key role. This has led to a dramatic rise in the volume of patient and healthcare data available within the healthcare ecosystem and, along with this, greater attention and concerns around data security and the need to prevent data breaches. Needless to say, proactive cybersecurity measures are essential to mitigate risks, ensure resilience, and uphold the highest standards of patient care and trust. However, despite the widely accepted notion that robust cybersecurity measures are essential to fortify the resilience of medical infrastructure and mitigate the risk of service interruptions, there remains sparse evidence as to the state of cybersecurity behavior of health care workers and medical private practices. In view of this, this study seeks to explore health professionals' attitudes to, and awareness of, cybersecurity considerations in a private healthcare setting, with a view to clarifying implementation barriers for routine cybersecurity measures. This survey-based cross-sectional study will adopt a thematic analysis approach that is aimed at identifying any patterns in clinicians' perception/awareness of the threat to cybersecurity with respect to medical records and patient data, as well as bottlenecks that prevent the implementation of cybersecurity measures in practice. This study, which will commence in Q2 2024 within a large ambulatory care center, will add to the body of knowledge that will support the removal of barriers to the practical implementation of routine cybersecurity practices, particularly in a private healthcare setting.**

Keywords- cybersecurity; physician awareness; healthcare; personal health information; health data breach.

I. INTRODUCTION

The positive impact of technological advancements in healthcare is evident as it has played a crucial role in improvements in the efficiency of patient care, as well as in medical research. Furthermore, there has been an escalation in digital health solutions, interconnected medical devices and telehealth provisions, all of which are designed to reduce fragmentation in patient care, whilst supporting positive patient experiences and better clinical outcomes.

The resulting exponential growth of healthcare data, from all the advancements, presents both opportunities and threats. On the one hand, big data analytics hold immense potential for accelerating medical research, improving patient care, and generating value for healthcare organizations [1]. However, on the other hand, such data-driven evolution in healthcare requires a high-level assurance of data integrity and confidentiality. The proliferation of health data and the increasing interconnectedness of health systems, as well as their integration into networked environments renders them vulnerable to hacking and exploitation. It will come as no surprise therefore, that healthcare systems face various risks, including data breaches, theft, and damage.

The relevance of such risks cannot be overstated as patient confidentiality stands as a cornerstone of ethical medical practice. Electronic Health Records (EHRs) store a wealth of sensitive information, including medical history, diagnoses, treatments, and personal identifiers.

The structure of this paper is as follows: Section II describes the significant role of cybersecurity in healthcare, whilst Section III outlines the part that human error plays in cybersecurity breaches within healthcare and thus providing a rationale for the stated objectives of this study. Section IV details the objectives of this study, and Section V describes the proposed methodology through which the study objectives will be achieved. In Section VI, there is a detailed description of the data source for this study, as well as the steps that will be taken to ensure that quality is maintained throughout the data collection process. Finally, Section VII concludes with an explanation of the added value that findings of this study intend to bring to the field of cybersecurity in healthcare, as well as highlighting any potential limitations of the study or areas of future research.

II. CYBERSECURITY AND HEALTHCARE

The imperative to protect patient privacy, safeguard medical infrastructure, secure connected devices, and preserve data integrity underscores the critical role of cybersecurity in healthcare delivery. A breach in cybersecurity not only compromises patient privacy, but also exposes individuals to identity theft, financial fraud, and reputational damage.

Experts in the field of internet security have argued that Personal Health Information (PHI) is often considered more valuable on the illegal market than credit card credentials or regular Personally Identifiable Information (PII), hence the higher incentive for cyber criminals to target medical databases [2].

As technology continues to evolve, and healthcare systems become increasingly interconnected, proactive cybersecurity measures are essential to mitigate risks, ensure

resilience, and uphold the highest standards of patient care and trust.

III. ROLE OF HUMAN FACTOR IN CYBERSECURITY BREACHES

Factors that lead to breaches in the healthcare sector can take different forms, including, but not limited to, hacking, purposeful or accidental disclosure of data, system failures and lost equipment. According to the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware [3]. Interestingly, other authors have argued that most breaches in cybersecurity have been attributed to human error [4]. Similarly, according to another data security survey, human error was the most common cause of data breaches, ahead of other factors like theft, malware, hacking and misuse of data [5].

IV. PROPOSED STUDY OBJECTIVES

Notably, research elsewhere has shown that despite the well-documented cyber threats to patients' PHI, sparse evidence exists about the state of cybersecurity behavior of health care workers and medical private practices [6]. In view of this, this study seeks to explore health professionals' attitudes to, and awareness of, cybersecurity considerations in a private healthcare setting.

Subject to obtaining the relevant Institutional Review Board (IRB) approvals, the objective of this study, which will commence in Q2 2024, is to:

- Assess medical professionals' perception of the threat to cybersecurity with respect to medical records and patient data
- Assess medical professionals' perspectives of the common cybersecurity practices
- Assess medical professionals' experience of challenges/barriers in implementing cybersecurity measures
- Assess the awareness of medical professionals, in a large private hospital, of cybersecurity measures and applicable regulations

V. PROPOSED METHODOLOGY AND ANALYTICAL PROTOCOL

To fulfil the stated objectives, a survey-based cross-sectional study will be implemented to assess medical professionals' perception/awareness of the threat to cybersecurity with respect to medical records and patient data.

