IFIP/IEEE WMNC 2013 - 6th Joint Wireless and Mobile Networking Conference, Dubai, UAE, 23-25 Apr 2013

Remote Health Monitoring Using Online Social Media Systems

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

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

***Abstract*—Remote monitoring is considered an essential part of future eHealth systems to enable the delivery of healthcare outside clinical sites at reduced cost, while improving quality of patient care. We examine the use of online social networks for remote health monitoring. By exploiting the existing infrastructure, initial costs can be reduced and fast application development is possible. Facebook is used as an example platform: as a platform allowing user-defined applications, development is flexible and can be arranged quickly to suit different requirements of patients and health professionals. We analyse the general requirements of a remote monitoring scenario and the process of building and using a Facebook application to meet these requirements. Four different access viewpoints are implemented to suit the requirements of each user in our example scenario to form a *carer network*: the patient, the doctor in charge, professional carers, and family members of the patient. The suitability of the application is analysed including security and privacy issues. We conclude that online social media systems could offer a suitable platform for developing certain types of remote monitoring capability.**

I. Introduction

Our previous investigation [1] has shown that the use of a smart phone as a sensor and a gateway to collect health data and connect to Internet for remote health monitoring is feasible. In this work, we will focus on how to access the collected health data and build suitable applications for using the data. We assess the feasibility of enabling remote monitoring applications by using online social network systems.

A. Remote monitoring example – an ageing population

We chose an example scenario of care for the elderly at home, a growing concern worldwide in the context of an 'ageing population'. The UN estimates that 12% of the world population was over 60 years of age in 2012, and by 2050 that figure will be 22% [2]. Advances in healthcare, medicine and technology assist people to live longer. However, longer lifespans means that we have to deal with more chronic illnesses and diseases and for longer, increasing health-care costs.

There is an increasing interest in assisted living technologies for the elderly based on ubiquitous computing. With the help of assisted living systems like remote health monitoring, the high burden on healthcare can be reduced. The intention is that some of the routine services and checking processes, which conventionally are conducted at clinical sites, can potentially be delegated to individual remote monitoring systems within the home. This would reduce healthcare costs, improve patient care and improve a patient's quality of life.

From a clinical point of view, the continuous remote monitoring may in some cases yield better data than the 'snapshot' monitoring that takes place within a clinical site. This enables a longer time scale and a finer granularity of health data monitoring. Also, from a patient's point of view, they need not spend time travelling to the clinical site. Furthermore, remote health monitoring could help to avoid a false or perturbed reading of health data (and so incorrect diagnosis) caused by 'white-coat syndrome'[1] during a visit to a clinical site [3].

While our specific scenario, described below, will consider the remote monitoring of an elderly patient, remote monitoring capability would have applications for many other scenarios, such as care for patients in rural areas, care for patients with acute conditions which require regular monitoring (e.g. recovery after surgery), as well as care for patients with chronic conditions (e.g. monitoring blood-sugar levels in patients with diabetes). Such monitoring may also help with diagnosis of conditions, not just care of patients.

B. Scenario

Figure 1 shows our simple scenario: data is collected from a patient and may need to be accessed by several actors who are remote. Facebook is used as an example of an online social network for our *remote monitoring application (RMA)*. An *elderly patient* is being monitored for a heart condition, and heart-beat readings are transmitted from the patient to the RMA. The RMA and collected data may need to be accessed by the following actors as part of a *carer-network* (our scenario and healthcare processes are based on a medical care regime in the UK):

- *Patient.* The patient may wish to turn the monitoring system on or off (for their own privacy), and may wish to see the data collected.
- *Doctor.* This is a healthcare professional who is responsible for the overall management of the patient's care, e.g. a consultant.
- *Carer.* This is a healthcare professional who is responsible for the delivery of the healthcare on a day-to-day basis, e.g. a local nurse or clinician.

[1] aka 'white-coat hypertension'

- *Family.* This is a family member (or friend) who is concerned about the patient and may wish to be informed quickly of any problems, in order that they can offer assistance to the patient as required.

