ICST Transactions Preprint

Remote Health Monitoring Using Online Social Media★

Chonlatee Khorakhun[1,*], Saleem N. Bhatti[1]

[1]School of Computer Science, University of St Andrews, St Andrews, Fife, UK

Abstract

Remote monitoring is an essential part of future mHealth systems for the delivery of personal and pervasive healthcare, especially to allow the collection of personal bio-data outside clinical environments. Yet, by its very nature, it presents considerable challenges: it will be a highly distributed task, requiring collection of bio-data for a myriad of cources, to be marshalled at the clinical site via secure communication channels. To address these challenges, we propose the use of an online social media platform (OSMP) as a key component of a near-future remote health monitoring system. By exploiting existing infrastructure, initial costs can be reduced, at the same time as allowing fast and flexible application development. An OSMP would have user benefits also: 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 applications. Additionally, the use of a social media context allows existing social interactions within the healthcare regime to be modelled within a *carer network*, working in harmony with, and providing support for, existing relationships and interactions between patients and healthcare professionals. We focus on the use of an OSMP to enable two primitive functions which we consider essential for mHealth, and on which larger personal healthcare services could be built: *remote health monitoring* of personal bio-data, and an *alert system* for asynchronous notifications. We analyse the general requirements in a carer network for these two primitive functions, in terms of four different viewpoints within the carer network: the *patient*, the *doctor* in charge, a professional *carer*, and a *family* member (or friend) of the patient. We discuss the suitability of OSMPs in terms of functionality, performance, security & privacy, as well as the potential for cost reduction.

Keywords: mHealth, eHealth, Remote health monitoring, Online social media platform

1. The growing need for mHealth systems

Advances in mobile technologies and the growing ownership of personal mobile phones have the potential to enable improved healthcare around the world. Figures for 2013 from the International Telecommunications Union (ITU)[1] [3] estimate that the number of mobile subscriptions (6.8B) is approaching the global population (7.1B), with penetration rates of 96% overall, as high as 89% even in developing countries and over 100% in developed countries (people have multiple phone services). In terms of devices, up to February 2014, the mobile phone market in 2013 is 39.2% growth over 2012, with the smartphone shipments being the largest area of growth – surpassed 1 billion units for the first time[2].

mHealth – the use of mobile technologies and services for healthcare – enables pervasive and personal healthcare services, as part of a larger eHealth strategy [4]. mHealth is gaining interest from governments, companies and non-profit organisations to develop and implement applications to improve healthcare worldwide, at the same time as reducing healthcare costs. It is of interest to developed regions of the world to reduce healthcare costs, and it is of interest to developing regions of the world to enable healthcare reach to its citizens, especially in remote areas. Two key primitive functions in such a scenario are remote monitoring and the use especially for

★This paper includes works previously published by the authors in [1] and [2]

*Corresponding author. Email: ck46@st-andrews.ac.uk

[1]http://www.itu.int '... the United Nations specialized agency for information and communication technologies ...'

[2]IDC Worldwide Quarterly Mobile Phone Tracker, Press Release, 26 Feb 2014, http://www.idc.com/getdoc.jsp?containerId=prUS24701614

routine monitoring of bio-data and asynchronous communication with (and feedback from) patients.

In 2009, the United Nations (UN) Foundation established the mHealth Alliance[3] specifically to promote the worldwide use of mobile technologies for healthcare [5] [6].

1.1. mHealth and patient generated data

An essential part of the mHealth ecosystem is the collection of patient-generated, biological data (bio-data), e.g. heart-rate, blood-pressure and other vital signs. This is due partly to the shifting policies in healthcare from late-stage treatments to prevention and early detection, but also a desire to enable routine monitoring for diagnosis, or 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 communicable diseases towards management of chronic illnesses, as a result of an ageing population [7].

Advances in healthcare, medicine and technology assist people to live longer. However, longer lifespans mean that we have to deal with more chronic illnesses and diseases and for longer, contributing to increasing healthcare costs. So, the ageing population also leads to an increasing interest in assisted living technologies for the elderly based on pervasive computing [8], coupled with approaches such as observations of daily living (ODL) in support of personal healthcare. 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% [9]. Caused by a growing concern worldwide in the context of an ageing population and an increasing healthcare burden, the European Commission has invested in an EU funding program focusing on personalising health and care [10]. The use of assisted living systems and remote health monitoring can help to control the increasing burden on healthcare systems by making more efficient use of resources and reducing healthcare costs.

However, as well as an ageing population, the number of citizens is increasing worldwide, and developing regions wish to extend the reach of healthcare services to all citizens, including in remote and/or rural areas [5]. This further compounds the healthcare burden specifically in those regions of the world [11].

1.2. Towards personal, pervasive healthcare

Some of the routine services and checking processes related to the collection of patient bio-data, which conventionally are conducted at clinical sites, can be delegated to individual remote monitoring systems outside the clinical environment. This would reduce healthcare costs, improve patient care and improve a patient's quality of life. We focus on two key *primitive functions*, i.e. building blocks to create higher-level, full mHealth services: **remote monitoring** and **alert systems**.

From a clinical point of view, the use of **remote monitoring** may in some cases yield better quality bio-data than the 'snapshot' monitoring that takes place within a clinical site. Remote monitoring could enable a longer timescale and a finer granularity of bio-data monitoring [12]. For example, as mHealth devices can collect data continuously over extended periods of time, it is possible to record bio-data continuously or intermittently during the activities of daily life on relatively long intervals, rather than a one minute recording taken in the clinic. Also, from a patient's point of view, they need not to spend time travelling to the clinical site. Furthermore, remote health monitoring could help to avoid a false or perturbed reading of bio-data (and so incorrect or delayed diagnosis) caused by 'white-coat syndrome' during a visit to a clinical site [13]. There is much evidence that monitoring patients at home for chronic conditions dramatically improves survival rates and healthcare outcomes [5] [14].

As well as collecting bio-data, the use of an **alert system**, can enable key interaction between patients and healthcare professionals in order to manage the healthcare regime when remote health monitoring is in use. Asynchronous notifications could be used to notify a healthcare professional of significant events related to the patient, e.g. a heart-rate reading shows a potential medical problem with the patient, or a need to adjust the healthcare regime, e.g. heart-rate monitoring intervals should be increased. Studies show that such interactions involving patients and healthcare professionals result in a more meaningful engagement in a diverse range of healthcare systems, and, in turn, a more successful healthcare regime. Two diverse examples are: alerts to pregnant mothers in Rwanda [15]; and alerts to healthcare professionals caring for the elderly in Ireland [16].

1.3. The *carer network*

For mHealth applications, it is important that patients are incorporated into the healthcare system. The use of an online social media platform (OSMP) provides a structure to enable a collaboration between patients and healthcare professionals in a *carer network*, supporting naturally the interactions and relationships that exist in traditional 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

[3] http://www.mhealthalliance.org

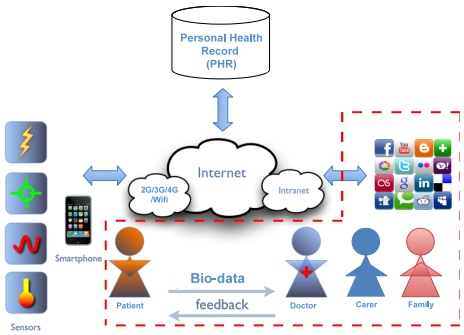

Figure 1. A remote monitoring application (RMA) using an OSMP to form a *carer-network*. OSMP enables communication and colloboration in a *carer-network* as well as provides a portal to access the collected bio-data and to generate a message alert for an emergency situation.

calls. The OSMP has the potential to improve this interaction and so improve the overall quality of healthcare. 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).

