To: The World Privacy Forum

From: Vika Li, first-year master's student at McCourt School of Public Policy

Date: Nov 20, 2023

RE: PRIVACY ISSUES IN AI + HEALTHCARE

Executive Summary

Integrating AI into healthcare presents challenges of extensive data requirements and patient privacy. Our client, the World Privacy Forum, is committed to improving data privacy, particularly in relation to patients' data privacy within AI applications. Two strategic options have been discussed, including restructuring the governance of AI health data and promoting data ownership through public awareness. Option 1 is recommended for its potential to safeguard patient privacy effectively. Future steps involve collaboration with the U.S. Department of Health has also been discussed.

Background on Policy Policy Objective:

In the pursuit of enhancing people's well-being, advanced technology softwares, Artificial Intelligence(AI) for example, have been utilized in health care. However, challenges arise concerning the extensive data requirements and data privacy associated with the integration of AI into healthcare practices. In the United States, The FDA has been formulating a regulatory framework for AI/ML-driven software alterations to establish suitable guidelines for safety and effectiveness. NIH has also engaged in collaborations and investments in AI-based projects, focusing on discovering health solutions in various research and medical environments (U.S. Department of Health and Human Services, 2021). Key stakeholders in the AI + Healthcare

realm include the FDA (Food and Drug Administration), responsible for establishing key guidelines for AI utilization in healthcare. Additionally, healthcare providers such as hospitals and clinics play a role in advocating the use of AI technologies in clinical practices, while tech companies like Amazon may advocate for increased accessibility of health data for AI applications. Patient advocacy groups, exemplified by the United States Department of Health and Human Services, contribute by championing fairness and privacy concerns related to the use of patient datasets. Other significant stakeholders include patients, physicians, pharmaceutical companies, and insurance companies.

Health data is very sensitive and involves patients' valuable personal information, which makes proper handling in AI applications imperative for advancing current US AI policies in healthcare (Yee & Raj, 2022). The World Privacy Forum, as the client, is dedicated to enhancing data privacy and governance. They have recognized the possibilities in data breach and ethics challenges in AI applications. Their patients-center approaches empower the fundamental stakeholders, patients, in the area and contribute to the overall well-being of individuals.

Strategic Options

Option 1: Enhanced Governance Structure of AI Personal Health Data Applications, Especially for Commercial Purposes:

The innate nature of AI technologies, to link scattered data together across platforms, disables current privacy regulations on health data (Winter & Davidson, 2019). There is an increasing need to enhance governance and current protocols to protect sensitive health data. Critical aspects, such as determining eligible recipients, specifying the aggregated/disaggregated forms

of data transmission, and defining the extent of decryption, require enhancement to effectively address the evolving challenges posed by sophisticated AI tools.

Pros:

- This is the bottom line to ensure the patients' data safety. Only reasonably adjusted and continuously improved management of health data can keep the application of AI under control and not lead to serious legal issues or adverse consequences for patients. Private companies can
- This will also lead to an increased trust from patients, as their personal health data have been securely guarded by the relevant organizations. With this trust, it will be easier to collect patient data when it is needed in the future.

Cons:

- Enhancing the governance structure of AI personal health data applications is a complex process that requires significant time and resources. Existing systems need to be thoroughly upgraded to accommodate the complex requirements for improved governance.
- The implementation of a strengthened governance structure is a substantial financial investment, involving both budgetary considerations and the willingness of the Government to act decisively.

Option 2: Data Ownership and Control Policies through Public Awareness Campaign Data Sharing:

Empowering patients is always necessary in facing potential data breaches. Strengthening data ownership ensures patients to understand why, how, and potential benefits and harms of their

personal data collections. Only with a full understanding of how patient information will contribute to the development of an AI model will they be equipped to decide whether or not to consent to participate in it. Letting patients know that they have the autonomy to suspend or withdraw their information from any ongoing AI health program is the most powerful weapon for them.

Pros:

- The strategy helps to increase transparency and control over sensitive health data (Chiruvella & Guddati, 2021). Patients can truly understand the data sharing process and pertinent outcomes. They will start to pay attention to terms of consent and identify risks associated with their participations. In addition, once patients are aware of their rights and know how to use them, they will be more protected.

Cons:

- Patients may not be interested in spending time learning. Thus, it is not promising if such education programs will be helpful. Even if patients have taken classes, different education levels and comprehension lead to uneven study outcomes. The effects of such public awareness campaigns are unforeseeable and uncontrollable. Another point is that even if patients already have a thorough understanding of data ownership, private companies can override the effectiveness of public education campaigns by using monetary incentives to induce them to waive their privacy rights.

Strategy Recommendation

I advocate for the first option, which is to restructure the governance system of health data, as the main solution to the above problems. The primary challenge in using AI in healthcare is how to

protect patient privacy. Option 1 provides a systematic solution to address these privacy concerns. The structured framework provided will likely mitigate potential risks and uphold ethical standards. Winter & Davison have argued that the most effective way to regulate health data in AI applications is through explicit requirements set by authorities (2019).

Moreover, this strategy ensures accountability for all stakeholders, clarifying their roles, responsibilities, and rights within the Health + AI industry. If they want to exercise power, they must undertake their responsibilities and follow the rules.

However, this does not mean that public education should be ignored. Instead, it is still necessary to implement it, but it needs to be adjusted in terms of importance. Data ownership education programs can only function well once a data protection structure is in place, operating under clear guidelines within the enhanced governance framework.

Next Steps

- Continuing working with the U.S. Department of Health and Human Services to prompt more patients-centric considerations in formulating policies.
- Advocating for Impact assessment, aiming at evaluating potential risks for any major projects requiring patients' data. How likely will the project succeed in achieving its tentative goals? How likely is it that patients' data might be reidentified and hurt their fundamental human rights? Questions like these should always be considered in granting approval in using AI.
- Calling attention to post-project evaluations to test risk mitigation strategies and provide insights for future applications to ensure continuous improvement and ethical data handling in AI projects.

Reference

Artificial Intelligence (AI) strategy - hhs.gov. (n.d.). https://www.hhs.gov/sites/default/files/hhs-ai-strategy.pdf

Chiruvella, V., & Guddati, A. K. (2020). Ethical Issues in Patient Data Ownership (Preprint). https://doi.org/10.2196/preprints.22269

Winter, J. S., & Davidson, E. (2019). Governance of Artificial Intelligence and Personal Health Information. *Digital Policy, Regulation and Governance*, *21*(3), 280–290. https://doi.org/10.1108/dprg-08-2018-0048

Yee, T. M., & Raj, K. (n.d.). The dual challenge of enhancing healthcare delivery and protecting patient privacy in the age of Advanced Artificial Intelligence Technologies. *Journal of Human Behavior and Social Science.* https://studies.eigenpub.com/index.php/jhbs/article/view/39