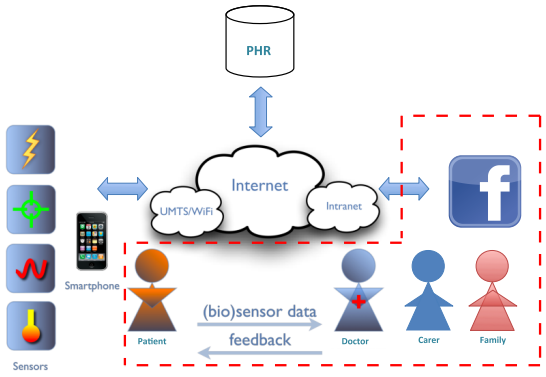


Fig. 1: A remote monitoring application using an online social network to form a *carer-network*. We do not consider the Personal Health Record (PHR), i.e the system concerning the management of individual medical health records. We consider only the specific remote monitoring of an elderly patient, and how to access the monitored health data for patients, doctors, professional carers and family members using an online social network. Our example application uses Facebook. The dashed (red) outline shows the scope of our study.

In this scenario, it is typical that the patient sees the doctor (or consultant) only a few times a year and, in between, needs to go to a local clinic for a regular recording of the heart rate, which is conducted by a professional carer. The health data is then uploaded to a health record for the use of professional healthcare providers, e.g. the PHR. This conventional measurement process taken at clinical sites can be replaced by means of remote health monitoring.

The remote monitoring of a patient can be used to support an ongoing healthcare regime, or to provide (perhaps pre-emptively) emergency assistance, or even for diagnosis of conditions. Sensors are attached to the patients's body and take measurements as configured (e.g. continuously or at intervals, as required). The collected bio-data, e.g. heart-rate, temperature and blood-pressure, are then sent via a gateway/relay on a smartphone to the RMA (and perhaps also cached on the smartphone or sent to another application, as required). Of course, the smartphone can make use of various connectivity, e.g. 3G network or WLAN. An online social network, which is Facebook in our scenario, is used as a portal to access the patient's collected data. Consequently, the professional carers in local clinics and the doctors in hospitals can access health data using the Facebook application (or via the online PHR, as required). Similarly, a patient's family members who live in another town can access the Facebook application to monitor the patient's health status. This enables communication and collaboration in carer networks. Threshold triggers can be set on certain bio-data types, e.g. heart-rate and blood pressure, to generate notifications to various actors as required. For example, if the heart-rate exceeds a threshold or drops below a threshold set by the doctor, family members and carers could be alerted to contact the patient. It is clear that different view points, levels of access to data, and control of configuration will be required for different actors.

C. Contribution

In this paper, our contributions are to assess the suitability of the use of online social networks to form a carer network for remote health monitoring with respect to:

- *Viewpoints.* We identify and define different viewpoints for actors in terms of visibility and control of data, including separation into three different data planes.
- *Security and Privacy.* In relation to the viewpoints, we discuss the security and privacy issues arising, and show how these can be managed.

After describing related work in Section II, we analyse our requirements in Section III. We describe our application development in Section IV, and present in Section V a discussion based on our experience. We finish with a short conclusions in Section VI.

II. Related Work

The related work can be considered in terms of the applications of remote/self monitoring itself, as well as the use of social media platforms.

A. Remote/self monitoring

The eCAALYX project [4] [5] is an example of Ambient Assisted Living (AAL) which aims at building a remote monitoring system targeting older people with multiple chronic diseases. The system deploys Wireless Body Area Networks (WBAN) as means to monitor a patient's health status. Various health data are collected from sensor devices. These devices can be wearable, portable or embeddable with patients, and there are also environmental sensors to provide real-time context on patient health indicators. A smart phone is used as a data collector and a mobile router to send data to a remote server (as in our previous work [1]). The sensed data (such as heart rate, blood pressure, temperature, accelerator or GPS positions), are continuously collected and sent to the remote server for access by healthcare professionals to monitor a patient's condition. The system can also be used to respond to emergencies and accidents related to the patient.

Additionally, there are many examples of commercial support for health/sports monitoring via personal devices (smartphones and music players), including DailyMile [6], RunKeeper [7], Nike+ [8], Adidas miCoach [9], FitBit [10] and LoseIt [11]. Such applications can also connect users to existing social networks to update and share their health data with friends and families.

B. Use of social media

There are many recent studies showing the popularity of online social media systems extended to the healthcare domain. The study by Scanfeld et al [12] showed that people start to share their health-related information online. This results in an increasing number of social networking communities targeted towards health and well-being. Many applications enable users to update their health status and health goals via online community support groups. Personal devices such as smartphones can be used by poeple to monitor their own health-related behaviour [13]. The work in [14] integrated social media such as Facebook, Twitter, Youtube with healthcare information systems as an input for decision support. Furthermore, the investigation by Norval et al [15] suggested the use of an established online social network like Facebook as a framework for telecare. Based on the current advances in technologies, e.g. the accessibility of the Internet, the availability of smart devices and the popularity of existing social networks, the use of social media as a platform for healthcare in some form is already in progress.

