Using Online Social Media Platforms for Ubiquitous, Personal Health Monitoring

Chonlatee Khorakhun
University of St Andrews, UK
ck46@st-andrews.ac.uk

Saleem N. Bhatti
University of St Andrews, UK
saleem@st-andrews.ac.uk

***Abstract*—We propose the use of an open and publicly accessible online social media platform (OSMP) as a key component for ubiquitous and personal remote health monitoring. Remote monitoring is an essential part of future mHealth systems for the delivery of personal healthcare allowing the collection of personal bio-data outside clinical environments. Previous mHealth projects focused on building private and custom platforms using closed architectures, which have a high cost for implementation, take a long time to develop, and may provide limited access and usability. By exploiting existing and publicly accessible infrastructure using an OSMP, initial costs can be reduced, at the same time as allowing fast and flexible application development at scale, whilst presenting users with interfaces and interactions that they are familiar with. We survey and discuss suitability of OSMPs in terms of functionality, performance and the key challenge in ensuring appropriate levels of security and privacy.**

I. Introduction

An essential part of the mHealth ecosystem is the availability of patient-generated, biological data (bio-data), e.g. heart-rate, blood-pressure and other vital signs. Priorities in global healthcare are shifting towards goals such as: prevention and early detection; routine monitoring for diagnosis; and treatment of chronic conditions. This latter issue is also important globally: the healthcare needs of the global population are changing, as improved healthcare regimes drive a shift of resources from dealing with acute conditions and communicable diseases towards management of chronic illnesses, as a result of an ageing population [1].

With the use of an online social media platform (OSMP) for remote monitoring outside the clinical environment, patients and healthcare professionals can be presented with familiar interfaces, while application developers can work with a set of technologies that are widely used and well-known. Internet-based access also helps to provide wide-ranging connectivity for mobile health applications at scale. Health service providers benefit from reduced costs by exploiting the scale of existing infrastructure, open technologies, and existing expertise in application and systems development. Based on existing social interactions, an OSMP enables the formation of a *carer network*, working in harmony with, and providing support for, existing relationships and interactions between patients and healthcare professionals.

A. The carer network

We focus on the use of an OSMP to enable two primitive functions on which larger personal healthcare services could be built: *remote health monitoring* of personal bio-data, and an *alert system* for asynchronous notifications. The use of an OSMP provides a structure to enable a collaboration between patients and healthcare professionals in a *carer network*, supporting the interactions and relationships that exist in healthcare systems today. The communication between patients and healthcare professionals in a healthcare regime today is mainly limited to clinical visits, letters and perhaps phone calls. The OSMP has the potential to improve this interaction and so improve the overall quality of healthcare, while reducing costs. Additionally, by use of the OSMP, the healthcare regime can be inclusive of both formal caregivers (e.g. doctors) and informal caregivers (e.g. family).

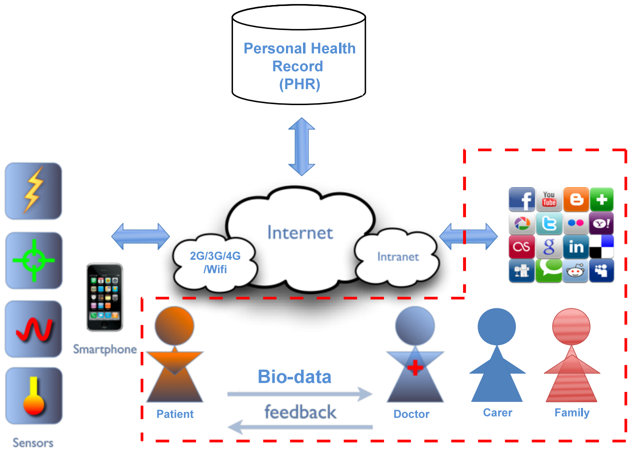

Fig. 1: A remote monitoring application (RMA) using an OSMP to form a *carer-network*. OSMP enables communication and colloboration in a *carer-network* as well as provides a portal to access the collected bio-data and to generage a message alert for an emergency situation.

