EasyChair Preprint

№ 15593

End-User Privacy, Security, and Data Ownership Concerns on the Helsenorge Platform: a Mixed-Methods Study

Abha Pokharel, Surya Kathayat and Casandra Grundstrom

December 18, 2024

End-users' Privacy, Security, and Data Ownership Concerns on the Helsenorge Platform: A Mixed-Methods Study

Abha Pokharel[1][0009−0005−4841−0011], Surya Kathayat[2][0009−0001−2615−1283], and Casandra Grundstrom[3][0000−0001−6410−144X]

[1,2,3] Norwegian University of Science and Technology, Trondheim, Norway
{[1]abha.pokharel,[2]surya.b.kathyat,[3]casandra.a.grundstrom}@ntnu.no

Abstract. This work-in-progress (WIP) study explored end-users perceptions of privacy, security, and data ownership (PSDO) of Helsenorge, a leading e-health platform in Norway. By surveying over 100 users from diverse demographics, this study evaluates their understanding of the PSDO landscape, sentiments, and expectations for future improvements. These early findings suggest that most users know the importance of PSDO features but are unaware of them, highlighting the gap between the significance of these features and user awareness. In addition, it suggests that privacy can be improved through selective data sharing, configurable consent, and granular access control. Simultaneously, security can be enhanced by increasing transparent data access, accountability, multi-factor authentication (MFA), transparent audit trails, and robust encryption. Moreover, improving data ownership might give users greater control and ownership over their health records, fostering trust in the platform and educating them on the related challenges and risks. The paper concludes by discussing the potential adoption of self-sovereign identity (SSI) and Web 3.0 technologies to address these challenges.

Keywords: Helsenorge · Privacy · Security · Data ownership

1 Introduction

The digitalization of healthcare has improved efficiency and patient empowerment; however, it has also introduced new security risks. Complex eHealth platforms can lead to breaches and excessive permissions. Social engineering attacks exploit human vulnerabilities, causing the unintentional disclosure of sensitive information or unauthorized access [1]. This highlights the need for robust cybersecurity measures for healthcare. In Norway, the Helsenorge eHealth platform has evolved into a comprehensive system offering healthcare services for both patients and providers [2]. Achieving the goal of becoming a national hub for patient-focused electronic health services requires addressing the socio-technical complexities of the current system, which demands significant economic effort [2]. One way to understand socio-technical complexities is to examine the platform from the end-user perspective, including patients, healthcare providers, and

other stakeholders. Experts have emphasized that end-user awareness and behavior play a critical role in maintaining the security of eHealth platforms [3]. Despite several studies on privacy and security [4][5][6], there is a notable gap in empirical research on end-user security awareness and behaviors related to eHealth platforms. *This work-in-progress (WIP) study aimed to provide valuable insights for developers by identifying end-user concerns about privacy, security, and data ownership (PSDO) towards the Helsenorge eHealth platform in Norway.* By addressing these concerns early in the digital transformation process, developers can create systems that meet privacy and security expectations, foster trust and encourage users to share their personal information. The rest of this paper is organized as follows: Section 2 describes the methods of our study, Section 3 presents the results, and Section 4 describes the discussion, and Section 5 presents the conclusion.

2 Methods

A mixed-method approach was employed for the problem identification phase of broader Design Science Research [7], gathering requirements from 103 end-users over two months via Nettskjema, an anonymous online survey. The end-users involved in this research included professionals from diverse backgrounds, ranging from general users to patients and medical professionals. The survey included 24 questions categorized into demographics, PSDO (Privacy, Security, Data Ownership) awareness, importance, sentiments and futuristic desires. PSDO awareness was measured using Yes, No, and Not Sure questions, while importance was scaled from 1 (very important) to 5 (not important). Open-ended questions assessed sentiments and futuristic desires. The analysis involved SPSS24, Cronbach's alpha for reliability, descriptive statistics, Shapiro-Wilk test for normality, and Kruskal-Wallis H-test ($P < 0.05$). Thematic analysis was used for open-ended questions facilitated by NVivo14 [8].