This study will adopt a thematic analysis approach with a view to identifying any patterns in participants' responses. This approach will entail a review of the frequency of response types under each survey category. A thematic analysis approach has been chosen for this study because it has been recognized as a credible research method for identifying, analyzing, organizing, describing, and reporting themes found within a data set [7]. In terms of choice of thematic analysis protocol, this study will adopt Braun & Clarke's six-phase framework for doing a thematic analysis [8] comprising: step 1- becoming familiar with the data; step 2- generating initial codes; step 3- searching for themes; step 4- reviewing the identified themes; step 5- defining the themes; step 6- write up of the interpretation. This framework is recognized as one of the most delineated methods of conducting a thematic analysis [9].

The results will categorize the respondents using demographic and screener questions, including clinical specialty, years of experience, as well as experience with EHRs, or with health technology in general.

Subsequently, the participants' anonymized responses with respect to the level of cybersecurity awareness, implementation of cybersecurity measures and experience of practical challenges with real world implementation of cybersecurity practices will be measured and reported.

No identifiable patient information will be collected as part of this study and there will be no direct patient contact or implementation of any clinical intervention as part of this study. Furthermore, responses by study participants will be anonymized and identities of study participants would not be revealed.

VI. DATA SOURCE AND QUALITY ASSURANCE

All licensed physicians contracted to large ambulatory care center in the United Arab Emirates will be invited to participate in the survey. Participation will be completely voluntary; no compensation will be offered to participants and complete anonymity of responses and participants will be maintained.

The survey questionnaire will be developed on Microsoft Forms and sent by email to all participants. The questionnaire would describe the background and rationale for the study, with participants given the opportunity to consent.

The survey themes and questionnaire contents will be supplemented and informed by relevant published literature search (including of published cybersecurity guidelines and regulations), as well as with qualitative discussions at Senior Leadership (SLT) and departmental meetings. This is with a view to validating understanding, applicable assumptions and to confirm the chosen themes and response categorizations for the study.

To assure good data quality during the data collection process, the study will:

- Implement a pretesting of the survey questionnaire and the channel of data collection (Microsoft Forms) before administering them. This is to ensure the tools are working as expected and that they adequately cover the research objectives
- Ensure that the survey duration does not exceed 10 minutes to avoid respondent fatigue
- Implement routine data collection checks to ensure that the data being collected is of the intended quality
- Ensure secured storage of the study data in encrypted and password-protected files

- Ensure that anonymity of responses and study participants is fully maintained and protected

VII. CONCLUSION

In an era where technological advancements have revolutionized healthcare delivery, cybersecurity is an indispensable safeguard for the sanctity of patient data and the integrity of medical systems. We believe that the insight that will be generated in this study will add to the body of knowledge that will support the removal of barriers to the practical implementation of cybersecurity practices and measures, particularly in a private healthcare setting. As the primary target audience for the study are clinicians working in a private healthcare setting, we recognize that an area of further research could include other stakeholders, e.g., Information Technology (IT) professionals within healthcare, who also play a critical role in healthcare cybersecurity.

REFERENCES

[1] R. Pastorino et al., "Benefits and challenges of Big Data in healthcare: an overview of the European initiatives," Eur J Public Health, Oct 2019, vol. 29 (Supplement_3), pp. 23-27, doi: 10.1093/eurpub/ckz168.

[2] MS-ISAC, "Data Breaches: In the Healthcare Sector," Center for Internet Security, New York: Insights and Blogs, 2016, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector.

[3] HHS, "Cyberattack on Change Healthcare," US Department of Health and Human Services, Washington: Press Release, 2024.

[4] K. Hore et al., "Cybersecurity and critical care staff: A mixed methods study," Int J Med Inform, 2024 May, vol. 185, p. 105412, doi: 10.1016/j.ijmedinf.2024.105412.

[5] A. Seh et al., "Healthcare data breaches: Insights and implications in Healthcare," Multidisciplinary Digital Publishing Institute, 2020, vol. 8, p. 133.

[6] J. Dykstra, R. Mathur, and A. Spoor, "Cybersecurity in Medical Private Practice: Results of a Survey in Audiology," IEEE 6th International Conference on Collaboration and Internet Computing (CIC), 2020, pp. 153–181, doi: 10.1109/CIC50333.2020.00029.

[7] L. Nowell, J. Norris, D. White, and N. Moules, "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," International Journal of Qualitative Methods, 2017 Oct, vol 16, p. 1, doi:10.1177/1609406917733847.

[8] M. Maguire, and B. Delahunt, "Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars," All Ireland Journal of Higher Education, 2017 Oct, vol 9, p. 3.

[9] D. Byrne, "A worked example of Braun and Clarke's approach to reflexive thematic analysis," Qual Quant, 2021 June, vol 56, pp. 1391–1412, doi: 10.1007/s11135-021-01182-y.