# Challenges in implementing mHealth interventions: a technical perspective

**Varadraj P. Gurupur[1], Thomas T. H. Wan[2]**

[1]Department of Health Management and Informatics, University of Central Florida, Orlando, FL, USA; [2]College of Health and Public Affairs, University of Central Florida, Orlando, FL, USA

*Correspondence to:* Varadraj P. Gurupur. Department of Health Management and Informatics, University of Central Florida, 4364 Scorpius Street, HPA II-210, Orlando, Florida 32816-2205, USA. Email: varadraj.gurupur@ucf.edu.

**Abstract:** Over the years, the healthcare community has witnessed many improvements in methods and technologies used in healthcare delivery, including mHealth as an emerging area of healthcare applications to improve access to health services. However, challenges involved in implementing mHealth to optimal advantage do exist. In this article, we identify some of the most important challenges and propose feasible solutions.

**Keywords:** Challenges to mHealth implementation; usability; mHealth use

Received: 27 May 2017; Accepted: 18 July 2017; Published: 08 August 2017.
doi: 10.21037/mhealth.2017.07.05
**View this article at:** http://dx.doi.org/10.21037/mhealth.2017.07.05

According to World Health Organization (WHO), mHealth has the ability to transform the delivery of health services all over the world and bring about a paradigm shift in healthcare delivery processes (1). This means that improvements in technological innovations can also help improve the clinical and operational processes involved in providing effective and efficient healthcare services (2). However, these changes will not occur smoothly, and many impending changes are to be expected. The barriers will emanate from a myriad of problems including resistance to change in general, existence of unreliable technologies, non-uniformity of technological availability, lack of end-user education, and many other such impediments. In this perspective, we attempt to analyze some of these challenges from the viewpoint of an engineer, who would like to design and implement an mHealth intervention with the intention of enhancing the quality of healthcare delivery processes.

Palazuelos *et al.* (3) detailed a study on the use of mHealth for administering a prescription dosing test using cell phones. The major variables used for this study were acceptability, comfort, preference, and accuracy. Interestingly, a large group of study participants agreed that the mHealth approach had a positive impact on the workflow processes. Some of the study participants expressed concern about the size of the text displayed by the cell phone. They were of the mindset that clear visibility represented in a paper-based system was of much help, while others appreciated the automation provided by the mHealth system. This supports our previous statement that mHealth brings necessary change into the healthcare world while also bringing its own baggage of challenges. An interesting feature of this study was that none of the participants had a college degree. This remarkability is based on the fact that education could be a critical criterion in acceptance of technology in healthcare as observed by Gurupur *et al.* (4).

## Usability

This example of users providing feedback to researchers about design improvements leads us to consider mHealth usability challenges (5,6). These challenges could be as simple as size of the cell phone screen, the font size or type on that screen, color combinations used to display necessary information, or efficacy of an individual to use cell phones for more than phone calls. Here we note that ISO 9241 defines usability as "the effectiveness, efficiency and satisfaction with which a specified user can achieve the specified goals of a

particular environment". Nielson (7) identified the following main components of usability: (I) learnability; (II) efficiency; (III) memorability; (IV) low error rate, and (V) satisfaction. Shneiderman (8) identifies the following as key usability attributes: (I) time to learn; (II) satisfaction; (III) time taken to recover from errors, and (IV) speed of performance. Shneiderman (8) also points at technology variety, user diversity, and bridging the gaps in user knowledge as key components of universal usability. Karvonen (9) explains the "beauty of simplicity" by pointing out that one of the key factors towards a user-centered design would be to keep it simple. For example, if a user has to browse through ten different hyperlinks to explore important information that is three links deep, the design may not be considered user-centric. Information that is necessary for the user must be readily available without requiring too much effort. Therefore, adopting the principle of simplicity is essential for mHealth applications, and this is a critical challenge that needs to be overcome.

Karvonen (9) also mentions the "trust factor" associated with simplicity. She argues that simplicity also leads to users trusting the application to be authentic. This trust factor, described by Karvonen (9), can be perceived by the following statement from the user: "*If it looks pleasant, I just trust it*." Alternatively, websites with flying banners and flashy statements many times reduce our perception of trustworthiness of the site's information. This is very true for mHealth applications. Therefore, designers of mHealth systems and applications must take into consideration the challenge of trustworthiness, which sometimes can be accomplished by establishing "authenticity through simplicity".

While improving usability and user-centered design is an important aspect of system development that fully applies to mHealth, there exist more technically intense challenges in implementing mHealth. Some of these challenges could be interoperability and data security, which include more stringent terms such as confidentiality and integrity. Gurupur *et al.* (10) explained the complexity of healthcare decision support, which applies to mHealth intervention design as well. This complexity is compounded with the challenge of integrating smaller information systems to build larger healthcare information systems, some of which may not have been originally designed and developed for healthcare purposes. Therefore, integrating these systems will be like an elephant in the room to tackle.

