

Security Concerns in Android mHealth Apps

Archived: 2026-04-05 13:19:41 UTC

Mobile Health (mHealth) applications lie outside of regulatory protection such as HIPAA, which requires a baseline of privacy and security protections appropriate to sensitive medical data. However, mHealth apps, particularly those in the app stores for iOS and Android, are increasingly handling sensitive data for both professionals and patients. This paper presents a series of three studies of the mHealth apps in Google Play that show that mHealth apps make widespread use of unsecured Internet communications and third party servers. Both of these practices would be considered problematic under HIPAA, suggesting that increased use of mHealth apps could lead to less secure treatment of health data unless mHealth vendors make improvements in the way they communicate and store data.

- General Medicine
- APA
- Standard
- Harvard
- Vancouver
- Author
- BIBTEX
- RIS

He, D., Naveed, M., Gunter, C. A., & Nahrstedt, K. (2014). Security Concerns in Android mHealth Apps. *AMIA ... Annual Symposium proceedings / AMIA Symposium. AMIA Symposium, 2014*, 645-654.

Source: <https://experts.illinois.edu/en/publications/security-concerns-in-android-mhealth-apps>