Although the use of social media has been extended into healthcare domains, there has been relatively little work examining applying the technologies directly for remote monitoring purposes as described here. The work by Griffin et al [16] proposes the integration of paradigms in social networks into healthcare, i.e. information sharing, monitoring and message alerts. However, only the adoption of the architecture adapted from social networking technologies was proposed, rather than a social media platform. A social network model for health monitoring is then proposed by Detmar et al [17]. Compared to other work, the process did not have much automation, and did not use mobile devices, but did enable patients to control the access to their data. Based on a similar model, work by Ding et al [18] and Ayubi et al [19] employed a monitoring unit, a smartphone and the Facebook platform for monitoring of physical activities.

C. Security and privacy

The work listed above, by Ding et al [18] and Ayubi et al [19], uses Facebook: a Facebook account and its security and confidentiality settings were used for authentication of users. Overall, Facebook was proposed as a platform for self-monitoring, sharing and goal setting, but not for remote monitoring and clinical use as we consider in our work.

Regarding work in the area of Personal Health Record (PHR), Google Health and Microsoft Healthvault [20] are examples of cloud-based platforms which offer services for users to collect, store and manage their own health data. As third-party PHR services, the platforms connect to medical devices to collect data and store it in cloud infrastructure, as well as providing custom APIs to develop Web and mobile applications. The users have full control over their health data to define the level of access and access rights for individual users, e.g. family members, health professionals and healthcare providers. Alternatively to cloud-based platforms, the work by Fox et al [21] proposes a PHR platform using a mashup approach, based on online social network technologies. The patients can add people to create their own carer networks and specify which health data record each member can have access to. Moreover, when data values cross pre-defined thresholds, the system will create alerts sent to relevant social network members to alert them to exceptional conditions and to take appropriate action, e.g. to send help. Although employing a mashup enables fast development and integration, it requires that the health data needs to be pushed to the provider of the Web components being used, so may raise privacy and security issues.

Meanwhile, a social network platform such as Facebook enables fast development while offering some levels of privacy and security. Of course, the platform also presents an interface that is widely known and used, which is also a great advantage.

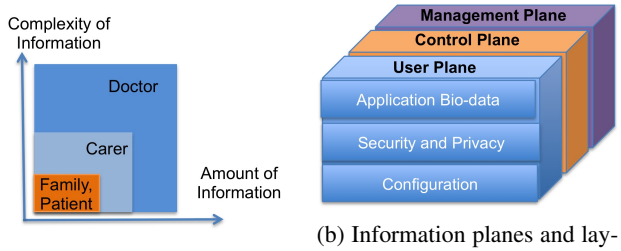
Our work investigated the use of Facebook as an application platform for remote monitoring. We used a mashup approach in our work to realise fast application development, by integrating Google Chart [22] widgets. Please note that we took no initial position that Facebook and Google Charts are particularity suited (or not) to such applications: indeed, our intention was to gain insight to the suitability of such applications development for the RMA.

III. Requirements Analyses

In this section, high level requirements for a remote monitoring application using an online social media platform will be discussed. We consider here general issues, but our discussion is in the context of our scenario in Figure 1.

A. General Requirements

We choose to examine the requirements in terms of data visibility *viewpoints*, in terms of an actor's involvement in the application scenario. Each actor has a different view point. We can establish a qualitative appreciation of the requirements for the viewpoints by considering Figure 2.



(a) Information seen by actors

(b) Information planes and layers within an application.

Fig. 2: Establishing information viewpoints: qualitative considerations based on actors and application. The viewpoints of an actor must incorporate these qualitative considerations.

In Figure 2a, we see a representation of the *amount* of information and *complexity* of information (in terms of medical detail) that we are likely to need for each actor. The patient and family members are likely not to require high-levels of medical detail. The professional carer will need more information and with additional detail. Finally, the doctor/consultant in charge

TABLE I: Summary of actor/bio-data/plane interactions.