As shown in Figure 1, our model of a carer network, which is based on a healthcare regime that is common worldwide [2], consists of four actors:

1) the *doctor* in charge of the management of the healthcare regime;
2) the professional *carer* implementing the clinical care;
3) a *family* member or friend who is concerned about the patient (e.g. a neighbour for an elderly patient);
4) and the *patient*.

B. Scenario and contribution

Figure 1 shows a general scenario for the monitoring of a patient, which we have previously examined, including a prototype remote monitoring system [3], [4]. Personal bio-data is collected from a patient, sent to a server and may need to be accessed by several actors who are remote. The dashed (red) outline indicates our use of an OSMP as a portal to access to the collected health data within our scenario.

We will later examine three OSMP systems in order to assess the suitability of OSMPs for remote monitoring. We have previously reported on examples using the Facebook application programming interface (API) to assess the utility of OSMPs for implementing two *primitive functions*:

1) Remote monitoring of personal bio-data [3].
2) Generation of asynchronous alerts [4].

Our examples [3], [4] used Facebook for convenience, in order to investigate the issues in the use of an OSMP:we would not expect a real healthcare OSMP to be on Facebook.

After describing requirements and challenges in mHealth systems in Section II, we survey examples of remote monitoring systems in Section III. Based on our experience from application development example written using Facebook for remote monitoring and remote alerts, we compare Facebook with two other OSMPs in Section IV. We summarise and conclude our discussion in Section V.

II. Requirements and Challenges in mHealth

We place in context our examination of the use of OSMPs for supporting mHealth. Three key challenges for eHealth/mHealth are the development and evaluation of suitable applications at *scale* given *cost constraints*, whilst ensuring appropriate provision of *security and privacy* for users.

A. Creating mHealth applications at scale

A key focus of eHealth systems has been on large scale access to information contained in a person's individual Electronic Health Record (EHR) or Personal Health Record (PHR). GoogleHealth [5] and Microsoft HealthVault [6] are two examples of cloud-based, third-party PHR platforms, which could offer services for users to collect, store and manage their own health data. However, developing PHR infrastructure is a challenge in itself, and at the start of 2013, the GoogleHealth service was shut down.

A study by Free et al [7] shows a lack of evidence on the effectiveness of mHealth but suggest this may be due to inadequate evaluation studies of mHealth applications. According to a survey from the World Health organisation (WHO) [8], the dominant form of mHealth system today is in small-scale pilot projects, whereas larger mHealth implementations are still limited. mHealth, by its nature, consists of a highly-distributed set of resources that have to be orchestrated, and from which potentially large flows of data have to be collected and organised at scale.

This creates a significant challenge for applications development in mHealth. A report from the mHealth Alliance in 2010 [9] states that a key barrier to implementing mHealth is the lack of the ability to assess its impact on health outcomes and cost effectiveness. It is clear that large scale implementations for mHealth are needed to mature, to enable better evaluation of such systems.

B. System development and implementation cost constraints

Reports from the UN [10], WHO [8] and the mHealth Alliance [9] have listed the barriers, challenges and needs for mHealth development and implementation. The most important barrier in mHealth development is funding. The cost required to deploy and maintain new eHealth/mHealth systems should therefore be minimal. Also, there is no proof of success for mHealth systems, i.e. lack of a large system evaluation and unknown cost effectiveness and cost-benefit studies. This is because a larger deployment, which is needed to assess real benefits, can be expensive. Additionally, there is difficulty in creating rapid, staged evaluations to assess the early effects of new applications. Accordingly, the use of the simplest available technology could solve the problem and provide a proof of concept cheaply and quickly. Precise and accurate requirements analysis can be difficult, and therefore, the development must be able to change quickly to meet the new requirements, i.e. agile development.

There is still a lack of collaboration for software development between mHealth organisations. A standardised platform and open architecture would be a key enabler for reducing costs, as in other IT applications. Employing existing infrastructure which is open, publicly accessible to users and developers, has low costs to enter the market, and is conformant to well-known, widely-deployed standards (e.g. WWW standards), could yield great benefits.

So, an OSMP has great potential to help ameliorate the problems faced by mHealth implementation and deployment. However, most of the previous mHealth studies have been based on private, small and closed architectures. This might in part be related to commercial incentives and market sensitivities, as the worldwide mHealth market is potentially huge.

