A Case Study of Privacy Protection Challenges and Risks in AI-Enabled Healthcare App

Ping Wang
Department of Computer Information Systems
Robert Morris University
Pittsburgh, USA
wangp@rmu.edu

Hossein Zare
Bloomberg School of Public Health
Johns Hopkins University
Baltimore, USA
hzare1@jhu.edu

***Abstract* — Artificial intelligence (AI) is increasingly used in healthcare systems and applications (apps) with questions and debates on ethical issues and privacy risks. This research study explores and discusses the ethical challenges, privacy risks, and possible solutions related to protecting user data privacy in AI-enabled healthcare apps. The study is based on the healthcare app named Charlie in one of the fictional case studies designed by Princeton University to elucidate critical thinking and discussions on emerging ethical issues embracing AI.**

Keywords — AI, healthcare, ethics, privacy, security, risks

I. INTRODUCTION

Artificial intelligence (AI) is a technology supported by inter-disciplinary fields such as computer science, machine learning, knowledge representation, and optimization. The applications of AI are increasingly finding their ways into modern life and industries including healthcare services. In spite of the technical capabilities and benefits of AI solutions, there have been increasing questions, challenges, and debates on the ethical issues and privacy risks associated with AI applications and AI-enabled devices in healthcare services. The issues and challenges regarding ethics and privacy protection identified in research so far include lack of accuracy of data, lack of privacy, lack of security, lack of transparency, and lack of informed consent for user data collection and sharing [1, 2, 3, 4].

Privacy protection is a significant issue for research in the technologically advanced age of AI. In the U.S., the individually identifiable health information is currently limited to the definition and protection under the Privacy Rule issued by the federal Health and Human Services as implementation of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [5]. The goal of this research is to analyze the ethical issues and data security challenges that contribute to the user data privacy risks in AI-enabled healthcare apps. The analysis and discussions of the privacy risks and challenges are illustrated in the case study of the Charlie healthcare app from the Princeton Dialogs on AI and Ethics series.

II. BACKGROUND

The lack of privacy protection has been a primary and frequently cited ethical issue for AI applications, which are vulnerable to security breaches such as the Mumbai lab hack and leak in 2016 and the ability of the machine learning technology of AI to detect patterns and pose privacy risks even without direct access to personal data [1, 2]. While AI applications in healthcare enable computational systems to learn from data and improve their performance, data privacy and privacy protection has been a primary ethical and legal challenge in the U.S. as the limited HIPAA protection does not apply to data triangulation (or re-identified data) and health information inferred from non-health purchase data collected by tech giants in the age of big data [6]. In terms of technology infrastructure for AI-enabled applications, organizations continue to experience growing security problems and threats [7]. Concerns for privacy risks not only apply to the access, use, and control of patient data in private hands but also arise from external privacy data breaches through AI-driven methods and algorithms to compromise the ability to de-identify or anonymize patient health data [8].

Informed consent for patients' self-determination is essential to privacy protection in healthcare. Growing challenges to the informed consent rules and de-identification of personal information with AI technology lead to increasing privacy risks in health data collection, use, and algorithmic prediction stages in AI-enabled healthcare environment [9]. Significant concerns occur when the collection and use of patient data may be done in ways unknown to and with no consent from the individual whose data was collected and used by AI systems [2]. Informed consent is thus necessary to maintain respect for patient privacy especially in cases of using health data generated or re-identified by AI technology beyond the knowledge of patients [8]. Informed consent may also be ethically necessary for the patient to determine if or not to use the AI solution for healthcare in the first place [3, 10].

The lack of transparency in AI-enabled healthcare further exacerbates privacy risks and user trust in AI solutions. Patients in the U.S. are expected to receive understandable disclosures and transparency about AI-enabled applications including their security and privacy vulnerabilities, risks, and protection policies [6, 10]. However, AI-enabled healthcare solutions are often "black boxes" with proprietary AI algorithms from developers, which make it difficult for health providers to explain the effectiveness, security, and privacy of the AI solutions [3]. Such "black boxes" contribute to more uncertainty and less trust and confidence from patients in the privacy protection in AI systems. In addition, transparency of the algorithms, data protection technology and governance, and sustainability of technical robustness in the technology of AI solutions is important for developing and maintaining patients' trust and confidence in the AI applications [11].

This research is supported by a grant from the U.S. National Science Foundation (NSF) – NSF Grant ID 2234554.

III. METHODOLOGY

The case study for this research is based on the Automated Healthcare App case from the Princeton Dialogs on AI and Ethics series [12]. The healthcare app in this case study is named Charlie, a multi-platform AI-enabled application developed by a university hospital medical research staff and computer scientists to make insulin administration process more efficient and effective for patients with type 2 diabetes and complications which have high rates of occurrence among certain socio-economic and racial groups. Charlie has unique features of using biosensors for blood testing and data collection for insulin dosage recommendation and health reminders as well as a forum for information sharing and social networking. Charlie has received IRB approval and mixed results from clinical trials.