	User plane	Control plane	Mgmt plane
Patient	R, simple	RW, simple	No access
Family	R, simple	No access	No access
Carer	R, limited	RW, Limited access	RW, Limited access
Doctor	R, full	RW, Full access	RW, Full access

R = read W = write
simple = 'switch' actions, e.g. on/off
limited = simple + some 'tuning' capability
full = all 'switch' actions plus all 'tuning' capability

of the care is likely to have access to all information with high levels of detail.

In Figure 2b, we see two key dimensions, represented by (a) the *user*, *control* and *management* planes, and (b) the *application information / data*, *security and privacy* and *configuration* layers. (The use of planes in this way is, of course, borrowed from communications system architecture, but lends itself very well to our analyses.) The planes remind us that information that is sent to or from the application could be for control or management purposes, and not just the user data related to bio-data (heart rate, etc.). The distinction between the control and management planes is, essentially, one of timescales and granularity of impact on the application. For example, control signals may be used to configure the minute-to-minute operation of the application at a 'switch' level, e.g. turn it on and off: management signals may impact the longer-term, fine-grained operation of the application at a 'tuning' level, e.g. change heart-rate monitoring from once every 10 mins to once every 2 mins.

This latter example also gives us an introduction to the interaction between the qualitative considerations between actors and information: the management plane is unlikely to be accessed by the user but may be accessed by the carer or doctor, at least in our scenario. So, a full-matrix exploration of the planes and layers is not necessarily required for our simple example, but could yield interesting results for other scenarios.

For considering the layers, we can also see that the security and privacy layer is required for the interaction between configuration signals and the access to the user/application bio-data. For example, the user may wish to turn off all monitoring for privacy purposes, and this may include preventing the 'turn-on' signal from being executed if sent by a carer but is executed if sent by the doctor.

B. Requirements for our scenario

From the general discussion presented above, for our heart-monitoring RMA, we can summarise the requirements in Table I. As space is constrained, this is a simple summary only, but it is enough to present the idea of how the actor/bio-data/plane interaction could be specified in terms of requirements for an application.

We see from Table I that it may also be possible, with appropriate programming models, e.g. by use of a domain specific language (DSL), to translate relatively easily such a set of interactions into a policy for the application.

Of course, there will be other requirements from a human factors perspective, e.g. ease of use, etc., as well as other non-functional requirements, e.g. reliability, etc. Our focus here is on the actors and the bio-data alone for this study.

C. Security and Privacy

Security and privacy are extremely important concerns in a remote monitoring application, both from the point of view of the patient, as well as to be conformant with any applicable laws and regulations. The use of authentication and access control mechanisms at a remote application are therefore necessary. The application needs to authenticate persons who can access the data, e.g. patients, doctors, family members and carers, as well as to restrict their access only to the part of the data they have rights for. The use of suitable access control systems is therefore important and subject to actor-personalised requirements, which are unique to their own environment, capability and responsibility. Additionally, there are practical issues to be concerned with, e.g. if the bio-data gateway is a smartphone, what happens if the device is lost or stolen? Again, we concern ourselves with the interactions between actors and the bio-data.

Studies by Adams et al [23], Caine et al [24], and Lim et al [25] have suggested that patients should have full control of who can access their data. However, most of the studies in this area are applied to Electronic Health Record (EHR) systems, such as a PHR, to allow patients to maintain and manage their own medical records and share them under a patient's control. Since we are dealing with a different environment focusing on remote monitoring, the control of data would be different.

Traditionally, patients do not have control of their data in traditional clinical processes. Therefore, we assume that the access control level should be kept the same even though the monitoring process is moved from clinical sites to, say, a patient's home. Despite the risk that patients do not have control over their own data (which should be kept private), the monitoring processes and clinical care remain the same as today.

We do not consider integration with a PHR: our focus is on acquiring health information from patients for clinical care rather than for managing a patient's health record data. Ideally, the use of a totally open platform, would reduce risks of business models specific to third parties, centralised platforms and healthcare application solutions which could result in high cost of deployment and development. However, currently, such fully-open systems are not widely deployed[2], even though SDKs and APIs for developers are widely available. Since our approach is based on using an online social media platform as an interface, the application could be developed independently without central control, and adapted as required for different social media platforms, using appropriate APIs and SDKs. Key to this is considering carefully the *viewpoints* related to the use of the the data and control flows related to the application.