As shown in Figure 1, our model of a carer network, which is based on a healthcare regime that is common worldwide [17], 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.

The actors in the carer network could communicate via an OSMP that implements a *remote monitoring application (RMA)*. By exploiting existing infrastructure (OSMP software and network connectivity), fast application development can be enabled and adapted quickly to suit requirements.

1.4. Scenario and contribution

To progress our discussion, we chose an example scenario of care for the elderly at home, a growing concern worldwide in the context of an 'ageing population'. 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.

Figure 1 shows the remote monitoring of an elderly patient. Personal bio-data is collected from a patient, sent to a server and may need to be accessed by several actors who are remote. Our previous investigation [18] has shown that the use of a smartphone as a sensor gateway, to collect health data and connect to the Internet for remote health monitoring, is feasible. The dashed (red) outline indicates our use of an OSMP as a portal to access the collected bio-data within our scenario.

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 [1].
2. Generation of asynchronous alerts [2].

By *primitive functions* we mean basic functions that would be used as building blocks, along with other data and other functions, in order to build a full RMA, fit for a specific use. *Our examples [1, 2] 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 built upon Facebook.*

After describing background in pervasive monitoring in Section 2, requirements and challenges in mHealth systems are provided in Section 3. The details of our design for remote monitoring and remote alerts are given in Section 4 and Section 5, respectively. We describe our application development example, written using Facebook, in Section 6, and discuss the suitability of our approach in Section 7. We describe the prototype description in Section 8, with a summary and conclusion in Section 9.

2. Background

We review an architecture for remote monitoring systems as well as other main areas of development in mHealth related to our focus on using an OSMP in pervasive monitoring: communication technologies, mHealth applications, the use of social media in healthcare along with some issues in pervasive health and well-being monitoring. Indeed, the current state of technology and systems means that self-monitoring – maintaining the *quantified self* – is increasing.

2.1. Technical architecture

Figure 2 shows our view of the technical architecture of typical remote health monitoring systems. The flow of the bio-data occurs as follows:

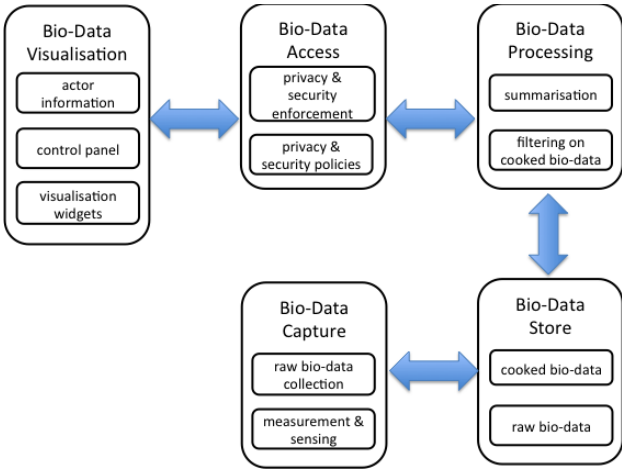

Figure 2. An overview of a technical architecture for health monitoring systems showing the flow of bio-data from being sensed and collected at the patient, being stored and processed at the server, to being accessed and visualised to actors in a carer network.

Bio-data capture. The capture of bio-data is through the use of sensors (for measurement and sensing of patient bio-data) and smartphones (for collection of raw bio-data, temporary storage and relaying of bio-data). A patient carries a personal mobile node (MN - such as a smartphone) which collects health-related information from portable sensor devices. The sensor nodes (SNs) are attached to the patient's body, e.g. a wireless body area network (WBAN) [19]. Using current wireless capability and computing power, a smartphone can act as an interface to sensors, and as a communication gateway, collecting bio-data and supplementary data, and using Internet connectivity to send the data to where it is needed by healthcare professionals, e.g. to a Personal Health Record (PHR). A smartphone can communicate with sensors using common interfaces like Bluetooth, for near-field communication (NFC). The sensed patient bio-data (e.g. heart rate, blood pressure, glucose level, temperature, accelerator or location, etc.) are collected according to a medical healthcare regime configured as part of the wider remote monitoring system.

Bio-data store. The collected bio-data is in the raw form, i.e. the form generated by sensor devices interfaces, and needs to be transformed – 'cooked', i.e. transformed to a format appropriate for a storage in a database. This may include appropriate security and privacy transformations being applied to the data.

Bio-data processing. The stored bio-data needs to be processed before it can be used. This may include a filtering process, e.g. remove noisy measurements or those data outside the date/time of interest. There may also be summarisation mechanisms applied on the filtered data, e.g. calculation of statistical algorithms. For example, vital signs might be measured every 10 seconds, but only the average value over a minute is required.

Bio-data access. Privacy and security policies describe the set of rules and access control policies for the bio-data and the system overall. Each actor has a different requirement and needs to access only the part of the data required, e.g. patients might not need to see all collected data in detail, but doctor would need maximum detail. Then, privacy and security enforcement is a set of code libraries or functions applying and checking that security and privacy policy has been implemented, including dealing with the interaction and access control rules and the various actors that need to use the data.

Bio-data visualisation. Bio-data visualisation provides a user interface that is appropriate to an actor. It consists of actor information (like user identity), a control panel (to configure the application) and visualisation widgets (like meters or graphs helping users to interpret monitored bio-data).

2.2. Communication technologies

In pervasive healthcare, mobile health monitoring can use a smartphone as an Internet gateway to send collected bio-data to a remote server. However, so far, there is no single mobile or wireless technology which can provide pervasive communication coverage. For example, 3G / 4G systems are not available globally, and even where they are available, there may be limited coverage, e.g. within an office building. Meanwhile, wireless local area network (WLAN, aka WiFi) technology is widely available in many office and home environments, but is not designed to provide coverage outside. Therefore, a mix of technologies which work across different mobile networks (2G/3G/4G/WLAN) is required, as provided by modern smartphones. Using the Internet Protocol (IP) allows connectivity across all such technologies [20], since IP is the only technology that provides general interworking by design, by working over the lower-level network technologies.

However, the use of smartphones in mobile health monitoring systems are still sometimes limited to specific-mobile technology, e.g. GSM/GPRS for remote monitoring and SMS for sending alerts [21] [22] [23].

2.3. Mobile health applications

As healthcare models move toward patient-driven models, people start to measure and track their own health data with the help of sensor devices and mobile platforms available for self-monitoring today. This so called the quantified self [24] can be

both individually and in collaboration with others. Accordingly, individual regularly collects own self health data and makes it available to a platform for monitoring. The monitored data can be made available for oneself for the use of self monitoring as well as for trusted thrid parties in healthcare for the use of RMA.

Based on available software development kits (SDKs) for popular mobile operating systems, there are a number of smartphone applications for quantified self-tracking. These range from general 'well-being' applications (monitoring fitness and nutrition) to systems aiding diagnosis and treatment. Many applications enable users to update their health status and health goals via online portals accessed as a web service.

