Medical Wearables Case Study

Karina Bhattacharya
University of Houston

Table of Contents

Overview of Medical Wearables

Medical wearables are the point at which advancements in technology reach advancements in health. Included in the medical wearables classification are health and fitness trackers, remote patient monitoring devices, and home healthcare devices. Medical wearables have increased in market value, from 6.22 billion USD in 2017 to a projected 14.41 billion USD in 2022 (Rohan). Shipments have increased from projected values 13,460 shipments in 2018 to 97,620 shipments in 2022 (Projected). These projections indicate that medical wearables will become ubiquitous.

As more people use these devices, the security of medical wearables is questioned. How can a consumer safely use a medical wearable without compromising their security? Designers and developers should prioritize medical wearables' security by considering usage patterns, the security of wireless sensor networks, and public policy.

Usage Patterns

Speculative usability, a design philosophy, is the understanding that a product may be used for another use than for which the product was intended (Jones). A Fitbit can be used to monitor sleep, but when paired with the adaptable technology IFTTT (If This Then That), a lightbulb can be turned on when the person wakes up. If wearables were designed to be adaptable to each consumer lifestyle, then the wearables market would reach a diverse population. For instance, health and fitness wearables are marketed towards Generations Y and Z, and those populations use those products the most (see Figure 1, Craver). Speculative usability, an open ended design process, could increase wearables' usage from older demographics.

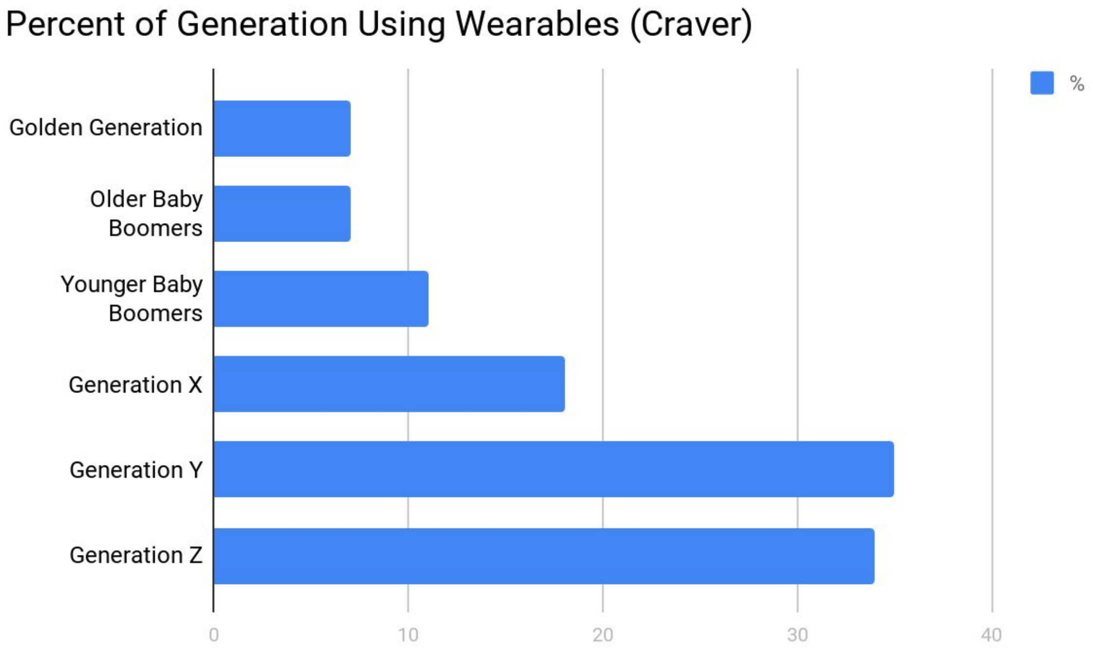

Figure 1. Percent of Generation Using Wearables (Craver).

Medical wearables should have unique security because of how they are used. These devices are worn continuously. Remote patient monitoring devices and home healthcare devices are used continuously or as directed by the patient's health professional. Health and fitness wearables are designed for long-term use, as they monitor use throughout the day. All medical wearables are worn continuously. Therefore, regular computing methods that were created for intermittent computer use can not be directly applied to wearables.

Solutions for medical wearables' security include the following: (1) Products may not be cryptographically secure from the vulnerabilities found in the software because of implementation errors; For updates, a proper chain of trust must authenticate a software stack; authenticating an update image is unreliable; (2) The microcontroller must be programmed before placed in the circuit board; (3) External programmability of the microcontroller must be disabled; (4) Any debug or unnecessary interfaces must be disabled.

Wireless Sensor Networks

The ideal wearable user is a “biocitizen,” or “a person who dutifully gathers information about their body and then shares that data with others to engage in proactive health self-management” (Swan). Wireless sensor networks transfer data from the patient to the health care provider. This transfer of sensitive information must be secure to ensure the biocitizen manages their health.