[2]The Disapora project, started in 2010, has yet to gain widepread use and deployment. http://diasporaproject.org

We are aware that there could be several problems from storing health data on a server of a third party or in cloud services. As with Google Health and Microsoft Healthvault, Facebook uses cloud-based systems. Some countries, have laws or other regulation which govern the collection, storage, use and distribution of personal information. For example, the Data Protection Act (1998) (DPA) in the UK requires that data collected by an organisation must only be used for the purpose for which it is collected and must be stored within the confines of the organisation that collected the data, in accordance with the Act. Overall, then, health data gathered by a health-provider are neither allowed to be stored outside the health institution nor to be given to a third party. So, to employ a commercial cloud-based system for storing health data would be a problem since a data location is physically unknown and data may be stored on servers belonging to third parties in a way which is not conformant with the DPA. There is not yet a defined standard for security and privacy interfaces for online social media networks, though security mechanisms are employed. However, examination of the larger security and privacy issues will be important for such systems, and we defer this to future work. Our goal here is to investigate the feasibility that a social media platform could be employed for constructing remote monitoring application. In a real system, service *provisioning* would need to consider the security and privacy issues that we highlight in this paper.

IV. Application Development

A simplified version of a remote monitoring application using Facebook is implemented in this work. In Figure 3, we show only the implementation of the user plane functions for accessing and viewing of monitored health data. For future implementation of other planes, an application dashboard could be further developed. For simplicity, one patient, one doctor, one carer and one family member were implemented to test interactions. Each actor accesses a Facebook application using his or her own Facebook account, but this account could, of course, be created specifically for this purpose. Figure 3 shows the information flows according to our implementation. The bio-data is collected from sensors and sent to an SQL database: in this case the sensor data is emulated. The Facebook application periodically access the database (a predefined, configurable interval) to update the bio-data display on a Facebook application canvas page. Facebook provides a portal for access control, i.e. each actor logs in to Facebook and sees a different view of monitored health data according to their roles, which are organised via Facbook groups.

Two functions are implemented in our Facebook application. The first function is the read-only access for the patient bio-data in the user plane as shown in Table I. The function is implemented with a different view of recorded bio-data for each user. The second function is a message alert for an emergency situation.

Each authorised actor can access the bio-data only as permitted by the application. Based on sensitivity of the bio-data and suitable policy regarding national laws and regulation,

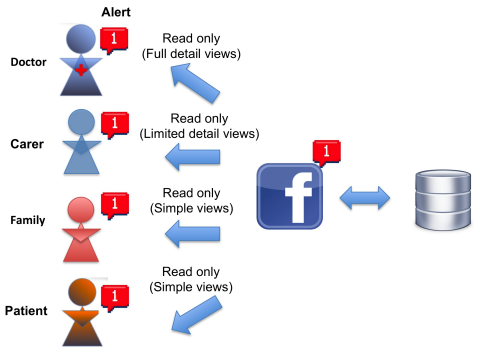


Fig. 3: Information flow and access viewpoint in a user plane implemented for this study. Read-only access with a different view for each user is enabled by using Facebook as a portal. As required, alerts are sent to all users by a Facebook application.

bio-data should be shared with each actor in such a carer network using a predefined application-wide policy.

In this study, we are focusing on four actor categories: a doctor, a carer, a family member and a patient. For simplicity, we assumed that access to the application is centrally assigned to all users by a central policy, which could be an appropriately trusted administrator at the clinical site where the doctor is resident. However, trust relationships could be established and trust delegated as required, e.g. doctors grant access to professional carers and patients grant access to family members, which is permitted via Facebook mechanisms. Facebook was set-up so that each actor has the detailed permissions as given below in the user plane.

- Doctor
  - Full access and complete control over bio-data recording
  - Read only access
  - Monitor bio-data and may send feedback to patient
  - Full textual / numerical data as well as graphical presentation
- Carer
  - Access only to partial bio-data, as specified by doctor
  - Read only access
  - Limited textual / numeric data as well as graphical presentations
- Family
  - No access to textual / numerical data
  - Read only access
  - Graphical presentation
- Patient
  - No access to textual / numerical data
  - Read only access
  - Graphical presentation

In this case, the patient and family views are the same. However, they would differ in the control-plane, as shown in Table I.

The doctor has full access and complete control to all bio-data due to the need for managing the longer-term care regime for the patient. The carer has access only to the part of information required for day-to-day assistance. The family member needs only viewing mechanisms to know if the patient is not needing attention. The same viewpoint is applied to the patient who needs also to monitor their health status but has no access to their detailed bio-data.

