

Carlos Betancur

Julia Netter

CSCI 1952B: Responsible Computer Science in Practice

5 May 2024

*Health Insurer Access to Patient Wearable Health and Fitness
Device Data: A Critical Analysis of the Justifications and
Long-Term Risks*

Introduction

The convergence of healthcare and technology has ushered in a new era marked by the widespread adoption of wearable healthcare devices. These devices, spanning from basic fitness trackers to advanced health monitors, provide individuals with unprecedented access to real-time health data. Concurrently, health insurance companies are exploring opportunities to leverage this wealth of information to refine risk assessment methodologies and encourage healthy behaviors. However, the integration of this data into insurance practices presents a host of ethical and practical challenges.

Implementation of a technical artifact aims to tackle these challenges by proposing an innovative solution: a user interface that empowers patients to review, censor, and approve the data included in their health reports provided to health insurance companies.

This report will delve into a critical analysis of the justifications behind health insurance companies accessing wearable healthcare device data and the associated risks of storing this information. The main argument will explore the methodology behind the development of the user interface, justify key design decisions, and examine the potential benefits and drawbacks of the proposed solution.

Problem Space: Conflicts and Tensions

Understanding the problem space of wearable device health data integration into healthcare insurance requires careful consideration of various factors:

Ethical Considerations:

Keeping in mind the principles of medical ethics, developers must grapple with questions surrounding patient **autonomy, beneficence, non-maleficence, and justice**. Tensions surround ensuring that data collection and usage respect patient rights, privacy (Canali 2022), and consent while also ensuring health providers and insurers have sufficient information to make vital healthcare decisions.

Regulatory Compliance:

Developers and health insurers face a complex web of regulatory requirements, including but not limited to HIPAA in the United States, GDPR in the European Union, and various national and regional regulations globally (Canali 2022). Community rating stipulations in the US prohibit insurers from price discriminating amongst users within respective geographic regions.

Equity and Justice:

Many wearable device data programs with health insurance companies offer lower premium rates, discounted wearable devices, and funding towards health services in exchange for increased physical activity (Robeznieks 2019). It is important to note that while individuals might be willing to engage in healthier lifestyles, they might not have the resources to do so. Thus, it is crucial to place guardrails to prevent unjust public health practices rooted in metrics skewed by social disparities.

Conceptual Guardrails

In researching ethical analyses of healthcare data exchanges and referencing expert recommendations, the aforementioned framework of *medical ethics* was identified as an adequate guardrail for the development of the artifact (Meyers 2024). Many of the principles of medical ethics overlap or envelop several key concepts addressed throughout the course this semester:

Data Privacy and Security:

One of the central concerns is privacy, as the collection and storage of sensitive health data raise questions about individuals' rights to control their personal information (Gay & Leijdekkers 2015). While legislation provides existing protections, patients may be apprehensive about insurers accessing their wearable device data, fearing potential breaches of privacy and unauthorized long-term use of their data for unethical business practices (ex: selling data to less regulated industries).

Transparency and Paternalism:

Transparency in the collection and use of wearable device data is essential to ensure that patients understand how their data will be used and have the opportunity to provide informed consent (American Academy of Dermatology Association 2023). This concept touches on the often paternalistic relationship between health providers and patients.

Consent and Autonomy:

Lastly, the concept of consent is fundamental, as patients should have the autonomy to decide whether to share their wearable device data with insurers and how it should be shared (Goldstein 2024). While healthcare providers are free to suggest specific treatments, it is up to patients to accept them.

Expert Consultation

The insights provided by experts highlight specific dimensions of the problem that warrant consideration.

Risks in Standardizing Healthcare Data

David J. Meyers, Associate Director for Advancing Health Policy through Research at Brown University, acknowledged the existing inequities within the healthcare system which are often rooted in distinct data sourcing and collection methods adopted across insurers, health providers, and beneficiaries (Meyers 2024). Standardizing this data through wearable device monitoring enables insurance companies to enhance outreach efforts for high-risk communities and incentivize habits to responsively promote healthy lifestyles amongst beneficiaries.

Existing regulation protects against the misuse or selling of patient data, including the aforementioned HIPPA act and Community rating; however, this data exchange remains subject to potential data breaches or future long-term changes in health insurance regulation.

Enhancing Health Monitoring Sustainably and with Integrity

According to Stephanie Paige Goldstein, Assistant Professor of Psychiatry and Human Behavior, accessible wearable fitness device data for health insurance companies can facilitate telehealth and telemonitoring, enable remote patient monitoring, and provide valuable insights for healthcare insurers to allocate resources (Goldstein 2024). In order to benefit from this data exchange, it is crucial to minimize the creation of unnecessary protected health information (PHI) and distinguish between data points based on degrees of sensitivity.

It is crucial to highlight that wearable health devices measure proxies for health rather than concrete measures. Commercial wearables are not always accurate, underscoring a need to perceive this information as supplementary and not requisite. This further emphasizes the theme of transparency, calling for detailed privacy agreements and the consent of beneficiaries.