Many researchers have dealt with the issue of integrating smaller healthcare systems (10). Health Level Seven (HL7), under the leadership of Kawamoto (11), has been working extensively to develop standards for clinical decision support systems using JSON. JSON is a Java based language used to develop generic constructs to ensure interoperability between health care systems. These standards could be used to guide development of mHealth applications and networks as well.

## Interoperability and integration of technologies used

Considering this myriad of issues, we begin with challenges associated with data security. The Health Insurance Portability and Accountability Act (HIPAA) passed by the United States Congress in 1996 "legalized" data security in health care, thereby legalizing and legitimizing additional aspects associated with data privacy. This segued to healthcare providers employing individual consultants and vendor organizations to ensure compliance with HIPAA regulations (12) for policy guidance and business solutions for data storage, access, retrieval and other necessary information management functions. When data are stored on an appropriate data-storing device and accessed through a wired network, ensuring data security is somewhat simple compared to dealing with it in a situation when data are transmitted across multiple devices and storage options using a wireless medium.

The National Institute of Standards and Technology (NIST) defines the process of de-identifying healthcare data as "*a process that is applied to a dataset with the goal of preventing or limiting informational risks to individuals, protected groups, and establishments, while still allowing for the production of aggregate statistics*" (13). By definition, mHealth uses healthcare data transmitted through wireless networks, and often the data may not be de-identified. This situation presents numerous complex challenges associated with data security. Bennett *et al.* (14) identified three aspects of security for electronic transmission of health records: (I) methodological; (II) technical, and (III) procedural. Here the methodological aspect pertains to: (I) application/intervention design; (II) technology, and (III) data collection and management, while the technical aspect pertains to: (I) software dependencies; (II) user input validation; (III) software design; (IV) software implementation, and (V) deployment of networks and servers. Finally, the procedural aspects cover: (I) data handling mechanism and protocols; (II) staff training, and (III) monitoring and revision of protocols.

## Data security and privacy

When considering methodological aspects such as managing passwords, training users on technology, and managing data that contains personal health information (PHI), it is important to consider the critical need of training users. Many times, ill-trained users find it very difficult to deal with technology, which may bring negative outcomes that might be magnified in a healthcare setting. This is very true when it comes to mHealth use. Another problem associated with methodology is the use of unsecured wireless networks to transmit protected information. For example, if physicians and nurses frequent a coffee shop next to the hospital, some of them may want to access health records on their personal devices using the shop's non-secure wireless network. This situation may help a cyber-criminal get access to personal health records, a threat to the privacy and security of an individual's data.

While this aforementioned example deals with a situation of data access, we also have to consider another problem pertaining to data storage. Cloud computing and application service providers are increasing in popularity as a business solution, even among healthcare organizations. However, there is an inherent problem with cloud computing—unknown locations of data storage. While some may argue that cloud computing poses increased security threat for data transmission, data may also be at risk from storage in a non-secure location. Stakeholders of mHealth implementation must consider this critical aspect of data storage when making business decisions that affect data governance. The general rule is to have patient data stored in secured server rooms with access limited to authorized individuals. However, if healthcare information vendors use cloud computing as part of their business model, the obscurity associated with the storage location of data can sometimes lead to violation of HIPAA privacy rules. Another important and critical feature associated with this data storage mechanism is backing up required data, i.e., redundant data storage in case of primary data loss. There are information system vendors that specialize in backing up healthcare data. However, if individual healthcare organizations decide to back up data on their own, they would need the technology and the expertise required to do it securely.

## Reliability

Above all, we consider the greatest challenge in implementing mHealth to be those associated with synchronizing mobile devices, and with synchronizing mobile devices with non-mobile devices. This assessment is based on awareness that these devices may be (and likely are) using different operating environments, different data formats, and many other disparities that may be less evident.

Reliability can be considered from a purely technical perspective—whether a device or app works when you want it to. One relevant factor in this technical assessment is availability of network connectivity. For example, Pearl River County in Mississippi is devoid of network connectivity when compared to Orange County in Florida. The same app or device will function quite differently in each place. A discussion on these topics may lead to ideas on using improved network technology and devices to implement mHealth applications.

A second element of reliability is the value of the content programmed in an app. Scher (15) reports that many readily available low-cost apps are not based on evidence from research. Such apps may provide incorrect information, which users presume to be correct. Unreliability in this instance is more evident when the application has not been reviewed and approved by a regulatory organization like the US Food and Drug Administration (FDA).

