Wearable devices in Healthcare

Introduction

With this busy lifestyle of the 21st century, keeping healthy is a main concern. Wearable devices in Healthcare like smart watches, wrist bands, fitness trackers, etc are the life saver for keeping healthy. These devices come with action packed features like counting steps, counting oxygen saturation levels, heart rate, running speed and several others. These devices then provide in depth analysis based on your activity which can be very fruitful if paid attention to. This whole data is visible on the device as well as on your smartphone on the respectful application. As this whole data is stored on the host cloud from where the privacy and information security issues arise. These issues are the biggest hurdle in this industry. As the storage of this huge amount of sensitive data gives major concern for security risks related to cloud, software application and many more. Moreover, GPS tracking is another major concern, it tracks the user's live location which if fallen into wrong hands can be harmful or sometimes even a national issue.
This report will discuss the various fairness and security issues concerning the wearable devices in healthcare. As the large amount of user data can be accessed by the manufacturers and third parties without user's consent.

Background

Aim for developing such a system

Aim for developing such a system was to enable users to keep track of their daily activities and helping them in discovering patterns which will in turn become helpful in leading a healthy life.

Why is there a need for such a system?

With our growing age, maintaining our fitness becomes the most important aspect to lead a healthy and happy life. It would be a surplus if one could track their wellbeing and achieve higher targets which when achieved makes one proud of themselves.

Benefits of such a system

Making a device which can track the steps you have taken, tells you about your SPO2 levels, your heart rate, your running/walking speed along with the feature of making calls without even touching your smartphone, this all in the form of a wristwatch would definitely be useful for human beings in tracking their wellbeing. Moreover, these devices give you in depth analysis of your performance from which you can track different patterns and make changes to have better results. These help in making better lifestyle choices, reducing stress, breaking vicious bad habits and many more.

Ethical issues in wearable devices

The use of wearable technology for data collection has generated a number of ethical questions, including concerns about disclosure of data collection, the selling of data, manipulation of insurance premiums, different ways of interpreting data and concerns about data loss.

Privacy

Privacy is defined as the claim of an individual or institution to determine for themselves when, how and up to what extent the information about them is communicated to others. The main concern of the user is that they have no control over the data collected and how it is used. Data that is collected through the wearable device is stored by the company in one database, which has the potential to expose if there's a privacy breach.

Fitbit is known for its smart fitness band that provides human health activity measurements and statistics. However, one of the major security vulnerabilities found in Fitbit is the lack of privacy. Fitbit is vulnerable due to leaky BTLE (Bluetooth low energy) technology. The Fitbit can be easily tracked because its unchanged privacy or MAC addresses can be tracked easily. Due to this the third parties can track activities of the specific users. Insurance companies may take advantage of this health data to create a gray market. It also allows malicious people to track the user's location or places visited to make phishing attacks which can disrupt an individual's privacy.

Transparency

Data transparency means utilizing data with integrity so that individuals know what data is being collected, who has access to it, and how they're able to interact with it. Though some companies are open about their data practices, most prefer to keep consumers in the dark. Companies should be more open and communicative about what data they need from their consumers and why. In turn, consumers will find it easier to trust that company and will be more willing to cooperate.

One of the risks that is often overlooked is the fact that outside applications are often given access to user data in Fitbit. Fitbit has instituted a mechanism in which a third-party application can access user data. The application can both read and write to the user data that is stored in the device of the Fitbit user. Third party applications can also request permission to access the scope of the user data. The third-party applications can also modify the data if given the access. The lack of user education on this part can lead to data breach if the user account is hacked. Currently there is no such mechanism for a user to grant read access but no write access to the data.

Legal codes of practice to prevent biased, discriminatory, unintended, or socially undesirable outcomes

While algorithms provide valuable insights from the data there are some models that infer from data about people which includes the identities, demographic attributes and their likely future behaviours. The range of models include movie recommendations, customer credit worthiness in banks, recruitment tools and criminal justice, etc. For instance, breast cancer is a common disease in women. An algorithm with training data would obviously predict most of the labels of breast cancer for females. But it has been discovered that breast cancer is a rare disease that occurs with Men. This as a result creates a bias against Males.

Bias is due to historical human biases in the training data. Incomplete training data could also result in algorithmic bias. If the training data is more representative of a certain category of people than others, the predictions from the models would be adverse for unrepresentative groups. For eg, in most of the cases, aged people or middle aged people get heart diseases. The wearable devices record the data and then predict that such kind of people will have heart disease in future. But this may not always be true, teenagers may also have a heart disease and the algorithm may undermine their age while considering heart disease. Even when the training data is corrected, the outcome may still have problems. Another example would be college admission excluding the applicants with lower income compared to the others who may not be protected to certain harms (Financial hardships). This will produce equal outcomes for different groups.

Detecting and Mitigating Bias

Comparing the results of various groups can be a good starting point.

Datasets with incomplete data may need additional training data to improve overall accuracy and reduce unfair results.

Companies following the government guidelines (non-description and fairness, privacy, technical robustness, accountability) would help them interpret fairness, design processes and equal treatment. Although, even with government guidelines, human interpretation may still be needed to define and measure fairness.