C. Security and privacy

The study by Avancha et al [11] from 2012 has defined a set of privacy properties that are required in mHealth systems. In summary, patients need to have a control over the collection, dissemination and access to their mHealth data even if the data is owned by another party, e.g. patient's medical record maintained by a hospital. The study is based on analysis of national requirements and laws. The emphasis is on the controls that should be made available for user control for legal compliance. This means that patients must be able to monitor their own health information, i.e. the location of their health information and which parties and/or organisations have access to it. A study by Prasad et al [12], also from 2012, proposes that a highly granular control is required in sharing of health information. This means detailed, and perhaps subtle, application of access control rules to health data, i.e. who can access the data and in which context, must be enabled. So, developers and users may have to deal with a complex set of security and privacy issues.

In remote health monitoring systems today, users collect their own personal bio-data, as well as information about their physical and social activity, for upload to a vendor website, social networking website, a PHR, or a health-provider-operated EHR. Once the data is uploaded, users must be able to choose with whom they can share which part of the information, e.g. with healthcare providers to diagnose and monitor their treatment, and/or with family and friends providing informal care and support. So, the portal must enable users to share health information with people involved in their healthcare.

III. Remote monitoring systems today

Table I shows the comparison of attributes we consider important in remote monitoring systems between four remote monitoring systems selected for this study. Note that the table summarises what users want to see and we do not perform a system-level analysis. More details on other remote monitoring systems can be found in [13].

eCAALYX [14] [15] is an EU-funded project to develop a remote monitoring system for elderly patients with multiple chronic conditions. The system uses a smartphone as an interface to collect data from patient-wearable health sensors and connect to a remote server over the Internet. Healthcare professionals who are in charge of the remote monitoring and healthcare of the elderly patient access the remote server via the Internet also.

Personal Care Connect (PCC) [16] proposes a remote monitoring solution for home monitoring of patients with chronic diseases. Unlike most remote monitoring systems, PCC is a standards-based open platform (with an open API). This means the system can integrate with any sensor devices and any remote applications. Unlike other third party solutions, PCC has an open and extensible architecture.

Alarm-net [17] is an assisted-living system to monitor environmental and physiological data of people in residences. The system has privacy policies which will be checked and enforced for each authorised user. This privacy configuration rules are dynamic and can be changed on based on context.

Alert portable telemedical monitor (AMON) [18] is a remote monitoring system which encapsulates various sensors into one wrist-worn device that is connected to a telemedicine centre via the GSM network. The system is designed to support three types of communication, i.e. SMS, virtual circuit switching and IP Internet-based channels.

From Table I, we can see that alert provision and autonomy of operation are two key attributes required in remote monitoring systems: the system must be autonomous and seamless in raising alerts. For data collection, the use of smartphones for active patients is preferred over the use of proprietary or custom devices. Using portable, generic and easily-available devices would reduce cost and increase accessibility and usability. To enable ubiquitous and seamless monitoring, communication over an IP network and the Internet is also highly desirable. However, to employ an additional communication channel which is already included in the core functionality of mobile phones, such as short message service (SMS), as an optional means to enhance reliability, is also advantageous. Furthermore, the application platform used for data access should be accessible across different devices, e.g. it is possible to access the patient data via a handheld device such as a smartphone, or via a personal computer (PC). So, an open platform with open APIs and SDKs would enable interoperability and extensibility, i.e. the application can work with any devices and medical systems. Last but not least, it is vital to have control over security and privacy for the patient.

Surprisingly, security and privacy features appear to have varying levels of priority. Particularly, the levels of control for security and privacy configuration and manageability of privacy policies varies greatly. From Table I, eCAALYX, PCC, and AMON have existing security and privacy mechansisms. However, they are not user-configurable, and the configuration is fixed. Users in Alarm-net can configure their own privacy rules. Nevertheless, the privacy policies are still controlled by the system administrators and not by users.

Unlike the research projects listed above, real-world mHealth pilot studies, as examined in a 2009 study [10], still lack many of the attributes mentioned above. Many other example projects, such as Cell-life [21], CADA [20], Curioso et al [22], Fleishman et al [23] and Medinet [19], do not support autonomous operation or ubiquitous monitoring.

