Sarah Manlove
June 18, 2018

How Do Companies Protect User Data on Mobile Health Applications?

Summary

Mobile health applications, some of which are considered part of wearable technology, have been gaining popularity over the past few years, and each new application produced adds new features, giving the applications more power than ever before. However, with this power comes concerns over privacy and security. Since these applications are gathering data about users' health, is this data being protected, or do outside parties have the ability to access this information? If this is occurring, do the users know about it? Do the users have access to privacy policies?

In order to answer these questions, I consulted research databases, government policies, and healthcare security sites. As I gathered research, I narrowed my focus to devices such as the Apple Watch, the Fitbit, the Samsung Gear, apps on cellular phones, and other devices or applications that record health data but aren't affiliated with healthcare providers or medical centers.

Do these applications collect sensitive information?

Personally identifiable information, or PII, is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual" (*Rules*). If medical information collected from a device or application also has access to PII, then there is much more vulnerability on the user's part. Additionally, many health and fitness trackers also have GPS components, so there is also the possibility of that being shared as well. For instance, Dey et al. found that imperfections on a smartphone's accelerometer allow users to be uniquely identified (Dey, Sanorita et al.), which means that users could be tracked and their locations recorded.

Along with PII and the user’s location, these mobile health devices and applications record health information. Many of these trackers record users’ activity, including heart rate, distance traveled, nutrition, sleep, and reproductive health (“IOS - Health.”). Personally identifiable information that is also stored with medical records such as the ones mentioned gives the company that owns the application enough data to potentially cause harm if not secured correctly.

How do these applications store and transmit data?

Each device or application has a different way to store and transmit its data. For example, an Apple Watch encrypts all data when the phone is locked, in transit to iCloud, and in the iCloud servers (“Privacy - Approach to Privacy.”). Some third party applications, however, send personal information over the Internet without encryption, such as when Huckvale et al. discovered in their study that 66% of sampled apps did this (Huckvale, Kit, et al.). Many devices also connect over Bluetooth or can be plugged into a computer to transmit information (Do, Quang, et al.).

Is this data protected by HIPAA?

The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law that protects individual’s health records and other medical information. This law pertains to “covered entities” like health plans, healthcare providers, healthcare clearinghouses, and business associates, who are defined as “a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information” (HHS Office). This means that unless a company making a health app or a wearable device are providing direct service to a covered entity, these companies are not required to comply with HIPAA standards.

Are there any policies in place to protect this data?

In a digitized world, privacy policies are a common pop-up occurrence. However, a 2016 study showed that 81% of Android health apps targeting diabetes did not have a privacy policy in place (Snell). For those apps and wearable devices that do have a privacy policy, however, they can either be hard to find or written with complex and technical language that the average person does not read. Without reading the fine print, users can inadvertently give companies permission to sell their data to third parties. These third parties may include advertisers or a person’s insurance company, as “selling data is an integral part of the business model for many health app developers” (Armstrong).

As for legal policies in place for this data, there are no laws other than HIPAA that protect user's medical information from being disseminated.

Conclusion

Companies have very few protections in place to secure their users' data. Aside from some of the larger, more well-known companies like Apple, many of the smaller app developers don't even provide a privacy policy to alert users as to how their data is being collected, used, and stored. Additionally, even though these applications and devices are dealing with medical data, they aren't covered by HIPAA regulations because they aren't affiliated with healthcare providers. In order to protect sensitive information that these apps and devices collect, lawmakers should propose regulations to create an open and honest environment for users. As Adam Thierer points out, too many regulations could stifle creativity and entrepreneurship (Thierer), so I propose that lawmakers require all applications to have a privacy policy available to all users when the application is downloaded. Thus, users have the opportunity to learn how their data is being used but does not dissuade entrepreneurs from wading into a new industry for fear of heavy regulations.

Until these companies change their current business practices, users need to be aware that their devices may not be as private as they once thought. Each company may have a different privacy policy, so it is important to read the fine print. However, companies must also be held accountable, as their primary duty is to their user. Creating a product that is misleading ultimately reflects onto the company and their own values.

Works Cited

Armstrong, Stephen. “What Happens to Data Gathered by Health and Wellness Apps?” *BMJ*, 2016, p. i3406., doi:10.1136/bmj.i3406.

Dey, Sanorita et al. “AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable.” NDSS (2014).

Do, Quang, et al. “Is the Data on Your Wearable Device Secure? An Android Wear Smartwatch Case Study.” *Software: Practice and Experience*, vol. 47, no. 3, 2016, pp. 391–403., doi:10.1002/spe.2414.

HHS Office of the Secretary,Office for Civil Rights, and OCR. “Summary of the HIPAA Privacy Rule.” *HHS.gov*, HHS.gov, 26 July 2013, www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Huckvale, Kit, et al. “Unaddressed Privacy Risks in Accredited Health and Wellness Apps: a Cross-Sectional Systematic Assessment.” *BMC Medicine*, vol. 13, no. 1, 2015, doi:10.1186/s12916-015-0444-y.

“IOS - Health.” *Apple*, Apple, www.apple.com/ios/health/.

“Privacy - Approach to Privacy.” *Apple*, Apple, www.apple.com/privacy/approach-to-privacy/.

Raij, Andrew, et al. “Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment.” *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11*, 2011, doi:10.1145/1978942.1978945.

Rules and Policies - Protecting PII - Privacy Act. GSA, 24 Apr. 2018, www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.

Snell, Elizabeth. “How Weak Mobile Health App Privacy, Security Affects Patients.” *HealthITSecurity*, HealthITSecurity, 19 June 2017, healthitsecurity.com/news/how-weak-mobile-health-app-privacy-security-affects-patients.

Thierer, Adam D. “The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation.” *SSRN Electronic Journal*, 2014, doi:10.2139/ssrn.2494382.