Examples of mobile applications supporting the quantified self and encouraging personal health monitoring and health coaching are DailyMile [25], RunKeeper [26], Nike+ [27], Adidas miCoach [28], FitBit [29] and LoseIt [30]. Such applications can also connect users to existing online social networks to update and share their health data with friends and family. mHealth applications can also be used as a monitoring platform to access health data or as an interface to users (patients and doctors), i.e. as a portal to access health information [31] or to monitor users own health-related behaviour [32]. One challenge in mobile applications development is that several implementations may be required to support different commercial platforms natively, and such applications may not be easily portable across platforms, e.g. Android (Google), Blackberry OS (RIM), iOS (Apple), and WindowsPhone (Microsoft).

So, an open platform with open APIs and SDKs would also enable interoperability and extensibility, i.e. the application could work with a wide range of devices and medical systems. However, according to Jurik et al [33], most of the existing remote monitoring systems have been based on private and closed architectures, e.g. eCAALYX [31] [34], Personal Care Connect (PCC) [14], Alarm-net [35] and Alert portable telemedical monitor (AMON) [36].

2.4. Online social media platforms and healthcare

Studies show the increasing popularity of online social media platforms (OSMPs) extended to the healthcare domain [37–40]. Online social media sites have been widely used to share health interests and concerns among patients, e.g. patientslikeme [41], as well as to support and collaborate between healthcare professionals, e.g. Doximity [42] and Sermo [43]. According to the report from the Pew Research Center [44], the use of social media continues to grow among all age groups of patients including the elderly. The study by Scanfeld et al [45] showed that people are willing to share their health-related information online, under certain conditions. This results in an increasing number of social networking communities targeted towards health and well-being. The work in [46] integrated social media such as Facebook, Twitter, and YouTube with healthcare information systems, as an input for decision support. Similarly, the study in [47] employed social network technologies for decision making to encourage collaboration among health professionals.

The investigation by Norval et al [48] suggested the use of an established online social network, like Facebook, as a framework for telecare, i.e. for communication to help carers stay in touch with patients and provide support when needed. 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 gaining interest.

2.5. Issues in pervasive health and well-being monitoring

Despite the popularity of digital health devices like wearable health sensors and fitness trackers in the market, e.g. Jawbone UP [49], Fitbit [29], Garmin [50], Shine [51], Basis [52], AgaMatrix [53], Lark [54], there has been a lack of interoperability and common development on health platforms. Each device has its own application with APIs to connect to other third party services, and information gathered by those application lives in silos.

Another concern in health and well-being monitoring is privacy & security. The nature of pervasive systems can easily violate the privacy of users [55], e.g. users use mobile devices to monitor their own data, but the data is aggregated and delivered to third party companies developing mobile applications. The article in [56] expresses the growing concern for privacy of using monitoring devices such as Fitbit, i.e. users have no access to their own data while companies developing mobile application make profits from users' data.

Based on these concerns, in this post-Snowden era, there is an increase interest in strong assurances of privacy and security for personal data. So, the challenge is to produce a platform to gather sensitive bio-data, that is open to developers to create applications for sharing of that bio-data, as well as protecting privacy of users. Recent examples are: Sami platfrom from Samsung [57], i.e. an open healthcare platform with cloud support, and with open APIs for both applications and sensor devices; the Healthkit platform from Apple which will be integrated in iOS 8 [58]; and Fluxtream [59], a totally opensource platform helping users gather their own data. These examples show the new trend and recent needs in using an open platform

for health and well-being monitoring, supporting the user desire for the quantified self, and the increase in competition amongst commercial platforms with business requirements as well as for users to have control over sharing of their own data.

3. Requirements and challenges

We place in context our examination of the use of OSMPs for supporting mHealth. Besides common properties and design requirements, 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 & privacy* for users.

3.1. Common properties and design requirements

As stated in a range of studies over many years – 2007 [14], 2011 [31] and 2012 [60] – some important common considerations should be applied to the design and implementation of remote monitoring systems.

Usability: This is considered as the most important requirement – the devices and applications must be easy for patients to use with minimal maintenance and minimal power consumption. Unlike a PC, portable devices like smartphones have a smaller internal storage capacity and processing power as well as a smaller screen size which requires applications to run in a reduced format. The design must therefore have the end user in mind. For example, if users are elderly and not familiar with technology, interfaces for data collection and access must be simple and clear, e.g. large touch screen with few, well-marked controls to help with poor eyesights.

Interoperabiliy: The application should be interoperable across devices and time. This means the system is able to connect and exchange information seamlessly with different sensor devices as well as with different health record systems or medical service providers. In order to achieve interoperability, a standard schema and protocol for data exchange is therefore needed. Mobile nodes could then transform the received data in a common format to support multiple types of biodata together. To overcome the barriers of integration in mHealth systems, there is a clear need for agreement of a common information architecture and data exchange standards.

Scalability: The application must be scalable to support not only large numbers of users (patients and care providers) but also large numbers of devices.

Reliability: Reliability is important for data availability and preventing loss of data due to network failures or poor connectivity. To enable system reliability as a whole, the collection and storage of patient data could be enhanced by additional functions implemented at mobile nodes, e.g. caching data for later transmission or retransmission. Accordingly, the resource limitation at mobile nodes must be balanced against data latency and risk of data loss.

Portability: One key factor to enable pervasive and seamless health monitoring is portability of applications. It is challenging for mobile application developers to select which platforms to support. Particularly, it is preferable that the applications can run on multiple platforms. For example, users should be able to access the application using either their mobile phones, PDAs, personal computers or any other mobile devices, receiving an appropriately transformed view that is suitable for the device being used. Modern WWW standards make this possible today with responsive web design [61].

3.2. 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 [62] and Microsoft HealthVault [63] 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 [64] shows a lack of evidence on the effectiveness of mHealth but suggests this may be due to inadequate evaluation studies of mHealth applications. According to a survey from the World Health organisation (WHO) [6], 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 [65] 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.

3.3. System development and implementation cost constraints

Reports from the UN [5], WHO [6] and the mHealth Alliance [65] 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.

3.4. Security & privacy

The study by Avancha et al [60] from 2012 has defined a set of privacy properties that are required in mHealth systems. In summary, patients need to have 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 analyses of national requirements and laws. The emphasis is on the controls that should be made available for users 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. Furthermore, a study by Prasad et al [66], 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 carefully configured. These two studies mean that developers and users may have to deal with a complex set of security & privacy issues. (We return to this issue of complexity in our implementation examples in Section 4.4.)

In remote health monitoring systems today, users can 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 which body of information, e.g. with healthcare providers to diagnose and monitor their treatment, or with family and friends to motivate them to work towards a healthier lifestyle. So, a mHealth monitoring systems must provide appropriate controls to allow the secure sharing by users of their private health information with people involved in their healthcare.

4. Remote monitoring

In this section, the design of an example Facebook application is discussed to show the implementation of a primitive function for a remote monitoring application (RMA). Our intention is to demonstrate that an OSMP can be a simple platform allowing user-defined applications, so development is flexible and can be arranged quickly to suit different requirements of patients and health professionals.

With respect to Sections 3.1 and 3.4, we address the following requirements:

Usability: By employing a simple web-based interface, we show how data can be presented with different viewpoints that are relevant to the different actors in our carer network (see below).

