



Nudging Data Privacy of Mobile Health Applications in Saudi Arabia

Abdulahkim Sabur, Taibah University, Saudi Arabia*

 <https://orcid.org/0000-0001-6373-3584>

Ahmad J. Showail, Taibah University and University of Prince Mugrin, Saudi Arabia

 <https://orcid.org/0000-0001-6026-9739>

ABSTRACT

Mobile health apps are a digital era revolution, facilitating direct patient-physician communication, lab and test orders, and medication refills. Despite these benefits, security and privacy issues arise due to handling sensitive data. This paper assesses the security and privacy of Saudi Arabian mobile healthcare apps, gauging compliance with the Personal Data Protection Law (PDPL). Results highlight varied PDPL compliance, underscoring the imperative for enhanced security measures in the digital healthcare landscape.

KEYWORDS

Data Privacy Laws, Mobile Health Apps, Security and Privacy, User Privacy

INTRODUCTION

Mobile devices have become essential objects that we all depend on in our daily lives. With the advancement of computing and technology, we can conduct all kinds of tasks using mobile devices by just connecting to the internet and having sufficient processing power. This improvement in technology has also led to advancements in using mobile devices to enhance the healthcare industry (Sim, 2019; Zhou et al., 2019). Nowadays, patients can benefit from mobile health applications to help them get proper medical care and/or facilitate how they receive medical care. The shift from traditional medical services, where patients need to go physically to the medical care facility, imposes substantial challenges in terms of the security and privacy of this type of activity. Patients can now consult a physician without having to physically go to a medical care facility; they can request to book online appointments, send private messages to the physicians, check the lab and radiology reports, and complete many other medical-related tasks that were not possible before the era of mobile health applications. However, the security and privacy challenges imposed by these applications raise concerns to the patients and health providers because of the sensitive and private nature of the data processed by these applications. Furthermore, it is crucial that mobile health applications comply with security and privacy regulations set by regulators to ensure that healthcare providers are preserving patients' data privacy.

DOI: 10.4018/IJISP.345647

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Recently, healthcare providers in Saudi Arabia migrated many services to mobile health applications to enhance the patient experience, increase efficiency, and optimize resource utilization. In fact, mobile health applications collect a lot of data from users to help them better comprehend their health status and to promote their overall well-being. These applications also store and process other sensitive information, such as users' health-related data, location, lists of contacts, and personal photographs (Papageorgiou et al., 2018; Yasini & Marchand, 2015). Yet, these health applications need to comply with the Saudi Arabia's Personal Data Protection Law (PDPL) to ensure the patients' sensitive information is protected and properly handled. Also, many of these applications have not been tested properly in terms of efficacy and safety (Armontrout et al., 2018). The need for proper verification and checking the security of this mobile health application is more important when it comes to elderly people who might have limited knowledge about the way these applications should be used and how to interact with the healthcare provider via the app (Davidson & Jensen, 2013; Harrington et al., 2018).

In 2016, the European Union (EU) proposed the General Data Protection Regulation (GDPR) (Li et al., 2019; Tankard, 2016; Truong et al., 2021; Voigt & von dem Bussche, 2017; Zhang et al., 2018), marking a significant milestone in the EU's recent accomplishments. This regulation replaced the 1995 Data Protection Directive, which was established during the early stages of the internet's development. The GDPR sets the base guidelines for any technology provider who might be dealing with, directly or indirectly, personal data and information. The GDPR directly impacts any technology platform that collects, stores, and manages personal data. The regulation is considered a massive transformation in how service providers can and should deal with users' data in a way that guarantees the safety of data and ensures its privacy preservation (Houser & Voss, 2018; Wachter, 2018; Zaeem & Barber, 2020). The GDPR sets the guidelines on how data should be processed, and some of these guiding principles of data protection include: Lawfulness, Fairness and Transparency, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Confidentiality, and Accountability (Gruschka et al., 2018; Houser & Voss, 2018). The risk of not complying with the GDPR can result in serious financial fines by regulators, just like what happened to Amazon and Google when they were fined for non-compliance, for which they paid \$887 million and \$391.5 million, respectively (Kendra Barnett, n.d.; Shead, 2021).

Since the implementation of the GDPR, many research works have been introduced to analyze mobile applications' privacy and their compliance with the GDPR. Garais et al. (2018) used the Resource Description Framework (RDF) to analyze data transfer processing in mobile applications. Liu et al. (2021) used a classification and rule-based approach to analyze a corpus of 36,610 labeled sentences from 304 privacy policies, where 1,180 compliance issues were detected out of the 304 privacy policies. Guamán et al. (2020) studied personal data movement across borders in Android mobile applications. Out of 100 analyzed apps, 66% of them did not have a clear disclosure on how the data transfer across borders was to be implemented, which presents a clear violation of the GDPR.

The Council of Ministers in Saudi Arabia approved the PDPL in September 2021 and approved an amendment in March 2023 to impose the proper regulations for technology providers working with personal data under the geographic limits of the Kingdom of Saudi Arabia (Saudi Data & AI Authority, 2023). The PDPL gives individuals in the Kingdom the right to control how their data is being processed. This new law is applicable to all hospitals and clinics that process the personal data of Saudi citizens, residents, and visitors. The newly proposed law is believed to make a great impact on how healthcare facilities handle individuals' personal data. Although the PDPL was approved in September 2021, the law has only been enforced since the end of September 2023 (Saudi Data & AI Authority, 2023). Hence, mobile healthcare application providers must ensure compliance with the PDPL in order to avoid hefty fines. In this paper, we focus on the PDPL and analyze to what extent private healthcare mobile applications are complying with it. Our analysis shows that many mobile healthcare applications in the Kingdom provide low-security protection on their platforms.

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/nudging-data-privacy-of-mobile-health-applications-in-saudi-arabia/345647

Related Content

Statistical Models for EHR Security in Web Healthcare Information Systems

Stelios Zimeras and Anastasia N. Kastania (2011). *Certification and Security in Health-Related Web Applications: Concepts and Solutions* (pp. 146-158).

www.irma-international.org/chapter/statistical-models-ehr-security-web/46880

Secure and Robust Telemedicine using ECC on Radix-8 with Formal Verification

Gautam Kumar and Hemraj Saini (2018). *International Journal of Information Security and Privacy* (pp. 13-28).

www.irma-international.org/article/secure-and-robust-telemedicine-using-ecc-on-radix-8-with-formal-verification/190853

An Adaptive Trustworthiness Modelling Approach for Ubiquitous Software Systems

Amr Ali-Eldin, Jan Van Den Berg and Semir Daskapan (2014). *International Journal of Information Security and Privacy* (pp. 44-61).

www.irma-international.org/article/an-adaptive-trustworthiness-modelling-approach-for-ubiquitous-software-systems/140672

Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method

N. R. Mead (2007). *Integrating Security and Software Engineering: Advances and Future Visions* (pp. 43-69).

www.irma-international.org/chapter/identifying-security-requirements-using-security/24050

Data Privacy and Security: HIPAA and Small Business Compliance

James Suleiman and Terry Huston (2009). *International Journal of Information Security and Privacy* (pp. 42-53).

www.irma-international.org/article/data-privacy-security/34057