Figures 4a, 4b and 4c show the screenshots from our Facebook application and give, respectively, the views seen by the doctor, carer and family member / patient in the user plane. Note that we have used simple visual presentations for proof of concept only. The charts and meter graphics are from Google Charts. We comment on this mashup usage later on. The monitored data is shown in details as a table and a graph, which can be accessed only by the doctor and the carer. In this example, the carer can access only the monitored heartbeat, whereas the doctor has full access to all monitored bio-data. An additional graphic of heartbeat in the form of a meter is used as an example of visualization required to help the carer for quick data interpretation. Finally, the family member has no access to the detailed data. Only a summary message and the graphical meter giving the patient's health status are shown. (The application snapshot of the patient viewpoint is not presented here due to space limitations. However, it is the same as the family viewpoint in Figure 4c.)

When the monitored data reaches a preset threshold value, the Facebook application sends an alert in the form of a notification to all actors in carer network. In our example, the threshold is set for a heartbeat value. When the monitored heartbeat exceeds the predefined threshold, the Facebook notification is sent to all users as shown in Figure 5.

V. Discussion

In the previous sections, we have considered the general requirements needed for a remote monitoring application and have developed an example application using Facebook. We present here a discussion based on the use of Facebook and indicate future directions in order to realise the use of such a platform for real remote health monitoring applications.

A. Suitability of application

In our scenario, we consider the remote monitoring application applied for an elderly patient at home. Therefore, the use of a smartphone and an online social media platform as means for monitoring would be appropriate in many cases, as an adult would be capable of using such devices and interfaces. However, there may be situations where an elderly person with other illnesses would not be able to use a mobile device, e.g. if they also suffered from arthritis in their hands. In a more general situation, the mobile device may not be suitable for all types of patient. For example, a younger patient, a child, may not be able to take care of such a device, e.g. make sure it is charged. However, such a younger patient may also not need any access to the bio-data on the device, and a parent or guardian would help to take care of the device, e.g. for charging. Nevertheless, it does mean that, for the same application – heartbeat monitoring – different devices may be required as suits the patient. While this is not a limitation related to any specific online media platform, e.g. Facebook, it may impose a constrain on its use.

B. Suitability of the Facebook platform

There are many benefits of using a platform such as Facebook for a enabling a carer network for a remote monitoring application, e.g. cost incentive and being a platform with usable SDKs and APIs. In addition, Facebook is also suitable for the following reasons:

1) Basic security and privacy mechanisms: In our implementation, we employ the basic security and privacy mechanisms provided by Facebook, i.e. access control and authentication mechanisms, to ensure the security and privacy of monitored health data. These were sufficient in our simple evaluation, but, of course, we have not conducted any clinical trials with real users.

Based on a Facebook user id, we can ensure that persons accessing the bio-data are who they claim to be, e.g. doctors, carers, family members or patients. Therefore, the appropriate access can be granted. Moreover, the data is still kept private since the application only accesses a specific snapshot from the database, presenting specific data to certain actors, e.g. carer and family. Only the doctor has the full view in our case, and this is controlled from the application canvas in Facebook.

2) Social channel: Facebook provides a social channel with many possibilities to share and publish data, e.g. news feeds, notifications, wall posts and messages, as well as a privacy setting to control who can see the shared information. In our study, a notification is used as a mechanism to send an alert as a direct short message to reach all members in an emulated emergency situation.

3) Grouping: Facebook provides functionality to connect users as a *group* or a *list*. Based on an open graph mechanism, a connection between users is bound by a unique object id. This *social graph* enables a relationship between users, e.g. patients can have lists of people who are their doctors, carers and family members can be grouped into a Facebook page group for communication within a carer network.

4) Use of a mashup: We used tools from Google Charts for the graphical presentation of the data. However, this means that data was sent to Google, which may not be appropriate for privacy reasons as discussed above. However, if such tools were implemented by the healthcare service provider, and hosted by the clinical site, then the graphic tools could be used within Facebook application without any such privacy/security issues. Other benefits may also be possible, e.g. if the data-storage and tools are 'close' in terms of connectivity, there could be a performance advantage; also if all applications use the tools provided by the clinical site, then standard look-and-feel could be adopted across applications, presenting uniform and familiar display of bio-data across different applications.

(a) The Facebook application with doctor viewpoint. Full detail access to bio-data.