Interoperability & Portability: A web-interface based on common standards allows the patient bio-data to be accessible on a variety of platforms. We choose to show views on a mobile handset (an iPhone 4s). The standard Facebook API is used.

Scalability: We do not assess this explicitly, but Facebook is used by many millions of users worldwide, and so, potentially, our example is usable on a diverse range of devices and has a global reach.

Reliability: We do not assess this explicitly here. Clearly, reliability issues could arise due to the Facebook service, the mobile device, or the communication service. These are more likely to be engineering issues, rather than architectural issues, so they will need to be assessed specifically for an operational system.

Security & Privacy: Specific, simple security and privacy requirements are implemented, based mainly on access control with respect to the data, as well as for control of the application. We specifically highlight the differences in security & privacy requirements between the actors and their respective viewpoints.

It is to be noted that we do not mandate the use of Facebook specifically for mHealth systems: we explore the functionality of Facebook in order to assess the feasibility

of our approach and to determine where additional work is required.

4.1. Actor viewpoints

Four different access viewpoints are implemented to suit the requirements of each user in our example scenario to form a *carer network*.

Figure 3 shows our simple scenario, based on Figure 1. 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.
- *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.

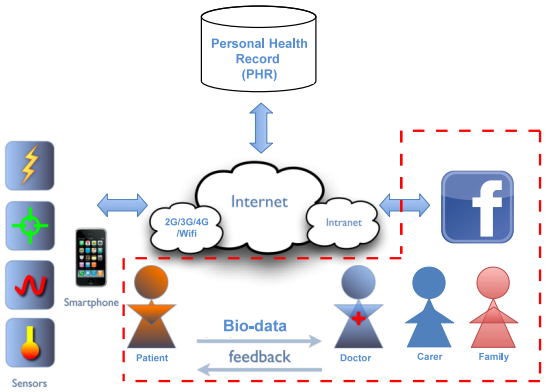

Figure 3. A remote monitoring application using an online social network to form a *carer-network*. We do not consider the Personal Health Record (PHR), i.e the system concerning the management of individual medical health records. We consider only the specific remote monitoring of an elderly patient, 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.

So far, we have tested and looked at the bit of bio-data processing and bio-data access in the technical architecture as described in Figure 2. This is according to a dash (red) outline in Figure 3. 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).

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.

4.2. Related work

The work by Griffin et al [67] 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 the use of an OSMP. A social network model for health monitoring is proposed by Detmar et al [68], but it does not consider mobile devices, even though it did enable patients to control access to their data. Based on a similar model, work by Ding et al [69] and Ayubi et al [70] employed a monitoring unit, a smartphone

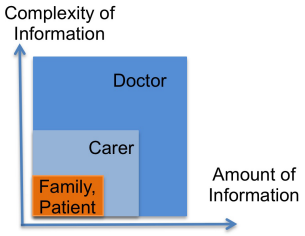

Figure 4. Information seen by actors. Establishing information viewpoints: the viewpoints of an actor must incorporate these qualitative considerations. Managing presentation of a potential large and complex data set is major issue with respect to the usability of the system.

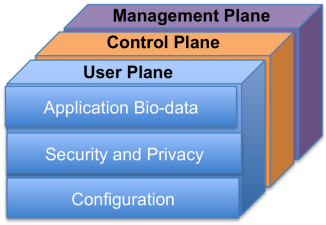

Figure 5. Information planes and layers within an application. This further characterises qualitative partitions for the viewpoints in terms of the data-flows that may exist within an application. The user / control / management model is borrowed directly from data communications.

and the Facebook platform for monitoring of physical activities: 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.

The work by Fox et al [71] proposes an interface to 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 is pushed to the provider of the Web components being used, so this may raise privacy and security issues.

We also used a mashup approach in our work to realise fast application development, by integrating Google Chart [72] 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.

4.3. Viewpoints for actors

According to privacy and security policies described in our archetecture in Figure 2, we choose to examine the requirements in terms of data visibility *viewpoints*, mapping an actor's involvement in the application scenario. Each actor has a different viewpoint. We can establish a qualitative appreciation of the requirements for the viewpoints by considering Figure 4 and 5.

In Figure 4, 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 of the care is likely to have access to all information with high levels of detail.

In Figure 5, 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.

In 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.

Table 1. 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

From the general discussion presented above, for our heart-monitoring RMA, we can summarise the requirements in Table 1. This is a simple summary only, in order to demonstrate applicability: a more detailed analyses would be required for a specific system. However, 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 1 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.

4.4. Security and privacy

In line with the security and privacy discussion in Section 3.4 and bio-data access part of our architecture in Figure 2, 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 only.

According to [60] and [66], the studies by Adams et al [73], Caine et al [74], and Lim et al [75] 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 EHR / 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 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 GoogleHealth 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. According to the study in patient privacy by Baker et al [76], the Data Protection Directive in the EU makes it in practice very difficult, even impossible to comply with the requirements if personal data is stored in the cloud. Similarly, 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 an OSMP could be employed for constructing the RMA. In a real system, service *provisioning* would need to consider the security and privacy issues that we highlight in this paper.

5. Remote alerts

In this section, we extend our design considerations of our architecture, i.e. bio-data access and bio-data processing in Figure 2, to also include an alert system.

Alerts are an essential part of future remote health monitoring. Coupled with appropriate sensing and communication systems, alerts could be used for a variety of purposes within the healthcare regime, e.g.:

- Notifying the carer network members about changes in a patient's condition.
- Flagging changes in operation of the RMA, e.g. the RMA is turned on or off.
- Sending periodic reminders to the patient to undertake a certain action, e.g. take medication.

- Allowing healthcare workers to send asynchronous requests to a patient as part of the overall healthcare regime.

We consider the first one of these only, and will present others in future work. We take the position that such alert-based systems will, initially, *not* be used for critical care, e.g. a patient with a severe heart-condition. Instead, we consider alert systems as part of care regimes dealing with more routine monitoring of less critical conditions; or for ambulatory monitoring and data collection in diagnosis; or for gauging the effectiveness of ongoing treatment.

We focus on *alerts* implemented using the notification services of the OSMP, Facebook. Under configuration control, alerts are sent to appropriate actors.

5.1. Related work

SMS has been used to send notifications or alert messages in telemedical applications. In such systems, a local PC receives monitored health data via a short range communication, e.g. RF or bluetooth, and sends SMS. Previous work [77] [78] shows example systems in which SMS messages are sent to concerned medical experts and/or to relatives by a GSM modem attached to a local PC when monitored vital signs exceed a threshold. SMS has also been used in telemonitoring for transmitting monitored health data which does not need high bandwidth. Other work [16] [79] has proposed the use of the SMS platform for health monitoring with fully automatic transmissions via GSM.

In pervasive healthcare, mobile health monitoring uses a smartphone as an Internet gateway to send collected health data to a remote server. In emergency situations, a server can possibly send an alarm or alert message via the Internet, SMS or email to handheld devices. However, in such systems, e.g. [21] [22] [23], SMS is still mainly proposed as a means for sending alerts. Similar to our work, [80] proposes heart disease monitoring and alerting systems using a smartphone.