Stakeholder Interests

Healthcare providers may be interested in leveraging wearable device data to improve patient outcomes but may also have concerns about data security and patient privacy. Some health insurers partner with third-party stakeholders who analyze health data whose sole interest might be financial gains from this exchange (Canali 2022). Regulators and policymakers must balance

these competing interests to ensure that the use of wearable device data by health insurance companies is ethical, equitable, and transparent.

Navigating Tensions in Access to Wearable Device Data

In the age of big data, accessible fitness device information can facilitate health providers' abilities to provide care for patients. While exchanging this data is inherently risky, much like any medical procedure, it is key to address user autonomy in this exchange to ensure they are subjected to these risks at their discretion.

Weighing the principles of medical ethics theory, by enhancing resource allocation effectiveness and facilitating the identification of at-risk patients, insurance Fitbit data programs enhance providers' ability to deliver beneficence to patients while mitigating the risk of malfeasance. It also provides patients with accessible self-monitoring health tools that further enhance their autonomy, care management programs, and ultimately lead to improved health outcomes and reduced healthcare costs.

Drawing insights from expert references, it is imperative to adopt a patient-centered approach that prioritizes individual autonomy and privacy while harnessing the potential benefits of wearable device data.

Artifact Description

The artifact is a [user-censoring interface](#) designed for patients who have agreed to participate in a data exchange program with health insurance companies. It serves as a platform for patients to control and manage the sharing of their wearable device data with insurers, as well as to review and approve the content of their health reports.

The repository contains a README file with explanations of critical files. To access the artifact click on the link and sign in with the following login info:

- *Email:* jane.doe@gmail.com
- *Password:* 1234

Important Features and Functionality

1. **Transparency and Security:** The censoring tool includes a sign-in page that requires user login information to ensure secure access to the data (a brief specification is included containing pseudo-code for *OAuth 2.0* integration) (Bergman 2023). Additionally, each

data section includes an information popup explaining the purpose and use of each data point.

2. **Interface Readability:** Color contrasts and proper hierarchical design principles facilitate navigation of the censoring tool. The data is graphed, at the user's discretion, to better draw insights from the datasets. The interface organizes health data into distinct sections to enhance readability for both patients and insurers. These sections include *heart rate, weight, diet, exercise, and insights*.
3. **Censuring Tools:** Patients have access to censoring tools that allow them to select the breadth and depth of the data they share with insurers. This includes the ability to omit certain data visualizations or entire datasets altogether based on a critical level.
 - a. **Critical:** Data that is essential for proper health evaluations and proper care management
 - b. **Voluntary:** Data that is not necessary, but beneficial to healthcare resource allocation. This information is often geared towards specific care programs (ex: weight loss, high-risk care). It also includes data that would limit user autonomy if strictly enforced to determine health status (ex: pressuring users to exercise).
 - c. **Unnecessary:** Data collected by the Fitbit app, but is not relevant to evaluating patient health status per expert consultation(ex: sleep). This also includes data points that might risk patient data privacy (ex: GPS location, determining sleep schedule from sleep data).

Type	Data	Time Frame	Classification
Heart Rate	Heart Rate measured in Beats Per Minute (BPM).	Average bpm per day.	Critical
Weight	Weight measured in pounds.	Average weight per week.	Critical
Weight Change	Weight change measured in pounds.	Total weight change from start of the week through end of the week (7 day intervals).	Voluntary
Caloric Intake	Number of calories consumed.	Total calories consumed per day.	Critical
Water Intake	Water consumed in ounces.	Total ounces of water consumed per day.	Critical

Walking Activity	Distance walked or run in kilometers (km)	Average km walked/run per day each week (7 day intervals).	Voluntary
Swimming Activity	Distance swam in kilometers (km)	Average km swam per day each week (7 day intervals)	Voluntary
Sleep Log	Number of hours slept.	Total hours slept per day.	Unnecessary
Friends	Friend profiles including: Names, Age, Date Joined Fitbit, and ID.	N/A	Unnecessary
Profile	Patient profile information: First and Last name, sex, age, weight, height, devices owned.	N/A	Mixed: First and Last initials are retained for identification purposes. For health purposes, age and sex are included as well. All other data points are omitted.
Location	GPS location in longitude and latitude.		Unnecessary

4. **Data Omission and Time Frame Limitations:** The censoring tool only includes data from the previous month, corresponding with monthly premium payments, and omits data classified as “unnecessary”. To safeguard patient privacy, data is presented at a daily average level, and certain data points, like exercise, are averaged across the week to prevent privacy breaches (ex: determining eating schedule from calories per hour, or workout schedule from daily km walked/swam).
5. **Opt-In Features:** The interface includes a voluntary insight feature that identifies health metrics indicative of the need for at-risk care management according to national benchmark standards. Patients can opt into sharing insights based on their health data with insurers.
 - a. *Heart Rate:* Patients are considered at risk if their per day average bpm falls below 60 or rises above 90 (Malcolm 2008).
 - b. *Exercise:* Patients who opt-in for insights in addition to share their exercise data to participate in incentive programs will notify insurers if they meet benchmark standards for daily physical activity of 7,000 steps per day (American Heart Association 2023).