(b) The Facebook application with carer viewpoint. Partial detail access of bio-data.

(c) The Facebook application with family viewpoint. No detailed access to bio-data.

Fig. 4: Facebook demo application viewpoints in the user plane (doctor, carer and family). We show a view from a mobile device, but, of course, non-mobile devices can also be with Facebook.

C. Challenges with the Facebook platform

As Facebook has been designed for sharing of social data, it may be considered too open in terms of privacy and security in some cases. Facebook is not designed for implementing private applications which require automated processes such as remote monitoring, but rather for open networks with socialisation as a goal. We found that many of the social plugins which are for general Facebook applications were not suitable for our remote monitoring application.

1) Requirement for user interaction: In order to protect users from unintentionally sharing or publishing information, a Facebook system requires users to confirm that they intend to make the actions they have initiated. Therefore, most Facebook functions require either user interactions or permissions. For example, to post on a user's Timeline, two possibilities are either using a feed dialog, which requires a user interaction, or using an application-generated post, which requires a user's permission to publish on their behalf. In this aspect, Facebook applications cannot support easily the *automated* process that might be required for bio-data monitoring, information dissemination and alerts.

2) Complicated privacy setting: Facebook provides a basic privacy setting for users to control who can see their shared information in an application and a news feed. However, the privacy setting can always be changed by Facebook policy, or easily changed by mistake by users, or simply erroneously configured. As a result, there is a possibility that the heath-related data can be unintentionally shared with one's entire network of friends rather than just the ones related to the remote monitoring applications. Due to the potential sensitivity of bio-data, this is a high-impact risk.

3) Information communication paradigms: It can be challenging to find suitable communication paradigms which enable both privacy and automation. For example:

- *Post to a user's timeline or to friend's news feed.* By using a feed dialog, a graph API could enable an automatic post. However, if users create an incorrect privacy setting, the information could be either exposed to the whole network or may not go to the correct people.
- *Send a message.* A message is sent directly from a user to others. This way, information can always be kept private. However, it is not possible to automate the message sending – user interaction is required.
- *Notifications.* A notification enables users to send a short custom message. Only receivers can see the notification pop up when they log in. Accordingly, 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 used in our application for sending alerts to all users, and is the best suited for our health monitoring application.

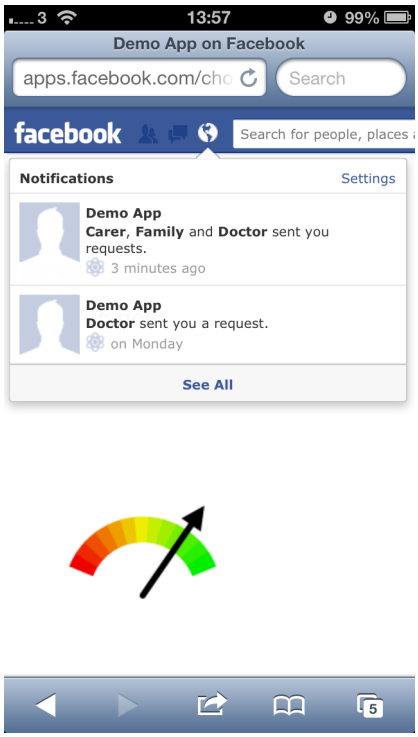


Fig. 5: Demo application with patient viewpoint notification.

VI. Conclusion

Our study shows that simple remote health monitoring applications are feasible using an online social media platform, with appropriate functionality and configuration capability. Our analyses shows that considering actors and the data/actions within user, control and management planes present the formulation of *viewpoints* that can combine the use of (and access to) the bio-data, as well as specific configuration capability, including use of security and privacy policy.

Given known security and privacy policy problems in Facebook, improved security and privacy mechanisms would be beneficial for a real system deployment. To avoid sharing health-related information accidentally, configuration of privacy settings would need to be less open, initially. For example, using a 'default' privacy setting which will be applied to all applications with similar clinical goals would provide a useful feature to protect user privacy.

We also propose that mashups, using components that could be standardised for medical use, e.g. for graphical displays, would enable quick application development.

Finally, we find that there needs to be careful consideration of the needs of automation with respect to use of the bio-data when different communication paradigms and security/privacy issues are considered. Again, the use of 'default' settings and standard communication paradigms, such as notifications, would help in this respect.

Overall, we believe that the development and deployment of online social media platforms for use in remote health monitoring for medical use has great potential for future eHealth/mHealth scenarios.