IV. Comparing OSMPs

We compare three existing OSMPs with respect to the attributes in Table I:

- Facebook: a widely used platform, with a public API.
- Google+: a relatively new competitor to Facebook, so it is instructive to see what a different service provider considers to be important for an OSMP offering.
- Diaspora[1]: a completely open source OSMP toolkit, allowing use to test our stated position that a completely open OSMP would have benefits.

Note that none of these OSMPs are designed specifically for eHealth/mHealth, and that while Facebook and Google+ offer APIs, they are not open platforms.

A. Facebook

Facebook provides mutual relationships and rich social channel constructs, with a range of possibilities for communication between users, as well as privacy settings to control who can see any messages. Facebook provides functionality to connect users as a *group* or a *list*. Based on an open graph mechanism, a relationship between users is enabled, e.g. patients can have lists of people who are their doctors. Also, carers and family members can be grouped by Facebook for communication within a carer network. There are three relevant methods for messages in Facebook:

- *Post to a user's timeline or to friend's news feed:* A user's 'status update' is made visible to friends or made public, and an API could enable an automatic post. However, if users create an incorrect privacy setting, the information

[1] https://diasporafoundation.org

TABLE I: Comparison of existing remote monitoring systems

Features	eCAALYX [14] [15]	PCC [16]	Alarm-net [17]	AMON [18]	Medinet [19]	CADA [20]	Cell-life [21]
Data collection	Smartphone	Smartphone	Emplaced sensors	Wrist-worn device	Smartphone	Smartphone	Smartphone
Data communication	GPRS	GPRS	IP network	SMS/VC/IP	GPRS	N/A	SMS
Data access platform	Web interface	Web interface	IBM websphere	PC server	Mobile app	Mobile app	Web interface
Software development	N/A	Open API	N/A	N/A	N/A	N/A	N/A
Alert system	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Autonomous operation	Yes	Yes	Yes	Yes	No	No	No
User policy definition	No	No	No	No	No	No	No
User configuration of security and privacy	No	No	Yes	No	No	No	No
Group-based access control	No	No	Yes	No	No	No	No
Data archiving	No	Yes	No	Yes	Yes	No	No
Data download	No	No	No	No	No	No	No
Data portability	No	No	No	No	No	No	No
Data deletion	No	No	No	No	No	No	No

TABLE II: Comparison of OSMP features

Features	Facebook	Google+	Diaspora
Colloboration in carer network	Grouping post/Messaging	Communities/Hangouts	Only messaging (no group/no chat)
Connected services	Apps to connect (e.g. Twitter)	No	Facebook/Twitter/Tumblr
Notifications	Email/SMS/In-browser	Email/SMS/In-browser	Email/In-browser
Mobile devices	Android/iOS/Web	Android/iOS/Web/SMS	Web only
Software	Open API	Open API	Open source
Alert	Yes	Yes	Yes
Autonomous operation	Yes (with user authentication)	Yes (with user/admin authentication)	Possible
User policy definition	No	No	Yes
User configuration of security and privacy	Yes	Yes	Yes
Group-based access control	Yes	Yes	Yes
Data archiving	No	Yes	Possible
Data download	No	Yes	Possible
Data portability	No	No	No
Data deletion	Yes	Yes	Yes

could be either exposed to the whole network or may not go to the correct people.

- *Send a message:* A message is sent directly and privately from a user to others. However, it is not possible to automate the message sending – user interaction is required.
- *Notifications:* Users can send a short, custom message. Only selected receivers can see the notification pop up when they log in, so the information is kept private. In addition, an automated process for sending a notification is possible. However, some user interactions are still required at the beginning of the process to grant permissions. This method is best suited for sending alerts for health monitoring application.