The fictionalized case studies in this series are designed for educational dialogs guided by the principles of empirical foundations of existing AI technologies, multi-disciplinary backgrounds for broad accessibility and diverse perspectives, and complex and interactive ethical questions and dilemmas for in-depth critical thinking [12]. The fictional nature of the case studies also has the advantage of being shielded from emotional sentiments and legal ramifications of real cases to encourage honest and in-depth discussions and reflections.

IV. DISCUSSION

The Charlie AI-enabled healthcare app case study has generated a number of ethical issues and questions for discussion. This research will focus on those related to privacy risks and protection. Charlie collects patients' medical data fed into and used by its AI algorithms to calculate and provide individualized medical recommendations. Charlie also has a social networking platform for information sharing and community support, along with a bonus capability of using natural language processing technology to analyze discourse for additional individual profile data to improve customized treatments. However, there is no information on the privacy risks and policies and technical controls to protect user privacy in the process of large amount of collection, processing, and sharing of sensitive information on the AI platform. The privacy protection component is missing from the informed consent for using the app.

The case study shows that medical treatments with the AI app had occurred without explicit consent of Charlie's users, which exposes a serious ethical issue of lack of transparency that contributes to further uncertainty and lack of trust about user privacy protection. Users of Charlie demand transparency on the AI algorithms of the app to understand how Charlie's algorithms worked in building individual profiles, in determining advice to present, and in deciding the offers of sub-optimal medical solutions to individuals [12]. Users of the app also deserve to be informed of all possible data privacy and security risks of the AI algorithms and necessary controls, policies and procedures for privacy and security incident handling and risk management. The case study confirms that there is no documentation of the AI algorithms in the research methodology even though the algorithms are a key component of the AI-enabled app [12].

V. CONCLUSION

The Charlie case study demonstrates the need for transparency of privacy risks and policies and usable privacy choice and consent mechanisms on AI-enabled healthcare devices. In addition to appropriate technical safeguards against privacy risks, the following proposed guidelines may help to provide practical privacy protection in AI implementations: 1) Address user needs, including need for transparency; 2) require minimal user effort; 3) Make users aware of privacy options; 4) Make privacy options and implications easily understandable to users; 5) Satisfy users to build trust; 6) Allow users to change their decisions on privacy options; and 7) Avoid pushing users to accept options with less privacy protection [13].

Programmers and developers play a key role in designing and implementing algorithms of AI technology. As a long-term and sustainable solution to privacy protection in technology, education of youths and future generations should emphasize ethical use of technology [14].

REFERENCES

[1] B. C. Stahl, "Ethical issues of AI," in Artificial Intelligence for a Better Future. Springer Briefs in Research and Innovation Governance. Springer, Cham, 2021, pp. 35-53. https://doi.org/10.1007/978-3-030-69978-9_4

[2] K. Murphy et al., "Artificial intelligence for good health: a scoping review of the ethics literature," in BMC Medical Ethics, (2021) 22:14, pp. 1-17.

[3] S. Pasricha, "AI ethics in smart healthcare", Retrieved from https://doi.org/10.48550/arXiv.2211.06346, 2022, pp. 1-7.

[4] S. Berger, and F. Rossi, "AI and neurotechnology:learning from AI ethics to address an expanded ethics landscape," Communications of The ACM, vol. 66 (3), March 2023, pp. 58-68.

[5] U.S. Department of Health & Human Services, "Summary of the HIPAA Privacy Rule," Oct 2022, Published at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[6] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," in Artificial Intelligence in Healthcare. Elsevier, 2020, pp. 295-334.

[7] R. Tsaih, H. Chang, C. Hsu, and D. C. Yen, "The AI tech-stack model," in Communications of The ACM, vol. 66 (3), March 2023, pp. 69-77.

[8] B. Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era," in BMC Medical Ethics, (2021) 22:122, pp. 1-5. https://doi.org/10.1186/s12910-021-00687-3

[9] C. Wang, J. Zhang, N. Lassi, and X. Zhang, "Privacy protection in using artificial intelligence for healthcare: Chinese regulation in comparative perspective," in Healthcare, 2022, 10, 1878, pp. 1-19.

[10] E. Chikhaoui, A. Alajmi, and S. Larabi-Marie-Sainte, "Artificial intelligence applications in healthcare sector: ethical and legal challenges," in Emerging Science Journal, vol. 6(4), August 2022, pp. 717-738.

[11] G. Karimian, E. Petelos, and S. M. A. A. Evers, "The ethical issues of the application of artificial intelligence in healthcare: a systematic scoping review," in AI and Ethics, 2022 (2), pp. 539-551.

[12] The Trustees of Princeton University, "Princeton Dialogs on AI and Ethics Case Studies," 2023, https://aiethics.princeton.edu/case-studies/

[13] L. F. Cranor, and H. Habib, "Metrics for success: why and how to evaluate privacy usability," in Communications of The ACM, vol. 66 (3), March 2023, pp. 35-37. DOI:10.1145/3581764

[14] A. Gillespie, "Designing an ethical tech developer," in Communications of The ACM, vol. 66 (3), March 2023, pp. 38-40. DOI:10.1145/354511