While SMS and the use of a smartphone for sending alerts have been considered previously, there has been no work examining the use of OSMPs, and the use of an Internet-protocol-based network has been limited to the use of email.

5.2. Requirements analyses

As we have discussed in Section 4.3 and in accordance with privacy and security policies bit of our architecture in Figure 2, information sent to and received from an RMA could be related to health bio-data (user plane), control (plane) data for the configuration of the application, or management (plane) data related to the overall operation of the application (systems-related), or the health-regime policy (user-related). Hence, we chose to specify three main types of alerts, based on Figure 3:

Table 2. Events signalling a state change (see Figure 6).

	e1	e2	e3	e4	e5	e6
Patient	yes, high	yes	yes, high	yes	yes	yes
Family	yes, high	yes	yes, high	yes	yes	yes
Carer	yes, high	yes	yes, high	yes	no	no
Doctor	yes, high	yes	yes, high	yes	no	no

yes = alert sent no = alert not sent
high = high level of reliability / urgency

- *bio-data alert:* This alert type is triggered from the bio-data, e.g. by the use of threshold triggers. Health alerts are sent to appropriate actors in a carer network.

- *system alerts:* This type of alert is triggered by a change in the configuration of the RMA. For example, when a patient switches on/off the monitoring, alerts will be sent to notify a healthcare professional in the carer network. Also, any configuration signal sent by a carer, e.g. adjusting of monitoring frequency should trigger an alert sent to the doctor responsible for overall care.

- *messaging alerts:* This type of alert is for user-level messages, either sent by manual intervention (e.g. a message from a doctor to enquire about a patients care) or automatically generated (e.g. a reminder for medication).

We consider these to be alert *primitives*, and further, higher-level alert-types could be realised based on these, as appropriate for a particular application. We examine the first of these. Alerts will be sent according to the values of monitored bio-data. We have chosen to emulate a heart-monitoring application with the following states:

- *Normal:* The monitored bio-data are in normal ranges. No need for any action.

- *Warning:* The monitored bio-data starts to deviate from normal values. Patients need to be notified to be aware of the situation. There is no need yet for doctors to take action, but, depending on the healthcare regime, a professional carer or family member may be notified.

- *Critical:* The patient is in a situation where some intervention is required by a medical professional. All actors will be alerted of this situation with urgency.

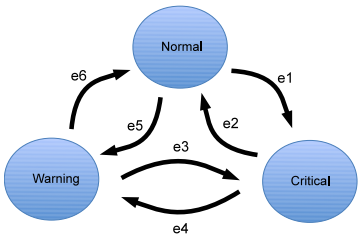

Figure 6. A state diagram showing all possible changes in health status and events (see Table 2) triggered by each change for our emulated heart-monitoring application.

The state diagram is shown in Figure 6, while Table 2 shows the alerts that are generated and which actors receive the alerts. Of course, this table could be configured as required for a particular patient or particular healthcare regime. For simplicity, we have so far considered a single actor for each part of the carer network. However, it is clear that the various actors we have chosen could in fact be *groups*, and the alerts are delivered to everyone within the group identified.

The triggering of alerts needs to be highly configurable, but the generation of alerts should not have to rely on manual intervention, i.e. should be automated via the OSMP. Where, 'high' urgency or reliability of delivery is needed for alerts, then the OSMP should support some sort of additional reliability mechanism accessible to the application developer, e.g. OSMPs can offer delivery of notifications via SMS as well as via the normal delivery mechanism via the Internet. However, the exact nature of the urgency/reliability mechanism would be application-specific.

6. Application development

We now consider the implementation of the remote monitoring and alert primitives in our example Facebook application. We reiterate that our implementation is created in order to further our discussion regarding the use of OSMPs for mHealth, and we do not claim this to be a deployment-ready mHealth application.

For monitoring, we chose to implement an application dashboard which includes read-only access for the patient bio-data in the user plane and read-write access for the application control in the control and management planes as shown in Table 1. The function is implemented with a different view of recorded bio-data and configurability of control data for each user. The second function is a message alert for an emergency situation.

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.

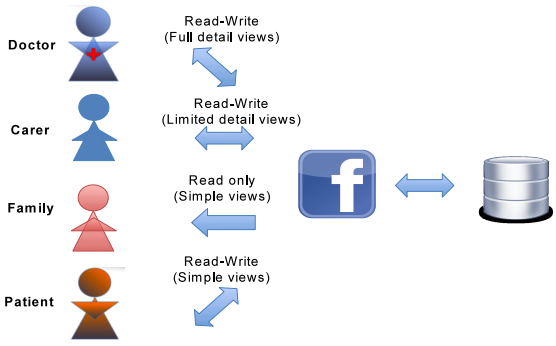

Figure 7. Information flow and access viewpoint in a dashboard implemented for this study. Read-only and Read-Write access with a different view for each user is enabled by using Facebook as a portal.

6.1. RMA dashboard

In Figure 7, we show the implementation of the user plane, control plane and management plane functions for accessing and viewing of monitored health data as well as for control of the application. Figure 7 shows the information flows according to our implementation. To model the bio-data capture and bio-data store part of our architecture in Figure 2, 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 process (the bio-data process in Figure 2) and 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 application dashboard according to their roles, which are organised via Facebook groups.

According to the bio-data access described in our architecture in Figure 2, each authorised actor can access the bio-data and control-data only as permitted by the application. Based on sensitivity of the bio-data and suitable policy regarding national laws and regulation, 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.

The doctor has full access and complete control to all 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. Although the patient and family views are the same in the user-plane, they would differ in the control-plane, as shown in Table 1.

According to the bio-data visualisation part in our architecture in Figure 2, application dashboards are implemented. Figure 8, 9 and 10 show the application dashboards for doctor, carer and patient viewpoints, allowing views of various bio-data as a table and graphs. It is possible via the dashboard to change RMA configuration, e.g. switch on/off or change monitoring frequency. Note that we have used simple visual presentations for proof of concept only. The charts and meter graphics are from Google Charts. 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. The patient and family member have no access to the detailed data. Only a summary message and the graphical meter giving the patient's health status are shown. The doctor has full read-write access over data in control and management planes, while the carer has less configurability. Finally, patient has only simple access to a control plane, i.e. for switching on/off the application. (The application snapshot of the family viewpoint is not presented here, because in this case it is the same as the patient viewpoint in Figure 10, but without access to a control plane.) We show a view from a mobile device, but, of course, non-mobile devices can also be used with Facebook.

6.2. RMA Alert

We have implemented medical alerts triggered by bio-data and notifications of management-related actions in relation to the operation of an example heart-monitoring application.

