A New Privacy Framework for the Management of Chronic Diseases via mHealth in a Post Covid-19 World

Farad Jusob, Carlisle George and Glenford Mapp
ALERT Research Group, Department of Computer Science Middlesex University, London.
(FJ105@live.mdx.ac.uk)

New challenges are being faced by global healthcare systems such as an increase in the elderly population, budget cuts as well as the ongoing COVID-19 pandemic. As pressures mount on healthcare systems to provide treatment to patients, mHealth is seen as one of the possible solutions to addressing these challenges. The emergence and rapid development of mHealth has the potential to play an important role in the transformation of healthcare and increase its quality and efficiency. mHealth solutions cover various technological solutions, that allow for their users to measure vital signs such as heart rate, blood glucose level and blood pressure. Patients, through the use of sensors and mobile applications, are able to collect medical, physiological, lifestyle, daily activity, and environmental data. This could serve as a basis for evidence-driven care practice and research activities as well as contribute to patient empowerment as they would be able to manage their health more actively whilst still living more independent lives in their own home environment due to self-assessment or remote monitoring solutions. Given the sensitivity of health data (i.e. special category data under the GDPR), the rapid development of the mHealth sector raises privacy and security concerns regarding the data collected from users. In the context of mHealth, managing privacy is a complex issue that may be best achieved by enabling patients a measure of control over data various processing activities such as the collection, recording, dissemination, and access to their mHealth data. The management of privacy can be facilitated by the use of suitable privacy frameworks that embody core privacy principles, best practices, and solutions to protect and manage the privacy of information and people. Having a suitable privacy framework for mHealth in the context of the management of chronic diseases is therefore essential to building patient trust and providing good healthcare.

In this study, a review of various existing regulatory frameworks for privacy (e.g. *GDPR; GAPP, Markle Common Framework; ONC privacy Framework; Information Systems Development Privacy Framework; OECD privacy Principles; Privacy by Design Principles, HPP Best Practice principles*) concluded that no single framework completely addresses privacy concerns regarding the management of chronic illnesses when using mHealth solutions. After investigating (i) privacy concerns when managing chronic diseases in the context of mHealth and (ii) how existing framework addressed these concerns, a novel privacy framework for mHealth in the context of chronic disease management was proposed. The framework consists of five layers forming a pyramid structure, from bottom to top namely:

- **Layer 1**: ***Regulatory Frameworks for Privacy and Privacy Threats/Concerns***. In this bottom layer, privacy obligations are identified from existing regulatory/privacy frameworks and threats/concerns are identified from research studies. This ensures that the framework is current and built upon existing regulatory provisions and research findings.
- **Layer 2**: ***Privacy Principles***. In this layer privacy principles are created from information gathered in the previous layer. Principles address issues such as: user autonomy, data accessibility, data control, data misuse/abuse, profiling, surveillance, consent, accountability and device visibility.
- **Layer 3**: ***Privacy Requirements***. In this layer, specific privacy (software) requirements are derived from the privacy principles for the development of an mHealth system.
- **Layer 4**: ***Mechanisms and Associated Technologies***. In this layer technologies and mechanisms are identified and selected in order to implement the privacy requirements in the previous layer.
- **Layer 5**: ***Prototype* -** In this top layer the technologies and mechanisms selected in the previous layer are used in the development of an integrated mHealth system facilitating privacy management.