Facebook offers the following relevant features:

- *Relationships.* A Facebook *group* or *list* can allow the formation of the carer network. Facebook also supports communities and friends across the groups and lists.
- *Communication channels.* Facebook supports access control, e.g. *post to news feed* can be sent to a specific users individual timeline. A *direct message* is possible in Facebook as well as notifications.
- *Automation.* Automatic processes for generating alerts are possible in Facebook. Facebook has no limitation on the number of messages that can be sent. Automation of notification generation is possible in Facebook, but user interaction is still required at the beginning of the process.
- *Mobile.* Facebook supports apps for iOS, Android and has a mobile mobile web interface, but SMS is deprecated.
- *Security and privacy.* The privacy, security and access control mechanisms must remain under the control of the carer network, but in the Facebook platform, the policies are controlled by Facebook and could change arbitrarily. Also configuring security and privacy features is complex, and so erroneous configuration is possible.
- *Link to other platforms.* Facebook offers a deprecated API for SMS services. Nevertheless, most OSMPs provide links to connect to Facebook, e.g. Twitter. Such links may permit increased reliability of message delivery via additional means of communication.

B. Google+

Google+ is a more recently-deployed online social network offering, but is gaining popularity, in part due to its integration with other Google services. The platform provides much useful functionality for a carer network:

- *Circles.* Similar to a Facebook list, a circle selects a group of people that a user wants to share information with.
- *Relationship.* A circle is a one-way relationship. Adding a user to your circle means you ‘follow’ them, but they may or may not choose to ‘follow’ you.

- *Communities.* Comparable with a group in Facebook, a community enables communication between people with similar interests.
- *Hangouts.* Combines a grouping mechanism with chat and messaging functionality, with no direct equivalent in Facebook, though Facebook does support messaging and chats. Hangouts allow people to send messages, photos and use video calls and conferencing. It could enable private conversations for people in a circle, e.g. enabling a live-meeting in carer networks.
- *Mobile.* Google+ supports mobile devices, i.e. iOS app and Android app, including mobile web and SMS.
- *Security and privacy.* Users have no control over security policy. Configuration of security and privacy is simplified by the use of circles (groups), but adding a user to a circle does not require that user's consent. Also, there is no 'exclude' option to eliminate users or groups from specific information unless a new circle is formed. That is, Google+ seems to have only 'allow' access, but not 'deny' access, and a specific post or message is associated with the users/groups that are 'allowed'.
- *Link to other platforms.* Unlike Facebook, Google+ lacks linkage for third-party apps. This has made it impossible to synchronise information from Google+ across other OSMPs, such as Facebook and Twitter. Since the Google+ API is still read only, automatic post or reshare from Google+ is not possible.
- *Google+ Domains API.* This is an enhanced Google+ API. It can be used as a tool for organisation and management, e.g. it is possible to send automatic posts, start Hangouts with specific teams, or manage circle membership within the same domain. The API supports not only reading, but also writing posts with a possibility that authentication can be granted from the domain administrator on behalf of all users.

C. Diaspora

Diaspora is a privacy-aware and decentralized OSMP. Diaspora servers are administrated by individual users or organisations, allowing users to stay in control of their data. Unlike Facebook and Google+, user-generated data is not stored at a central server or owned by a single entity who administers the site. Diaspora users decide on which servers their information will be stored. As Diaspora is an open source OSMP toolkit, it is possible for users to maintain their own Diaspora servers to keep complete control of their data.

The decentralised and cooperative nature of Diaspora would allow individual health service providers to create OSMP-based services, but allow sharing of data for the benefit of the patient, under appropriate policy, security and privacy constraints. Disapora offers the following relevant functionality:

- *Aspects.* Based on the same concept as circles in Google+, an aspect is a selected group of people who can see your post. It is a follow system closely resembling Twitter. People can chose to share with a selection of aspects or share with the world. Mutual relationships are needed for a communication in a carer network.
- *Relationship.* Diaspora is similar to Twitter and Google+, i.e. having asymmetric sharing relationship, dynamic sharing, and permitting 'following' of users.
- *Communities and grouping.* Diaspora does not yet implement a general group functionality. Currently, it is only available on the Diaspora Canada pod.
- *Conversations.* A conversation is a private message stream, shared with one or multiple followers. However, conversations only work with mutual followers.
- *Notifications.* Users receive notifications for a post, comment or start sharing. Like Google+, there are no third-party apps available as yet, or a full intra-OSMP application development platform. Therefore, the notification mechanism used in our Facebook RMA for sending alerts would need to be implemented as a new function, rather than leveraging an API to an existing function.
- *Mobile.* There are no mobile apps for iOS and Android apps are somewhat out of date, at the time of writing. Currently the best way to access diaspora from mobile device is through a browser with a mobile version which should work well on all devices. However, as we have stated above, with appropriate use of responsive web-design this is not necessarily a disadvantage, and may reduce an overhead of keeping a separate set of apps updated, but potentially at the cost of usability on a mobile platform.
- *Security and privacy.* The use of an open source OSMP, such as Diaspora, would enable customised functionality and customised security and privacy. A real mHealth system built from such an OSMP could be administered by a health service provider, improving the security and privacy aspects for collection of the bio-data.
- *Cross-posting* Diaspora allows you to easily share your messages with Facebook, Twitter and Tumblr.