Figure 11 shows the view of our experiment for generating alerts. The emulated heart-rate bio-data is collected every 20s from our 'patient' and stored in a MySQL database. A Facebook application polls the data every 1 second and generates alerts as required, based on the discussion above (see Figure 6 and Table 2). This means that alerts should be available within ≈20s of an event occurring at the patient, and of

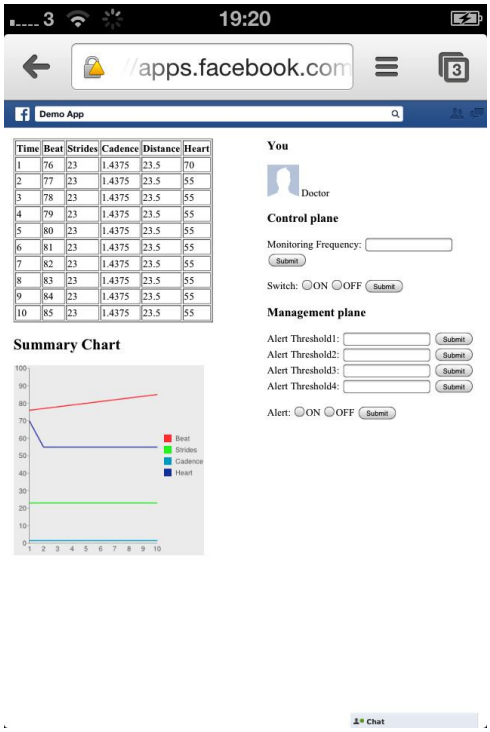

Figure 8. The Facebook application: doctor viewpoint. Dashboard access to bio-data and control-data. The doctor sees a table of data, a summary chart and has access to control of the application.

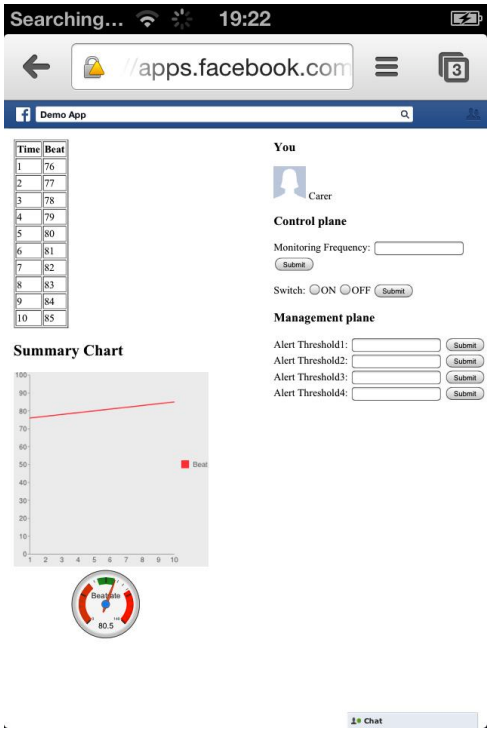

Figure 9. The Facebook application: carer viewpoint. Partial detail access of bio-data and control-data. The carer sees a simplified table of data, a summary chart and meter (for heart rate only), but still has access to control of the application.

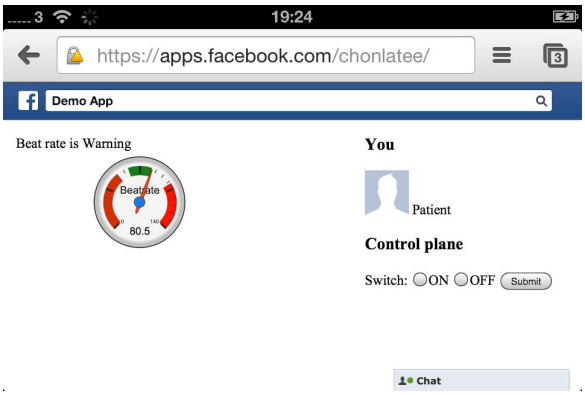

Figure 10. The Facebook application: patient viewpoint. No detailed access to bio-data and a simple access to control-data. A simplified version of a heart rate display, with a simple on/off control.

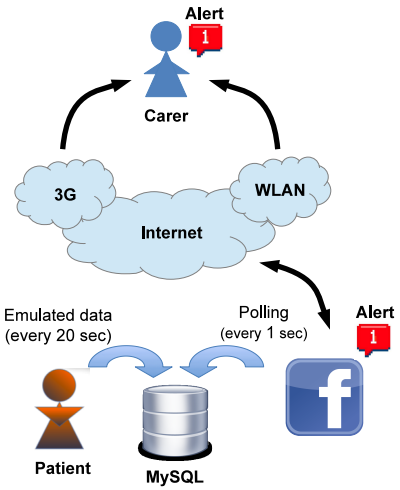

Figure 11. Testing alert delivery latency. Heart-rate bio-data is emulated and stored in a MySQL database with a timestamp every 20 seconds. Our Facebook application polls the database every second, issuing an alert when new bio-data is seen.

Figure 12. Alerts delivered as Facebook notification messages: doctor viewpoint. Both bio-data and system alerts are shown.

course this could be changed as required. Given the nature of the monitoring – non-critical – sub-second alerts are not required. (Polling-based systems have inherent scalability issues, but our intention here is to understand if timely delivery of alerts is feasible.) We record a timestamp when the alert was generated at the 'patient', then check the Facebook timestamp when the notification was visible to an actor.

When the monitored bio-data reaches predefined thresholds or there is a configuration change in the application, alerts in the form of Facebook notifications will be generated.

For the bio-data, the thresholds would be tuned to a specific patient as required. For our proof-of-concept, we have used a simple threshold model based on a document from *Heart Research Australia* [81] (bpm = beats per minute):

- *Normal:* 60-80 bpm.
- *Warning:* 50-60 bpm or 80-100 bpm.
- *Critical:* less than 50 bpm or more than 100 bpm.

Alert delivery latency. A smartphone with browser access to Facebook was tested on 3G and WLAN connectivity each for a 2-hour period. The emulated patient was configured to generate 3 notifications per minute. The distribution of latency of alerts is shown in Figure 13 with some statistics in Table 3. Overall, our simple experiment shows that the alert delivery latency using Facebook is low, albeit with significant differences between 3G and WLAN.

Alerts are implemented as Facebook notifications, e.g. Figure 12. Facebook groups are used for actors and individual users are assigned to the appropriate group. Alerts are sent to the predefined group of people according to Table 2. We are aware that there are other factors that could affect the heart rate, e.g. activities, temperature and body size. Therefore, additional bio-data and a more sophisticated model would be needed to detect any abnormality correctly, in reality.

Using an OSMP for remote monitoring would allow a range of user terminals for the actors, e.g. desktop, tablet, smartphone. We choose to use a smartphone, as alerts are asynchronous, and so actors, such as family

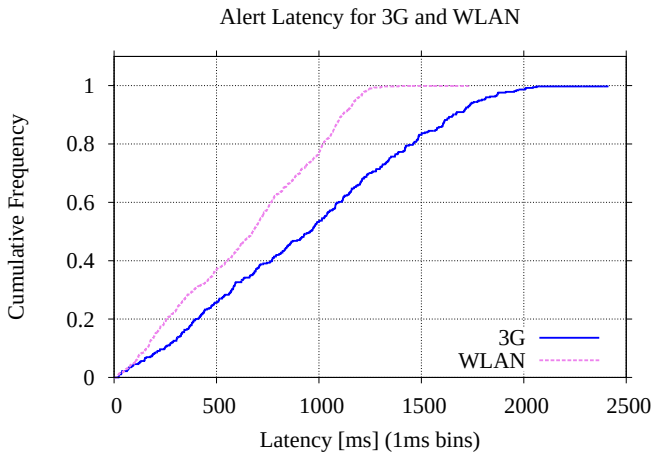

Figure 13. Alert latency: Cumulative distribution of Facebook to smartphone latency (see also Table 3).

