In this issue: POCT – making the point

The Journal of the International Federation of Clinical Chemistry and Laboratory Medicine

eJIFCC

Controlling reliability, interoperability and security of mobile health solutions

Damien Gruson[1,2,3]

[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

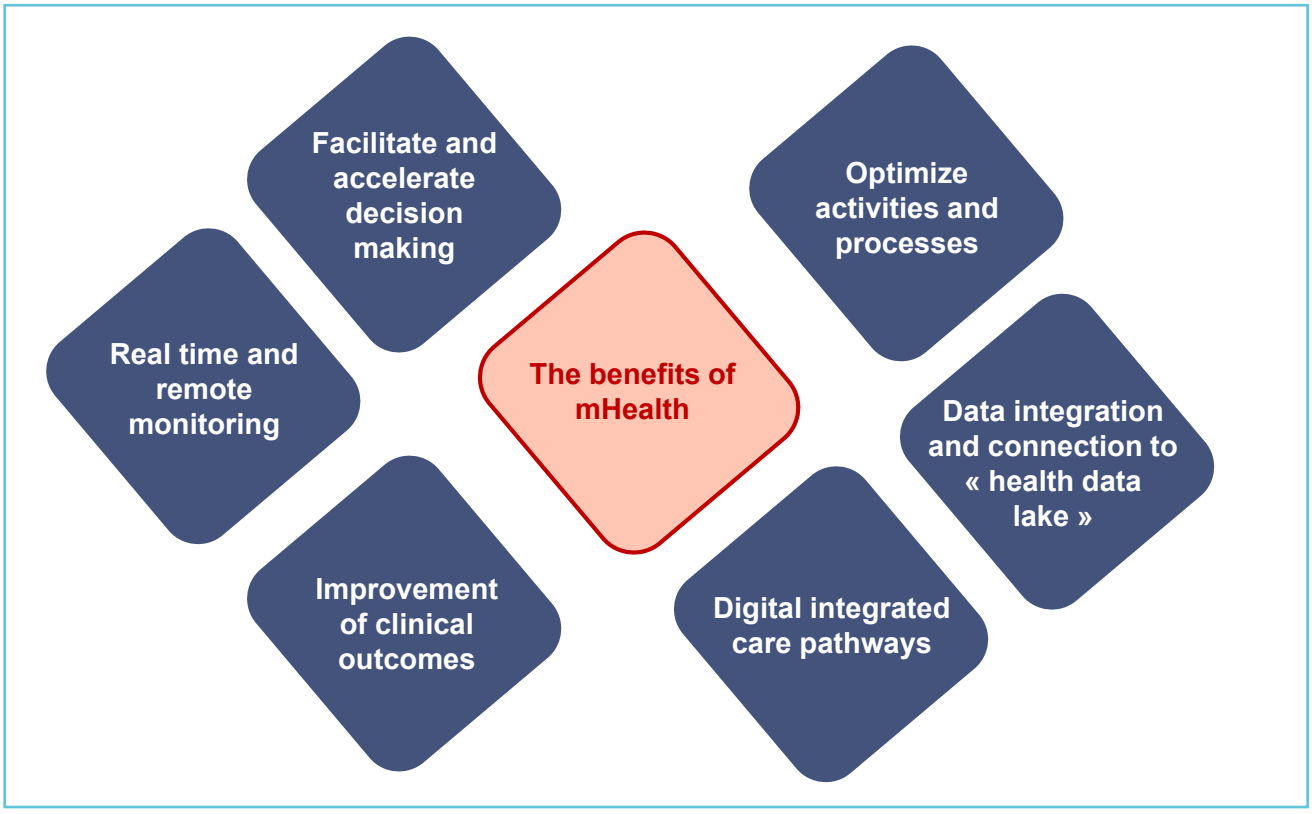
Mobile health (mHealth), including mobile devices and digital services, is a component of the transforming health ecosystem. The validation of the scientific validity, analytical performance, clinical performance and security of mHealth solutions is critical to guarantee patient care and safety. To this 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 introduce 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 possilble 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 assess 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)

Table 1 Multidimensional score card to assess components of mHealth solutions

Dimension evaluated	Potential indicators
Clinical performances and clinical outcomes	Sensitivity, specificity, negative predictive value, positive predictive value, length of stay, mean time between readmission to hospital
Behavioral	Quality-adjusted life year, symptom clusters, patient satisfaction
Technical	Limit of quantification, limit of detection, range of measurement, fault detection systems, connectivity, interoperability, usability
Organizational	Turnaround time of analysis, impact on resources, integration in care pathways
Environmental	Waste and energy consumption, impact on test ordering
Economical	Price, total cost of ownership, time for training, resources needed for implementation and management of solution, cost of management

Table 2 Aspects related to security and privacy

Security	Guarantee of secure storage, secure communication and secure content
Identity management	Ensure authentication for users, devices, applications and associated services
Privacy	Maintain privacy
Scalability	Capacity of evolution to sustainable and scalable solutions
Reliability	Solutions should support identification of fault and self-repairing
Data integration	Real-time data collection, analytics, aggregation and transmission

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 continouous 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

1. Greaves RF, Bernardini S, Ferrari M, Fortina P, Gouget B, Gruson D, et al. Key questions about the future of laboratory medicine in the next decade of the 21st century: A report from the IFCC-Emerging Technologies Division. Clin Chim Acta [Internet]. 2019 Aug [cited 2020 Feb 2];495:570–89. Available from: http://www.ncbi.nlm.nih.gov/pubmed/31145895