D. Comparison of platforms

OSMPs provide basic security and privacy mechanisms for access control of collected health data, but a real deployment would need to improve on what is currently available. To enable appropriate control over security and privacy, we propose the use of a fully open platform to enable a health provider to introduce appropriate policy and mechanisms, based on local policy, national laws and user requirements, and reduce the risk of lock-in to business models specific to third parties. An open source OSMP, such as Diaspora, can provide maximum flexibility for connectivity, as well as allowing enhanced application capability and customised security and privacy controls.

As a summary, we could generalise our findings with these three key points:

1) Facebook has a well-developed API, and supports directly the creation of full applications within the OSMP. However, security and privacy *policy* is not under user-control, even though *configuration* of security and privacy is under user control.

2) Google+ potentially has better support for developing and administering mHealth with its Domain API, e.g. with hangouts. However, it does not allow the development of full applications, lacks linkage with other OSMPs and suffers the same security and privacy *policy* drawback as for Facebook.
3) Diaspora does not have a rich set of functions for social interactions as either Facebook or Google+, but its open source nature means that missing functionality could be imported and/or built and integrated as required using open standards and technologies. Its emphasis on users retaining ownership of their data, as well the security and privacy *policy* for services, means that it has a key feature that Facebook and Google+ do not.

V. Conclusion

We have examined the suitability of the use of an online social media platform (OSMP) in support of remote monitoring for eHealth/mHealth. From our analysis, we see that the use of an OSMP has the following benefits:

- *Exploiting existing social relationships.* Our *carer network* is a natural social network within a healthcare environment, and similar relationships exist in health systems worldwide. The use of an OSMP allows us to implement communication between actors within a carer network, and includes the *patient*, the *doctor* in charge of the health regime, professional *carers*, as well as concerned *family* members or friends.
- *Remote monitoring.* The features and functionality available in existing OSMP platforms provide many useful features for use in an mHealth scenario. Grouping mechanisms and social communication channels of various sorts allow a rich set of relationships and information viewpoints to be implemented.
- *Alerts.* The OSMP allows the provision of alerts to be delivered using the asynchronous notification mechanisms that exist in many OSMP platforms.
- *Security & privacy.* We find that OSMPs offer many useful functions, but no single OSMP currently offers natively the correct security and privacy primitives required for mHealth. However, an open source OSMP platform could provide such capability, in manner that can be adapted for local, national and user requirements.

We take the position that the use of an open source OSMP platform would allow flexible application development and modifications, reduce the costs of systems, and allow fine-grained control of security & privacy for a future mHealth system. We believe that the use of OSMPs would enable the collection of patient-generated data for personal and ubiquitous healthcare in a future mHealth scenario, exploiting existing infrastructure to reduce costs, improve application development and allow scalability of solutions.

References

[1] L. M. Gutiérrez-Robledo, "Looking at the future of geriatric care in developing countries," *The Journals of Gerontology Series A: Biological Sciences and Medical Sciences*, vol. 57, no. 3, pp. M162–M167, 2002.

[2] N. Carpentier and F. Ducharme, "Care-giver network transformations: the need for an integrated perspective," *Ageing and Society*, vol. 23, no. 04, pp. 507–525, 2003.

[3] C. Khorakhun and S. N. Bhatti, "Remote Health Monitoring Using Online Social Media Systems," in *Proc. 6th IFIP/IEEE Wireless and Mobile Networking Conference (WMNC2013)*, Apr 2013.