Table 3. Alert latency: Statistics for Facebook to smartphone latency (see also Figure 13).

	min	mean	max	median	range	95%-tile	99%-tile
3G	23	940	2410	959	2387	1785	2008
WLAN	16	651	1730	677	1714	1179	1248

latency values all to the nearest millisecond

members and carers, may choose to monitor such alerts while engaged in other activities which mean that the use of a desktop or tablet is not practical.

7. Performance and cost

In the previous sections, we have considered the general requirements needed for our RMA and have developed an example application using Facebook. We present here a discussion discussing the suitability of the application, and indicate future directions in order to realise the use of an OSMP as platform for real remote health monitoring applications. The suitability of the application is analysed including cost reductions as well as security and privacy issues.

7.1. Usability

In our scenario, we consider the remote monitoring application applied for an elderly patient at home. Therefore, the use of a smartphone and an OSMP 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 handheld 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 OSMP, e.g. Facebook, it may impose a constrain on its use. While our study does not include an in-depth examination of usability issues, we acknowledge that this is an important area for further research.

7.2. Reflections on the use our RMA

There are many benefits of using a platform, such as Facebook, for enabling a carer network for a remote monitoring application, as we have discussed. In addition, Facebook is also suitable for the following reasons:

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.

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.

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 which can be grouped into a Facebook page group for communication within a carer network.

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 previously. 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 the 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 where large volumes of data are involved. 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.

7.3. Security & privacy

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[4], can provide maximum flexibility for connectivity, as well as allowing enhanced application capability and customised security and privacy controls.

The decentralised and cooperative nature of Diaspora would allow individual healthcare providers (or sites), to create OSMP-based services, but allow sharing of data for the benefit of the patient, all subject to appropriate policy, security and privacy constraints. Indeed, a user may choose to run his/her own Disapora node to hold their own data and share with the healthcare provider.

Accordingly, users would have control over their own data as well as security and privacy configuration. Individual health service providers could implement policy and data management that is compliant to national laws, and to administer OSMP-based services to enable the remote monitoring application functionality, as well as fine-grained control over privacy and security. So, by employing an open source OSMP, health data can be stored on servers belonging to a healthcare provider, conforming with legal requirements.

[4]https://diasporafoundation.org

7.4. Cost estimates

We have said in Section 3.3 that costs are considered a barrier for large scale use of mHealth systems. So, we provide here an outline cost of using the Diaspora platform in order to provide a remote health monitoring system.

Cost of devices. The purchase of devices, i.e. sensors and smartphones, are unavoidable. In our prototype system (as will be described in Section 8), Fitbit One is used. However, this would make no difference in the real deployment since sensor devices would also need to be purchased. The cheapest suitable smartphones on the market are sufficient to allow web access, and patients may have existing smartphones that can be used directly, further reducing costs. Also, the measurement device might be re-usable for more than one patient, e.g. our Fitbit is reusable. For our experiment, the combination of Fitbit device and (low end) smartphone would be ~US$150 (GB£100).

Cost of IP service. For Internet connectivity, the cost of IP service varies depending on Internet providers. Our observation is that the measurement data has low capacity requirements (a few 10s of Kbps at the most). Assuming we use a UK Internet SIM such as [82], the cost is ~US$15 per month (GB£10). Again, a patients' existing smartphone connectivity could be leveraged, removing this cost. At the measurement server, 1000 users would generate traffic of a few Mbps, a modest traffic load.

Cost for server(s). As data rates are low (see above), a measurement server could handle many users, e.g. perhaps 1000 or more. A low-end enterprise class server in the UK (1U rackmount) is ~US$750 (GB£500). The real server load would come from access to the data by the actors and for visualisation. However, this might be possible through a marginal increment of the existing IT infrastructure by the healthcare provider. Excluding the cost needed for hardware, our implementation is based mainly on an open, freely available platforms and software, i.e. Diaspora and Google Charts.

Development costs. These will depend on the application, but will be lower than for applications using custom hardware with non- standard technologies and APIs. We envisage these to be the main costs. Its detailed assessment would be required to establish true costs for application development.

8. Enabling the carer network

In this section, we show that it is feasible to build an OSMP with suitable functionalities in line with our architecture today.

8.1. Prototype description

To realise our vision, we are currently building a prototype based on an open source Diaspora

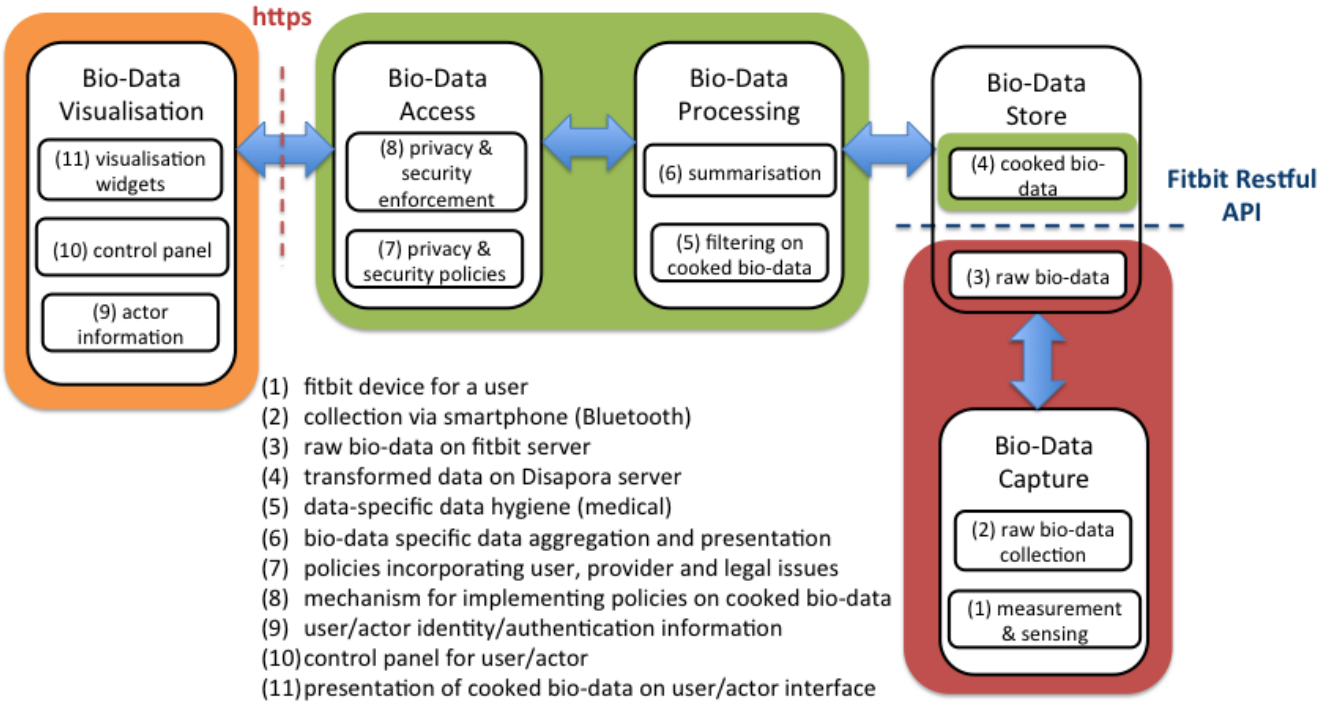

Figure 14. A technical architecture for our monitoring systems showing a flow of bio-data from measurement devices (shown in red), i.e. Fitbit and smartphone, to Diaspora platform (shown in green and orange).