2. Gruson D. New Solutions for the Sample Transport and Results Delivery: A Digital Lab. EJIFCC [Internet]. 2018 Nov [cited 2019 May 29];29(3):210–4. Available from: http://www.ncbi.nlm.nih.gov/pubmed/30479606

3. Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S. Security Requirements for the Internet of Things: A Systematic Approach. Sensors [Internet]. 2020 Oct 19 [cited 2021 Mar 29];20(20):5897. Available from: https://www.mdpi.com/1424-8220/20/20/5897

4. Katsikas S, Gkioulos V. Security, Privacy, and Trustworthiness of Sensor Networks and Internet of Things. Sensors [Internet]. 2020 Jul 10 [cited 2021 Mar 29];20(14):3846. Available from: https://www.mdpi.com/1424-8220/20/14/3846

5. Schwamm LH, Estrada J, Erskine A, Licurse A. Virtual care: new models of caring for our patients and workforce. Lancet Digit Heal [Internet]. 2020 Jun 1 [cited 2021 Mar 29];2(6):e282–5. Available from: http://www.ncbi.nlm.nih.gov/pubmed/32382724

6. Bassan S. Data privacy considerations for telehealth consumers amid COVID-19. J Law Biosci [Internet]. 2020 Jul 25 [cited 2021 Mar 29];7(1). Available from: https://academic.oup.com/jlb/article/doi/10.1093/jlb/lsaa075/5905251

7. Yasaka TM, Lehrich BM, Sahyouni R. Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App. JMIR mHealth uHealth [Internet]. 2020 Apr 7 [cited 2021 Mar 29];8(4):e18936. Available from: https://mhealth.jmir.org/2020/4/e18936

8. Arora S, Yttri J, Nilse W. Privacy and Security in Mobile Health (mHealth) Research. Alcohol Res [Internet]. 2014 [cited 2021 Mar 29];36(1):143–51. Available from: http://www.ncbi.nlm.nih.gov/pubmed/26259009

9. Pennestrì F, Banfi G. Value-based healthcare: the role of laboratory medicine. Clin Chem Lab Med [Internet]. 2019 May 27 [cited 2021 Mar 29];57(6):798–801. Available from: https://www.degruyter.com/document/doi/10.1515/cclm-2018-1245/html

10. Getting ready for the new regulations | Public Health [Internet]. [cited 2021 Mar 29]. Available from: https://ec.europa.eu/health/md_newregulations/getting_ready_en

11. Pires IM, Garcia NM, Pombo N, Flórez-Revuelta F, Rodríguez ND. Validation Techniques for Sensor Data in Mobile Health Applications. J Sensors [Internet]. 2016 [cited 2021 Mar 29];2016:1–9. Available from: https://www.hindawi.com/journals/js/2016/2839372/

12. Kanzler CM, Rinderknecht MD, Schwarz A, Lamers I, Gagnon C, Held JPO, et al. A data-driven framework for selecting and validating digital health metrics: use-case in neurological sensorimotor impairments. npj Digit Med [Internet]. 2020 Dec 29 [cited 2021 Mar 29];3(1):80. Available from: http://www.nature.com/articles/s41746-020-0286-7

13. Mathews SC, McShea MJ, Hanley CL, Ravitz A, Labrique AB, Cohen AB. Digital health: a path to validation. npj Digit Med [Internet]. 2019 Dec 13 [cited 2021 Mar 29];2(1):38. Available from: http://www.nature.com/articles/s41746-019-0111-3

14. Objets Connectés | SFIL [Internet]. [cited 2021 Mar 30]. Available from: https://www.sfil.asso.fr/objets-connectes

15. Frederix I, Caiani EG, Dendale P, Anker S, Bax J, Böhm A, et al. ESC e-Cardiology Working Group Position Paper: Overcoming challenges in digital health implementation in cardiovascular medicine. Eur J Prev Cardiol [Internet]. 2019 Jul [cited 2020 Feb 2];26(11):1166–77. Available from: http://www.ncbi.nlm.nih.gov/pubmed/30917695

16. Page not found | ISA2 [Internet]. [cited 2021 Mar 29]. Available from: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf; http://www.ehgi.eu/Download/European_eHealth_Interoperability_Roadmap_%5BCALLIOPE - published by DG INFSO%5D.pdf.

17. Hernández-Álvarez L, de Fuentes JM, González-Manzano L, Hernández Encinas L. Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. Sensors [Internet]. 2020 Dec 25 [cited 2021 Mar 29];21(1):92. Available from: https://www.mdpi.com/1424-8220/21/1/92

18. Galvin HK, DeMuro PR. Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019. Yearb Med Inform [Internet]. 2020 Aug 21 [cited 2021 Mar 29];29(01):032–43. Available from: http://www.thieme-connect.de/DOI/DOI?10.1055/s-0040-1701987

19. Qiu Y, Liu Y, Li X, Chen J. A Novel Location Privacy-Preserving Approach Based on Blockchain. Sensors [Internet]. 2020 Jun 21 [cited 2021 Mar 29];20(12):3519. Available from: https://www.mdpi.com/1424-8220/20/12/3519

20. Gruson D, Helleputte T, Rousseau P, Gruson D. Data science, artificial intelligence, and machine learning: Opportunities for laboratory medicine and the value of positive regulation. Clin Biochem [Internet]. 2019 Jul [cited 2020 Feb 2];69:1–7. Available from: http://www.ncbi.nlm.nih.gov/pubmed/31022391

21. Level 2 of the validation pyramid for health apps is now activated in Belgium | Med Tech Reimbursement Consulting [Internet]. [cited 2021 Apr 4]. Available from: https://mtrconsult.com/news/level-2-validation-pyramid-health-apps-now-activated-belgium