3 Preliminary Results

For the **closed-ended questionnaire**, PSDO awareness was low with a mean of 2.21 (SD 0.73) and a Cronbach's alpha of 0.31, while PSDO importance was high with a mean of 1.47 (SD 0.50) and a Cronbach's alpha of 0.75. For PSDO awareness, a mean score of two was considered negative. For PSDO, an importance mean of 3 and above was considered negative. The Kruskal Wallis test showed that most demographics were not statistically significant for PSDO awareness and importance, except for data portability among age groups ($P = 0.042$) and informed consent among occupationa groups ($P = 0.021$).
The **open-ended questionnaires** revealed several themes;
End-users' were concerned about **data transparency and user empowerment**, with 50% lacking the control over consent and desiring clearer language with a common sentiment and desire: *"I am worried how my data is used, I want clear, simple language and easy options to manage and withdraw my consent."*

Endusers wanted **data sharing and user empowerment** with 81% desired selective data sharing and granular access control as current options were insufficient. One participant noted- "*If I visit a dentist, I don't want my dentist to see my entire medical history, just what's relevant for my checkup. This way, my privacy is better protected [...].*"
Data transparency and accountability 57% of end-users wanted detailed access logs for who and when their data were accessed and 34% desire real-time alerts whenever their data were accessed. One participant stated- *"I'd like to track who accesses my information and its purpose and monitor how healthcare providers handle my records."*
Data security and user trust were another major concern with 62% emphasizing the need for strong encryption and 38% advocating for enhanced security standards, such as Multi-Factor Authentication (MFA). One participant elaborated- *"I don't want any third party seeing my sensitive health data. I want strong security to approve or deny access, and security like MFA could probably add security further."*
User empowerment and ethical data managementwere also highlighted with 72% of the users frustrated by a lack of control over data. 27% of the users expressed uncertainty about ethically protecting it. One participant expressed- *"I believe that, as the owner of my health record, I would be more motivated to protect and use my health records ethically, given my investment in maintaining my privacy and well-being."*

4 Discussion

These preliminary results revealed differences in end-users PSDO awareness and perceived importance, indicating a lack of knowledge and training. These differences pinpointed the areas that required the highest level of attention. This research builds on previous studies [3][6], highlighting the importance of addressing the awareness gap in PSDO features to ensure users can fully protect their data. Further analysis showed that PSDO awareness and importance did not vary significantly with demographic characteristics except for data portability and informed consent. As these data didn't allow deeper analysis, further research is needed to explore additional predictors such as Helsenorge usage duration, gender and IT knowledge. Moreover, an open-ended questionnaire identified end-users sentiments and desires, highlighting areas that need to be enhanced. The current study expands on previous research [4][5][6] by offering a more comprehensive, user-centric approach to PSDO features in eHealth solutions. Unlike previous studies that focused on general security recommendations, this research provides a detailed examination of data ownership, privacy and security using open-ended questionnaires to capture user specific sentiments. Moreover, this investigation goes beyond merely identifying end-user concerns. It will delve into the potential of emerging technologies such as Web 3.0 and self-sovereign identities (SSI) could be leveraged to enhance data security, privacy, and user control in eHealth contexts.

5 Conclusion

This preliminary study used a mixed-method approach to understand the PSDO concerns of 103 end-users on the Helsenorge platform through a questionnaire. The findings highlighted low PSDO awareness but perceived high importance, along with desirable features such as selective data sharing, configurable consent, granular access control, transparent data access, accountability, MFA, transparent audit trails, robust encryption and control. However the study had limitations, including small sample size, reliance only on the end-user perspective and potential bias from open-ended questions. To address these concerns our future research will aim to balance end-user perspectives with expert knowledge through semi-structured interviews, particularly focusing on Web 3.0 and Self-sovereign Identity (SSI), to better understand and address end-user concerns.

References

1. Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 12, 6042. https://doi.org/10.3390/app12126042
2. Aanestad, M., Grisot, M., Hanseth, O., & Vassilakopoulou, P. (2017). Information infrastructures and the challenge of the installed base. In M. Aanestad, M. Grisot, O. Hanseth, & P. Vassilakopoulou (Eds.), *Information infrastructures within European health care: Working with the installed base* (pp. 25-33). https://doi.org/10.1007/978-3-319-51020-0_3
3. Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., & Seeam, A. (2016). Pervasive eHealth services a security and privacy risk awareness survey. In 2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA) (pp. 1-4). IEEE. https://doi.org/10.1109/CyberSA.2016.7503293
4. Zhou, L., Bao, J., Watzlaf, V., & Parmanto, B. (2019). Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR mHealth and uHealth, 7(4), e11223. https://doi.org/10.2196/11223
5. Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. Health informatics journal, 18(3), 191-201. https://doi.org/10.1007/978-3-319-20376-8_53
6. Denkovski, V., Stojmenovska, I., Gavrilov, G., Radevski, V., & Trajkovik, V. (2023). Investigating Privacy and Security Concerns in a Running eHealth Information System. In 2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (pp. 39-44). IEEE. https://doi.org/10.1109/MeditCom58224.2023.10266398
7. Vom Brocke, J., Hevner, A., & Maedche, A . Introduction to design science research. Design science research.(2020) Cases, 1-13.
8. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77–101. https://doi.org/10.1191/1478088706qp063oa