Controlling reliability, interoperability and security of mobile health solutions

Damien Gruson1,2,3

1 Department of Clinical Biochemistry, Cliniques Universitaires St-Luc and Université Catholique de Louvain, Brussels, Belgium
2 Pôle de recherche en Endocrinologie, Diabète et Nutrition, Institut de Recherche Expérimentale et Clinique, Cliniques Universitaires St-Luc and Université Catholique de Louvain, Brussels, Belgium
3 Emerging Technologies Division, International Federation of Clinical Chemistry and Laboratory Medicine

ARTICLE INFO

Corresponding author:
Prof. Damien Gruson
Department of Clinical Biochemistry
Cliniques Universitaires St-Luc and
Université Catholique de Louvain
10 Avenue Hippocrate
B-1200 Brussels
Belgium
Phone: +32-(0)2-7646747
Fax: +32-(0)2-7646930
E-mail: damien.gruson@uclouvain.be

Key words:
mobile health, framework, privacy, sensors, digital, data

ABSTRACT

Mobile health (mHealth), including mobile devices and digital services, is a component of the transforming health ecosystem. The validation of the scientific validity, analytical performance, clinical performance and security of mHealth solutions is critical to guarantee patient care and safety. To this end, laboratory experts, scientific societies and notified bodies should define and recommend validation framework addressing multiple dimensions.
1. MOBILE HEALTH AS A PIECE OF A NEW HEALTH ECOSYSTEM

Mobile health (mHealth), including mobile devices and digital services, is a component of the transforming health ecosystem (1,2). The development of smart devices, sensors and digital applications is exponential since several years in our daily life and in health care (3,4). Through remote monitoring and digital services, mHealth also contribute to the accessibility to virtual health and new models of caring (5). The coronavirus disease 2019 (COVID-19) pandemic has generated a global public health crisis and rapid testing and contact tracing using smartphone technology are used to limit disease transmission (6,7). Covid19 pandemic has therefore clearly accelerated the transition to mHealth services (6,7). Covid19 also speeded up the use of telemedicine for safer consultations and diagnoses, and of artificial intelligence (AI) for epidemiologic modeling, prediction of severe forms or allocation of resources (6,7).

Mobile Health is offering new solutions and opportunities to healthcare professionals, to patients and citizen for monitoring health status and for improving health outcomes (5). Sensors, mobile devices and health applications allow also to collect and exchange a large amount of health data for offering a new class of advanced services characterized by being available anywhere, at any time and for multiple healthcare stakeholders (8). Through an interactive and structured data lake, interventions can therefore be conducted in real time (8). By allowing real time monitoring of clinical and biological variables as well as the integration of remote monitoring and telemedicine, the follow-up of outcomes is easier, which facilitates transition to value-based care (9). Figure 1 is summarizing some features related to mHealth.

Figure 1  The benefits of mHealth
It is clear that a new form of interconnection between the physical and digital worlds is accompanying mHealth (3). It is also clear that if mHealth is offering multiple advantages, several challenges such as safety and privacy of the solutions need to be overcome for a safe and valuable use and will be introduced in this article.

2. RELIABILITY AND SAFETY

The conformity assessment of the components of mHealth ecosystem is mandatory to ensure the quality of solutions or devices and to guarantee patient safety. In Europe, the new CE IVDR regulation is also reinforcing the control of the performances of device and post-market performance follow-up (10). With the new CE IVDR, as of May 2022 the level of clinical evidence needed to demonstrate the conformity of a device becomes progressively more stringent as the risk class increases.

The control of the mHealth solutions involving testing monitoring of laboratory data needs to involve specialist in laboratory medicine and scientific societies to ensure that multiple dimensions are evaluated according to recognized international standards. Experts in laboratory medicine have to validate the scientific validity, analytical performance and clinical performance of the mHealth solutions. Laboratory experts, scientific societies and notified bodies should define and recommend validation techniques and a standardized framework integrating of the mHealth solutions (11–13). Multiple dimensions should be considered in such validation framework and multiple players will be involved (13).

Manufacturers play a major role in setting internal diagnostics methods to improve the quality, control and maintenance of devices (11). This type of internal performance monitoring has to ensure a faulty data detection method consisting of the detection of faulty or incorrect values during the data acquisition and processing stages. Introduction of a data correction method consisting of the estimation of faulty or incorrect values obtained during the data acquisition and processing stages also has to be considered. In addition, a data context classification or uncertainty mechanism could be considered as possible approaches for the correct validation of data (11).

Specialist in laboratory medicine will play a critical role for the education and training of the users, as well as in a dynamic control of the device supervised by clinical laboratories as illustrated by the initiative of the French society of laboratory informatics Control of glucose meter and INR device (14).

Another important point for the evaluation of mHealth solutions will be their level of data standardization and interoperability (15). Such interoperability allows mHealth solutions to communicate effectively without compromising the content of the transmitted data and to share patient health information among healthcare professionals and organizations (15). Interoperability and data exchange can be assessed based on the recommendations of the European Interoperability Framework (16).

Table 1 summarizes some of the important dimensions to be considered for the assessment of mHealth solutions.

3. SECURITY AND PRIVACY

Ensuring the confidentiality of health data stored in mHealth solutions with rapidly advancing technology is a fundamental aspect for protecting personal information and privacy and mandatory at the time of Global Data Protection Regulation (GDPR) (3,17,18). A secured design of mHealth solutions will also allow more opportunities for scalability, usability and connectivity (3,17). (Table 2)
Different possible threats and attacks have been identified and include communications, device/services, users, mobility and integration of resources (3). To face these risks, lessons can be learned from other communities such as cybersecurity or internet security which offer various techniques to reduce the potential risk of data breaches or tampering in mHealth (8). Different elements need to be considered:

- Include user-informed consent and privacy/policy information
- Carry out continuous user authentication, to guarantee only allowed device use while protecting authentication data
• Explore a combination of biometric features with privacy-preserving approaches
• Introduce risk assessments protocols and audits of the security system
• Combine multiple private blockchains to provide users with stronger location privacy protection without reducing the quality of service (19)

The evolution of legal frameworks allow also to gain better control of these issues and the recent European GDPR is a good example (20). According to their importance, these aspects could be considered in the criteria for funding. In Belgium, the National Institute for Health and Disability Insurance (INAMI) has introduced a structural framework for funding of digital solutions and including criteria such as the verification of the therapeutic relationship and informed consent, interoperability and data protection (21).

4. CONCLUDING REMARKS

The validation of the scientific validity, analytical performance, clinical performance and security of mHealth solutions is critical to guarantee patient care and safety. To this end, laboratory experts, scientific societies and notified bodies should define and recommend validation framework addressing multiple dimensions. To ensure an efficient and safe use of mHealth solutions, specialists in laboratory medicine and scientific societies must also provide guidance, education, and training to healthcare professionals, patients and helpers.

REFERENCES