Operators of algorithms could use a bias impact statement that includes a set of questions to guide them through the design implementation and the monitoring phases. This will assist in evaluating the potential detrimental effects of an algorithm. During the implementation phase, if the potential bias listed has occurred, feedback could be retrieved from the impacted populations.

Operators should focus on the potential risk while considering the decision that should be automated.

Operators who develop and use algorithms should be acknowledged by policymakers and customers, who will place greater confidence in their actions.

Stakeholders should be involved to aid programmers in selection of inputs and outputs of certain automated decisions. Engaging users throughout the process would yield improvements to the algorithms which results in improved user experiences.

Finally, operators can consider the role of diversity in training data and decision making processes.

Regularly auditing the algorithms for checking bias is yet another best practice for detecting and mitigating bias.

Automated decisions benefit from knowledge about how this system functions, so algorithmic literacy is important for mitigating bias. Programmers should incorporate feedback systems so that users can respond when the bias negatively affects them.

Possible trustworthy operations

The end user knows that their data is encrypted but they don't know what is happening with their data. That means the system lacks transparency.

Coming to the privacy, User's data is collected without them knowing. So, let's discuss the Transparency and Privacy in relation to the wearables in healthcare.

Transparency

The wearable devices providers need to be transparent about the data being collected. The end user should know where and how their data is being used with prior consent. Any hidden loops in the usage of data should be deemed punishable by law even though that usage is not harming the user.

Companies which are open about the data they collect, give consumers power over their personal data, and provide equal value in exchange for it. Companies can be trusted, and gain continued and increased access. Those who hide how they use personal data and fail to provide value and in return risk losing their customers' trust and their business.

Privacy

The wearable devices providers must educate their employees about privacy and data security, which can be done by enrolling them into various certification programs.

Also, the employees must be encouraged to read and understand the terms and conditions thoroughly so that the important information does not go unnoticed. Moreover, user experience can also be improved by introducing integration of privacy into their system designs.

Users should not share their wearable device with other people because doing so they are risking their trackable information to be misused. Moreover, this will lead to incorrect information being stored which will in turn affect their stats.

Health Insurance Portability and Accountability Act which sets the standard for sensitive data protection. Many of these companies are not HIPAA compliant. Whereas some of the approved HIPAA compliant devices might require users to give explicit consent to share their data. Consumers who are looking for more privacy are provided with the choice to give the consent of what information is being collected and how it will be used.

Conclusion

To sum up, wearable devices have significantly changed the lifestyle of people where they are used as a means for improving health by consistently discovering the activities and patterns. The data is captured for providing depth analysis of any individual's health. While wearable devices have their own advantage, they potentially risk sharing the sensitive information of people present in the collected data. This brings ethical concerns like privacy, fairness and transparency to individual or certain groups of people. Systems like this may lead to bias, discriminatory, unintended or socially undesirable consequences. The system should be responsibly designed with a purpose to avoid any unfortunate consequences to the people. Introducing more transparency to people about what's happening with their information and administering users with choice to give consent for gathering their content are some of ways through which people would gain the trust of the system and thus will fetch more adoption of the users.

References

"Ethics of wearables", 2021. [Online].
Available: https://healthinformatics.uic.edu/blog/ethics-of-wearables/
[Accessed: 25- Apr- 2021].

"Privacy and information security issues", 2021. [Online]. Available:
https://www.researchgate.net/publication/333511479_Wearable_devices_in_healthcare_Privacy_and_information_security_issues
[Accessed: 25- Apr- 2021].

"Wearable technology device security and privacy issues", 2021. [Online]. Available:
https://www.researchgate.net/publication/303870892_Wearable_Technology_Devices_Security_and_Privacy_Vulnerability_Analysis
[Accessed: 25- Apr- 2021].

"Data Transparency", 2021. [Online]. Available:
https://em360tech.com/tech-articles/importance-data-transparency-and-ways-go-about-it#:~:text=Data%20transparency%20allows%20them%20to,be%20more%20willing%20to%20cooperate.
[Accessed: 25- Apr- 2021].

"A look at privacy and security of Fitbit tracker", 2021. [Online]. Available:
https://www.researchgate.net/publication/332926208_A_Look_at_the_Security_and_Privacy_of_Fitbit_as_a_Health_Activity_Tracker
[Accessed: 25- Apr- 2021].

"Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms", 2021. [Online]. Available:
https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/?: amp
[Accessed: 25- Apr- 2021].

“How to Reduce the Security Risks of Wearable Technology for Your Organization | Premise Health”. 2021. [Online]. Available: https://www.premisehealth.com/blog/how-to-reduce-the-security-risks-of-wearable-technology-for-your-organization/
[Accessed: 25- Apr- 2021].

Wearable Devices: Keep Data Privacy In Check - InformationWeek. 2021. [Online]. Available:https://www.informationweek.com/mobile/mobile-devices/wearable-devices-keep-data-privacy-in-check/a/d-id/1298085
[Accessed: 25- Apr- 2021].