## Conclusions

We summarize the major categories of mHealth challenges in *Table 1*, identifying the key components to address, and explaining the components in user language. Overall, we identified five major areas of technical challenges in implementing mHealth: (I) usability; (II) system integration; (III) data security and privacy; (IV) network access, and (V) reliability. We illustrated some of the important concepts associated with these challenges. To conclude, mHealth is definitely a much-needed boon for improving the healthcare delivery process. However, these challenges call for a focus on areas in need of change. Some of the feasible solutions for these challenges would include: (I) identification of storage locations when cloud computing is in use; (II) usability analysis of mHealth applications and improvements made based on this usability analysis; (III) considering HL7 standards for interoperability, and (IV) reliability analysis of mHealth applications before use. It will be interesting to observe how some of these challenges will be resolved in the years to come.

**Table 1** Categories of mHealth challenges

| Challenge | Key components | User definition |
|---|---|---|
| Usability | User interface design | Keeping the user interface simple, using the right font type and size, and improving user satisfaction |
| | Trust worthy design | The user interface design must be simple enough to be trust worthy |
| | Learnability | The mobile application must be easy to learn |
| System integration | Interoperability | Must be able to exchange required information with systems developed by other vendors |
| | System design | The associated system design must be scalable and allow integration with other systems |
| Data security and privacy | Confidentiality | Confidentiality of patient data to ensure HIPAA compliance |
| | Data storage | Data must be stored in a secure location |
| | Data access | Data must be accessed through secure transmission channels |
| Network access | Availability | Availability of wireless networks |
| | Speed and strength | The available wireless network must be strong enough to transmit and receive data |
| Reliability | Accuracy of the result | The result provided must be accurate enough to help the patient |
| | FDA approval | FDA approval is required for clinical use in United States |

HIPAA, Health Insurance Portability and Accountability Act; FDA, Food and Drug Administration.

## Acknowledgements

None.

## Footnote

*Conflicts of Interest*: The authors have no conflicts of interest to declare.

## References

1. World Health Organization. mHealth: New horizons for health through mobile technologies. Available online: http://www.who.int/goe/publications/goe_mhealth_web.pdf
2. Malvey D, Slovensky DJ. mHealth: Transforming Healthcare. New York, NY: Springer, 2014.
3. Palazuelos D, Diallo AB, Palazuelos L, et al. User Perceptions of an mHealth Medicine Dosing Tool for Community Health Workers. JMIR Mhealth Uhealth 2013;1:e2.
4. Gurupur V, Shettian K, Xu P, et al. Identifying the readiness of patients in implementing telemedicine in northern Louisiana for an oncology practice. Health Informatics J 2016. [Epub ahead of print].
5. Kamana M. Investigating usability issues of mHealth apps for elderly people. 2016. Available online: https://www.diva-portal.org/smash/get/diva2:913110/FULLTEXT02.pdf
6. Novak G. Developing a usability method for assessment of M-Commerce systems: a case study at Ericsson. Available online: https://pdfs.semanticscholar.org/b5cb/51f336f3c36873407bc854cd1d3091a37430.pdf?_ga=2.6298033.2093334166.1499200956-1141212521.1499200956
7. Nielsen J. Usability Engineering. San Diego, CA: Morgan Kaufmann, 1993.
8. Shneiderman B. Universal usability. Communications of the ACM 2000;43:84-91.
9. Karvonen K. The beauty of simplicity. Proceedings of the 2000 conference on universal usability. Arlington, Virginia, USA, 2000 Nov 16–17:85-90.
10. Gurupur V, Gutierrez R. Designing the Right Framework for Healthcare Decision Support. J Integr Design and Process Sci 2016;20:7-32.
11. Kawamoto K, Honey A, Rubin K. The HL7-OMG Healthcare Services Specification Project: motivation, methodology, and deliverables for enabling a semantically interoperable service-oriented architecture for healthcare. J Am Med Inform Assoc 2009;16:874-81.
12. Arora S, Yttri J, Nilse W. Privacy and Security in Mobile Health (mHealth) Research. Alcohol Res 2014;36:143-51.
13. National Committee on Vital and Health Statistics (NCVHS). 2017. Available online: https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf

 

14. Bennett K, Bennett AJ, Griffiths KM. Security Considerations for E-Mental Health Interventions. J Med Internet Res 2010;12:e61.
15. Scher DL. The Big Problem with Mobile Health Apps. Medscape 2015. Available online: http://www.medscape.com/viewarticle/840335

doi: 10.21037/mhealth.2017.07.05
**Cite this article as:** Gurupur VP, Wan TT. Challenges in implementing mHealth interventions: a technical perspective. mHealth 2017.

 