Additionally, users must approve the final censored report before it is shared with insurers.

Technical Limitations

As this is a prototype, the artifact does not have real-time data synchronization capabilities with wearable devices. Data must be manually uploaded. The artifact emulates data collected by the Fitbit App and may not speak clearly to many of the other popular wearable health or fitness devices.

The voluntary insight feature is based on predetermined benchmarks that may not capture all potential health risks or needs for care management (Canali 2022). While it serves the purpose of a prototype, it is not indicative of the nuances involved in health evaluations that often reference confounding or supplementary health metrics.

Technical Design Principles

These technical choices prioritize user autonomy, privacy, and data integrity, reflecting responsible technology practices. In doing so, it maximizes beneficence and minimizes the risk of malfeasance while preserving user autonomy.

User-Controlled Data Presentation

Empowering users to selectively share data aligns with the principle of autonomy and privacy protection.

Data Minimization

Presenting data at a daily average level and averaging certain metrics across the week safeguards patient privacy. While security protections and legal regulations are in place, this prevents the long-term negative impacts of data breaches.

Opt-In Features

The inclusion of voluntary insight features and visualization tools allows users to opt into sharing health metrics indicative of at-risk care needs. This approach respects user autonomy while also facilitating proactive care management by providing insurers with actionable insights based on agreed-upon benchmarks.

Limitations of the Approach

While the artifact empowers individuals to control their health data and participate in data exchanges, it may not address underlying disparities in access to healthcare resources. Moreover, while the data minimization prevents the risks associated with data breaches, it is not responsive to potential loosening of data privacy regulation in the future.

Additionally, I think a trade-off in providing users input regarding the use of certain data or insights features is that it limits healthcare experts' response abilities. While the opt-in features try to avoid excessive paternalism, they place a level of responsibility in the hands of patients who might lack the expertise to accurately monitor their health.

Conclusion

The design of this user censoring tool aims to uphold principles of autonomy, beneficence, and privacy in designing responsible technology solutions. While the artifact empowers individuals to control their health data and engage in data exchanges with insurers, it's essential to recognize its limitations in fully addressing healthcare disparities and systemic inequities. Moving forward, a holistic approach that considers broader societal implications and promotes equitable access to healthcare resources will be critical in realizing the full potential of wearable device data in improving healthcare outcomes.

Works Cited

Robeznieks, Andis. "Insurers Want Patients to Use Wearables. That Could Be a Problem."

American Medical Association, American Medical Association, 26 Aug. 2019,
www.ama-assn.org/practice-management/digital/insurers-want-patients-use-wearables-could-be-problem.

Arnold, J Malcolm, et al. "Resting Heart Rate: A Modifiable Prognostic Indicator of Cardiovascular Risk and Outcomes?" *The Canadian Journal of Cardiology*, U.S.

National Library of Medicine, May 2008,
www.ncbi.nlm.nih.gov/pmc/articles/PMC2787005/.

Bergman, Andy. "Two Factor Authentication on O2 ." *Two Factor Authentication on O2 - HMS*

IT RC O2 - Confluence, Harvard Medical School,
harvardmed.atlassian.net/wiki/spaces/O2/pages/1605009747/Two+Factor+Authentication+on+O2. Accessed 5 May 2024.

Canali, Stefano, et al. "Challenges and Recommendations for Wearable Devices in Digital

Health: Data Quality, Interoperability, Health Equity, Fairness." *PLOS Digital Health*,
Politecnico de Milano, 13 Oct. 2022, www.ncbi.nlm.nih.gov/pmc/articles/PMC9931360/.

Gay, Valerie, and Peter Leijdekkers. "Bringing Health and Fitness Data Together for Connected Health Care: Mobile Apps as Enablers of Interoperability." *Journal of Medical Internet*

Research, U.S. National Library of Medicine, 18 Nov. 2015,
www.ncbi.nlm.nih.gov/pmc/articles/PMC4704968/.

Meyers, David J. Personal Interview with The Author. 22 April 2024.

Goldstein, Stephanie. Personal Interview with the Author. 26 April 2024.

“Start with a Step and Walk Your Way to Better Health.” *Www.Heart.Org*, American Heart Association, 28 Mar. 2023,

www.heart.org/en/affiliates/start-with-a-step-and-walk-your-way-to-better-health#:~:text=While%20the%20goal%20of%2010%2C000,than%20those%20who%20walked%20fe
wer.

“Stop Wearable Medical Devices from Sharing Your Data.” *American Academy of Dermatology*, American Academy of Dermatology Association, 23 June 2023,
www.aad.org/public/fad/digital-health/wearable-devices.