For the security of wireless sensor networks, confidentiality, integrity, and authenticity must be considered (Sabbah). To achieve this, security protocols must be stronger than usual sensor network protocols. Privacy is considered by prioritizing authorization over authentication, to determine what level of access is available to different users. For instance, a patient should have different access to information than insurance personnel. To prevent Denial of Service (DoS) attacks, transfer of information must be timely, reliable, and persistent. Wearables, such as glucose monitors, must be operating consistently to maintain the patient’s health. It is important to protect the base/station access point and to have reliable routing. Different services can accompany different data from the wearable as well. False data injection can cause an unsuspecting patient to follow potentially harmful dosage instructions for medicines. To prevent against false data injection, the physical home and base station must be protected.

Public Policy

Policy also regulates the security of wearables. The Texas Data Breach Notification Law requires that any person or entity that conducts business in Texas holding sensitive personal information must notify the individual of any unauthorized access of their privacy information (including name, government ID info, and card numbers) (Tuma). This law expands beyond Texas because it requires the notification of persons, not only Texas citizens, of the privacy breach.

For medical devices, The Health Information Privacy and Portability Act included that healthcare providers would have different access to health information than the patient (Sabbah). And more recently, the privacy policies of wearables have changed due to GDPR (General Data Protection Regulation). Specific health metrics can only be measured with user consent.

Consumer Impact

Wearables are not currently marketed for their privacy. A study was conducted to determine the most desirable features of fitness wearables. The top two features were the device’s 24-hour battery and the device’s physical comfort.

Wearables for remote patient monitoring and home healthcare pose a high security risk. When wearables’ security falters, the patients’ immediate health could be at risk. Since health fitness wearables’ information (such as daily steps) devices is less sensitive, these wearables pose less of a risk than the other medical wearables.

All medical wearables can be protected by considering usage patterns, wireless sensor networks, and public policy. With those considerations, companies could market their products as secure. A reputation of security could benefit a company among any future public concerns for data privacy.

References

Rohan. (2018, January 23). Wearable Medical Devices Market Worth 14.41 Billion USD by 2022. MarketsandMarkets. Retrieved from https://www.prnewswire.com/news-releases/wearable-medical-devices-market-worth-1441-billion-usd-by-2022-670703613.html

Projected healthcare wearable device shipments worldwide from 2015 to 2021 (in 1,000 units). (2018). [Graph illustration on health wearable shipments worldwide as of September 2016]. *Statista*. Retrieved from https://www.statista.com/statistics/607932/projection-of-the-healthcare-wearable-device-shipments-worldwide/

Jones, J. & Gouge, C. (2017). Design Principles for Health Wearables. *Communication Design Quarterly, 5*. Retrieved from http://delivery.acm.org.ezproxy.lib.uh.edu/10.1145/3140000/3131205/p40-jones.pdf?ip=129.7.158.43&id=3131205&acc=ACTIVE%20SERVICE&key=B63ACEF81C6334F5%2E4E5EDBE671A33DAE%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1530842875_f8ab5cc1801cbf36b583b5f13f7232d0

Ho, K. & Yao, C. (2017, December). Health apps, wearables, and sensors: The advancing frontier of digital health. *British Columbia Medical Journal, 59*(10). Retrieved from http://web.a.ebscohost.com.ezproxy.lib.uh.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=aaad58df-d9dd-419a-a83b-5fa92535a736%40sessionmgr4010

Arias, O. & Wurm, J. (2015, April-June). Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7321811&tag=1

Rantakari, J. & Ignet, V. (2016, February). Charting Design Preferences on Wellness Wearables. *Proceedings of the 7th Augmented Human International Conference 2016, Article 28*. Retrieved from https://dl-acm-org.ezproxy.lib.uh.edu/citation.cfm?doid=2875194.2875231

Tuma, S. (2013, January 11). Texas' Amended Data Breach Notification Law is Expansive. BrittonTuma. Retrieved from https://www.jdsupra.com/legalnews/texas-amended-data-breach-notification-33265/

Craver, J. (2015, October 7). Young people way ahead of use in wearables. Benefits Selling. Breaking News. Retrieved from https://search-proquest-com.ezproxy.lib.uh.edu/docview/1719467329?accountid=7107&rfr_id=info%3Axri%2Fsid%3Aprimo

Sabbah, E. & Kang, K. (2008). An application-driven approach to designing secure wireless sensor networks. Wireless Communications and Mobile Computing. 8. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1002/wcm.583

Sample Case Study Questions

1. How should security be considered for the different types of medical wearables: health and fitness, remote patient monitoring, and home healthcare? All medical wearables can be protected using the same security methods. Health and fitness wearables pose a low security risk because personal fitness data is not highly sensitive information. Remote patient monitoring devices and home healthcare devices pose a high security risk because device hacking and malfunction can pose a health risk to the patient.
2. How can security be marketed to consumers? Customers concerned of data privacy may choose not to buy the product. A medical wearable equipped with thorough security features could be marketed to these consumers.
3. Why does speculative usability apply specifically to wearables? The wearable device market is very new, and wearables have a wide range of uses. The wearable device market changes as consumers look for new ways to adapt wearables to their personal use.
4. How does public policy affect the future of medical wearables? Public policy is reactionary to the advancements of wearable technology. Privacy policy has changed companies' interactions with their customers' data.
5. Why do medical wearables need unique security? Regular computing methods are insufficient to protect wearables that are worn continuously.