[4] ——, "Alerts for Remote Health Monitoring Using Online Social Media Platforms," in *15th IEEE Intl. Conf. on e-Health Networking Applications and Services (HealthCom)*, Oct 2013.

[5] Google, "GoogleHealth," http://www.google.com/intl/en_us/health/about/, (Apr 2014).

[6] Microsoft, "Microsoft HealthVault," https://www.healthvault.com/gb/en, (Apr 2014).

[7] C. Free, G. Phillips, L. Watson, L. Galli, L. Felix, P. Edwards, V. Patel, and A. Haines, "The effectiveness of mobile-health technologies to improve health care service delivery processes: a systematic review and meta-analysis," *PLoS medicine*, vol. 10, no. 1, p. e1001363, 2013.

[8] M. Kay, "mHealth: New horizons for health through mobile technologies," *World Health Organization*, 2011.

[9] P. Mechael, H. Batavia, N. Kaonga, S. Searle, A. Kwan, A. Goldberger, L. Fu, and J. Ossman, *Barriers and gaps affecting mHealth in low and middle income countries: Policy white paper*. Columbia University. Earth Institute. Center for Global Health and Economic Development (CGHED): with mHealth Alliance, 2010.

[10] V. W. Consulting, *mHealth for development: the opportunity of mobile technology for healthcare in the developing world*. UN Foundation-Vodafone Foundation Partnership, 2009.

[11] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 3, 2012.

[12] A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz, "Understanding sharing preferences and behavior for mHealth devices," in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 2012, pp. 117–128.

[13] A. D. Jurik and A. C. Weaver, "Remote medical monitoring," *Computer*, vol. 41, no. 4, pp. 96–99, 2008.

[14] M. Boulos, S. Wheeler, C. Tavares, and R. Jones, "How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX," *Biomedical engineering online*, vol. 10, no. 1, p. 24, 2011.

[15] A. Rodrigues, C. Resende, L. Carvalho, P. Saleiro, and F. Abrantes, "Performance analysis of an adaptable home healthcare solution," in *13th IEEE Intl. Conf. on e-Health Networking Applications and Services (HealthCom)*, 2011, pp. 134–141.

[16] M. Blount, V. M. Batra, A. N. Capella, M. R. Ebling, W. F. Jerome, S. M. Martin, M. Nidd, M. R. Niemi, and S. P. Wright, "Remote healthcare monitoring using Personal Care Connect," *IBM Systems Journal*, vol. 46, no. 1, pp. 95–113, 2007.

[17] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," *University of Virginia Computer Science Department Technical Report*, vol. 2, 2006.

[18] U. Anliker *et al.*, "AMON: a wearable multiparameter medical monitoring and alert system," *IEEE Trans. Infn. Tech. in Biomedicine*, vol. 8, no. 4, pp. 415–427, 2004.

[19] P. Mohan, D. Marin, S. Sultan, and A. Deen, "MediNet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony," in *30th IEEE Intl. Conf. Engineering in Medicine and Biology Society*. IEEE, 2008, pp. 755–758.

[20] J. H. Flaherty, "Smart Phones for older Chinese with diabetes," *Aging Successfully*, vol. 18, no. 1, p. 17, 2008.

[21] U. Rivett and J. Tapson, "The Cell-Life Project: Converging technologies in the context of HIV/AIDS," *Gateways: Intl. Jrnl. Community Research and Engagement*, vol. 2, pp. 82–97, 2009.

[22] W. H. Curioso, A. E. Kurth, R. Cabello, P. Segura, and D. L. Berry, "Usability evaluation of personal digital assistants (PDAs) to support HIV treatment adherence and safer sex behavior in Peru," in *AMIA Annu Symp Proc*, vol. 918, 2008.

[23] A. J. Fleishman, J. Wittig, J. Milnes, A. Baxter, J. Moreau, and K. Mehta, "Validation process for a social entrepreneurial telemedicine venture in East Africa," *Intl. Jrnl. Service Learning in Engineering, Humanitarian Engineering and Social Entrepreneurship*, vol. 5, no. 1, pp. 1–24, 2010.