Quokka

WHITEPAPER

Healthcare Hacking & Protecting mHealth Apps

Quokka

Whitepaper

Healthcare Hacking & Protecting mHealth Apps

As our world becomes increasingly digitized, we see new apps emerging daily. In recent years, one industry where we've seen the emergence of mobile apps is the healthcare, wellness, and fitness industry, also known* as mHealth apps.

Since 2020 and the rise of the pandemic, hospitals and healthcare providers have been gravitating more towards mHealth apps and rely on the technology to provide adequate information and communication for their patients. The trend of these healthcare apps has been to innovate first and secure their data second, leaving patients' valuable information vulnerable to attackers. Whether you use a mHealth app for fitness or healthcare, these apps give you access to a wide array of data, from sleep monitoring, analyzing your metabolic rate, or reviewing blood work, all of which is valuable health information that can be stolen by cybercriminals.

Threat actors are incentivized by money, and currently, selling healthcare records is one of the most lucrative forms of cyber theft. Cybercriminals know that healthcare organizations have a wealth of valuable personal data from their clients and patients, and, with such a large attack surface, they can easily gain access to payment and insurance information, among other data, making application security of the utmost importance for the ever-evolving healthcare industry.

Healthcare Hacking

Excess Scripts, a mobile app that allows patients to access and manage their prescriptions easily from their phones or tablets, announced a data breach directly related to unauthorized access via their mobile application. According to a notice that was sent to customers, the information leaked included prescription history for 24 months prior to the breach and potentially included the patients' names, medications, dosages, physicians, and pharmacy on record.

The Express Scripts data breach is not an anomaly; according to TechTarget, "the number of healthcare breaches in the first five months of 2022 has nearly doubled from the same period last year." For sensitive healthcare data to remain secure, leaders must rally around data security as a corporate value and implement appropriate procedures to stay ahead of threats.

Does HIPAA Protect mHealth Apps?

HIPAA—the Health Insurance Portability and Accountability Act—protects sensitive patient information from being disclosed without the patient's consent or knowledge. However, this governing standard does not always safeguard mHealth apps and the data they collect because the vendor is not a covered entity or business associate. In fact, most mobile apps do not fall under the scope of compliant apps, as they are made for personal use and do not feature protected health information (PHI).

Applications, such as patient user portals, ambulance dispatch, and prescription management, remain covered by HIPAA Rules and Regulations, only sharing electronic patient health records with the patient's explicit consent. While other applications, such as sleep monitoring, fitness apps, maternity, and mental health, can collect user-provided data and share it with advertisers or other third parties. Mhealth apps have major benefits when it comes to monitoring and accessing data related to your health, but they can also pose significant privacy threats.

HIPAA Compliance: The 5 Crucial Rules for mHealth Apps

Rule 1: Privacy

Healthcare clearing houses, employer-sponsored health plans, health insurers, and medical service providers are examples of protected HIPAA entities, and this rule intends to secure individuals' medical records and other personal health information maintained by these organizations. The privacy rule imposes restrictions on the range of disclosures and uses that can and cannot be undertaken without patient consent.

Rule 2: Security

The purpose of this rule is to safeguard individuals' electronic personal health information (ePHI), which is produced, acquired, used, and/or stored by covered entities.

To maintain the confidentiality, integrity, and security of a person's health information, it is generally necessary to apply three types of safeguards: administrative, physical, and technical.

Rule 3: Breach Notification

A breach is any unauthorized use or disclosure of PHI by a party other than a covered entity. The Breach Notification Rule aims to alert patients when their protected health information is improperly used or disclosed.

Rule 4: Enforcement

This rule entails stringent oversight for compliance with the Security and Breach Notification Rules and the Privacy Rule and carries regulations on compliance, investigations, hearings, as well as fines for infractions.

The HHS reserves the authority to punish businesses and impose other sanctions if they violate this regulation.

Rule 5: Omnibus

Healthcare providers must amend their Business Associate Agreements in order to comply with HIPAA requirements, according to the final rule.

This rule modifies the Security, Privacy, Breach Notification, and Enforcement Rules with the goal of enhancing data sharing's confidentiality and security.

It takes special expertise to create an mHealth app that complies with HIPAA regulations. You must be meticulous and strictly adhere to the HIPAA rules and requirements, and, in most cases, this requires the help of a mobile security expert.

Assessment of Health App Security

We understand what it takes to be considered “safe” as an mHealth app, but how many apps within the Health and Fitness category actually meet these requirements?

We’ve compiled some data on apps within the health and fitness category for the last two years. Since 2021, Quokka (previously Kyptowire) has scanned over 3 billion lines of code across 70,000 Android and iOS applications. From these scans, applications classified as mHealth apps totaled 384 unique iOS apps and 269 unique Android apps.

Using our Mobile Application Security Testing platform, we’ve assigned threat scores to applications rating their security and privacy readiness, with higher scores indicating lower readiness. For Android apps, the average threat score was 58.7; for iOS apps, the average threat score was a lesser, but still notable, 43.2. The total average threat score across all apps is 58.7.

The top IoRs, or inter-organizational relationships, found for each software platform:

- Android has an extra 175 permissions, a constant HTTP URL, links with social media networks, and allows backups.
- On the other hand, iOS executes external libraries.

The Quokka Advantage

App security is of the utmost importance at Quokka, and we are a leading cyber security company.

We offer expert, secure end-to-end mobile application security solutions because we believe everyone who uses or creates mobile apps deserves the highest degree of protection and privacy imaginable.

We go above and beyond with mobile application security testing so that you can be confident that your app is secure, and you can also verify the security levels of your mHealth app for added peace of mind.

Understand your security, privacy, and compliance risks and protect your apps today with Quokka.