References

[1] D. Rehunathan, S. Bhatti, O. Chandran, and P. Hui, "vNurse: Using virtualisation on mobile phones for remote health monitoring," in *13th IEEE Intl. Conf. on e-Health Networking Applications and Services (HealthCom)*. IEEE, 2011, pp. 82–85.

[2] M. Greene, S. Joshi, and O. Robles, *State of World Population 2012*. UNFPA - United Nations Population Fund, Nov 2012, https://www.unfpa.org/public/home/publications/pid/12511.

[3] T. G. Pickering, G. D. James, C. Boddie, H. G. A., S. Blank, and J. H. Laragh, "How common is white coat hypertension?" *JAMA - Journal of the American Medical Association*, vol. 259, no. 2, pp. 225–228, 1988.

[4] 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.

[5] 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.

[6] "DailyMile," http://www.dailymile.com, (Jan 2013).

[7] "RunKeepper," http://runkeeper.com, (Jan 2013).

[8] "Nike+," http://nikeplus.nike.com/plus/, (Jan 2013).

[9] "adidas miCoach," http://www.adidas.com/us/micoach/, (Jan 2013).

[10] "FitBit," http://www.fitbit.com, (Jan 2013).

[11] "LoseIt," http://www.loseit.com, (Jan 2013).

[12] D. Scanfeld, V. Scanfeld, and E. Larson, "Dissemination of health information through social networks: Twitter and antibiotics," *American journal of infection control*, vol. 38, no. 3, pp. 182–188, 2010.

[13] B. Silva, I. Lopes, J. Rodrigues, and P. Ray, "SapoFitness: A mobile health application for dietary evaluation," in *13th IEEE Intl. Conf. on e-Health Networking Applications and Services (HealthCom)*, 2011, pp. 375–380.

[14] M. Afzal, M. Hussain, W. Khan, S. Lee, and H. Ahmad, "Social media canonicalization in healthcare: Smart cdss as an exemplary application," in *IEEE 14th Intl. Conf. on e-Health Networking, Applications and Services (HealthCom)*, Oct 2012, pp. 419–422.

[15] C. Norval, J. Arnott, N. Hine, and V. Hanson, "Purposeful social media as support platform: Communication frameworks for older adults requiring care," in *Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2011 5th Intl. Conf. on*. IEEE, 2011, pp. 492–494.

[16] L. Griffin and E. de Leastar, "Social networking healthcare," in *Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th Intl. Workshop on*. IEEE, 2009, pp. 75–78.

[17] S. Detmar, N. Aaronson, L. Wever, M. Muller, and J. Schornagel, "How are you feeling? Who wants to know? Patients and oncologists preferences for discussing health-related quality-of-life issues," *Journal of Clinical Oncology*, vol. 18, no. 18, pp. 3295–3301, 2000.

[18] D. Ding, S. Ayubi, S. Hiremath, and B. Parmanto, "Physical activity monitoring and sharing platform for manual wheelchair users," in *IEEE Intl. Conf. Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2012, pp. 5833–5836.

[19] S. Ayubi and B. Parmanto, "PersonA: Persuasive social network for physical Activity," in *IEEE Int. Conf. on Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2012, pp. 2153–2157.

[20] A. Sunyaev, D. Chornyi, C. Mauro, and H. Kremar, "Evaluation framework for personal health records: Microsoft healthvault vs. google health," in *System Sciences (HICSS), 2010 43rd Hawaii Intl. Conf. on*. IEEE, 2010, pp. 1–10.

[21] R. Fox, J. Cooley, and M. Hauswirth, "Creating a virtual personal health record using mashups," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 23–30, 2011.

[22] "Google Charts," http://nikeplus.nike.com/plus/, (Jan 2013).

[23] E. Adams, M. Intwala, and A. Kapadia, "Med-lights: a usable metaphor for patient controlled access to electronic health records," in *1st ACM Intl. Health Informatics Symp.*, 2010, pp. 800–808.

[24] K. Caine and R. Hanania, "Patients want granular privacy control over health information in electronic medical records," *Journal of the American Medical Informatics Association*, 2012.

[25] J. Lim, A. Zhan, E. Goldschmidt, J. Ko, M. Chang, and A. Terzis, "HealthOS: a platform for pervasive health applications," in *2nd ACM Workshop on Mobile Systems, Applications, and Services for HealthCare*, 2012, p. 4.