platform to implement primitive functions for remote monitoring application. Figure 14 shows our design mapping to the system architecture presented in Figure 2. In our application development, Fitbit activity tracker devices [29] are used as a measurement system for convenience, but a real medical application would use a different measurement system. The role of Fitbit and smartphone with respect to our architecture is shown in red and numbered (1)-(3) in the diagram. The raw Fitbit data is uploaded and stored in the Fitbit server via the use of a smartphone. The Diaspora platform accesses the raw data using the Fitbit RESTful API and stores the cooked data in a Diaspora server. Our focus on the use of the Diaspora as an open platform is shown in a green and numbered (4)-(8) in the diagram. The platform is modified to provide the RMA functions, as well as the interaction between the actors in a carer network. For real deployment, the process of bio-data (5) can be done by medical experts. For bio-data access, each actor accesses the platform and will see a different viewpoint of monitored data depending on their roles in the carer network. This is controlled by access control policies, i.e. number (7) in the diagram, implemented according to the description in Section 4.1. However, this will be configured by the healthcare provider in real scenarios, with appropriate consideration of patients personal privacy preferences, national laws, etc. The access to the platform is also secure via https.

So, our main focus is on development of the online social media platform numbered (4)-(8) in the diagram. We use Fitbit to provide functionality for items (1)-(3), but another measurement and collection system could be used. The visualisation of bio-data, i.e. items (9)-(11) in the diagram, are implemented only to allow our work to be demonstrated: this would be an excellent place for those with expertise in HCI to consider this relatively new approach and make advances.

9. Conclusion

In this work, our contributions are to assess the suitability of the use of online social media in support of implementation of a remote monitoring for mHealth systems. We examine the design and implementation of two primitive functions, *remote monitoring* and *alert systems*, which could be used to build higher-level, full remote monitoring applications (RMAs) for a mHealth system.

From our analyses, 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 in 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 functionalities 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. We make the case for the suitability of an OSMP as a future platform for eHealth platform.

- *Alerts.* The OSMP allows the provision of alerts in an RMA to be delivered using the asynchronous notification mechanisms that exist in many OSMP platforms. We examine the practicality of delivery alerts using WiFi access and and 3G connectivity.

- *Security & Privacy.* We identified and defined different information *viewpoints* in the carer network, in terms of the actors and their respective relationships. The security and privacy issues can be analysed in terms of these viewpoints for coherence of policy and to reflect the visibility of information that would exist in the natural relationships that exist for the actors. We find that OSMPs offer many useful functions, but no single existing OSMP provides the full set of security and privacy features that we might need for an OSMP in support of 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] Khorakhun, C. and Bhatti, S.N. (2013) Remote Health Monitoring Using Online Social Media Systems. In *Proc. 6th IFIP/IEEE Wireless and Mobile Networking Conference (WMNC2013)*.

[2] Khorakhun, C. and Bhatti, S.N. (2013) Alerts for Remote Health Monitoring Using Online Social Media Platforms. In *15th IEEE Intl. Conf. on e-Health Networking Applications and Services (HealthCom)*.

[3] ITU, The World in 2013: ICT Facts and Figures, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf. (Feb 2013).

[4] WHO and ITU (2012) *National eHealth Strategy Toolkit* (WHO Press). URL http://www.itu.int/pub/D-STR-E_HEALTH.05-2012.

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

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

[7] Gutiérrez-Robledo, L.M. (2002) Looking at the future of geriatric care in developing countries. *The Journals of Gerontology Series A: Biological Sciences and Medical Sciences* **57**(3): M162–M167.

[8] Kwan, A. (2012) *Using Mobile Technologies for Healthier Aging* (mHealth Alliance, United Nations Foundation). URL http://www.mhealthalliance.org/images/content/mhealth-and-aging-report.pdf.

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

[10] European Commission, Health, Demographic Change and Wellbeing, http://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing. (Feb 2013).

[11] Lionis, C. and Petelos, E. (2013) The impact of the financial crisis on the quality of care in primary care: an issue that requires prompt attention. *Quality in primary care* **21**(5): 269–273.

[12] Liang, X., Li, X., Barua, M., Chen, L., Lu, R., Shen, X. and Luo, H. (2012) Enable pervasive healthcare through continuous remote health monitoring. *IEEE Wireless Communications* **19**(6): 10–18.

[13] Pickering, T.G., James, G.D., Boddie, C., A., H.G., Blank, S. and Laragh, J.H. (1988) How common is white coat hypertension? *JAMA - Journal of the American Medical Association* **259**(2): 225–228.

[14] Blount, M., Batra, V.M., Capella, A.N., Ebling, M.R., Jerome, W.F., Martin, S.M., Nidd, M. *et al.* (2007) Remote health-care monitoring using Personal Care Connect. *IBM Systems Journal* **46**(1): 95–113.

[15] Ngabo, F., Nguimfack, J., Nwaigwe, F., Mugeni, C., Muhoza, D., Wilson, D.R., Kalach, J. *et al.* (2012) Designing and Implementing an Innovative SMS-based alert system (RapidSMS-MCH) to monitor pregnancy and reduce maternal and child deaths in Rwanda. *The Pan African Medical Journal* **13:31**. URL http://www.panafrican-med-journal.com/content/article/13/31/full.

[16] Scanaill, C.N., Ahearne, B. and Lyons, G.M. (2006) Long-term telemonitoring of mobility trends of elderly people using SMS messaging. *IEEE Trans. on Inform. Technology in Biomedicine* **10**(2): 412–413.

[17] Carpentier, N. and Ducharme, F. (2003) Care-giver network transformations: the need for an integrated

perspective. *Ageing and Society* **23**(04): 507–525.

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

[19] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H. and Leung, V.C. (2011) Body area networks: A survey. *Mobile Networks and Applications* **16**(2): 171–193.

[20] Bui, N. and Zorzi, M. (2011) Health care applications: a solution based on the internet of things. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (ACM): 131.

[21] Moron, M.J., Luque, J.R., Botella, A., Cuberos, E., Casilari, E. and Díaz-Estrella, A. (2007) J2ME and smart phones as platform for a Bluetooth Body Area Network for Patient-telemonitoring. In *29th IEEE Annual Intl. Conf. Eng. in Medicine and Biology Society*: 2791–2794.

[22] Lv, Z., Xia, F., Wu, G., Yao, L. and Chen, Z. (2010) iCare: A Mobile Health Monitoring System for the Elderly. In *IEEE/ACM Int'l Conf. Cyber, Physical and Social Computing (CPSCom)*: 699–705.

[23] Lee, R.G., Lai, C.C., Chiang, S.S., Liu, H.S., Chen, C.C. and Hsieh, G.Y. (2006) Design and implementation of a mobile-care system over wireless sensor network for home healthcare applications. In *28th IEEE Intl. Conf. Engineering in Medicine and Biology Society (EMBS'06)*: 6004–6007.

[24] Swan, M. (2009) Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. *International journal of environmental research and public health* **6**(2): 492–525.

[25] DailyMile, DailyMile, http://www.dailymile.com. (Jun 2014).

[26] RunKeeper, RunKeepper, http://runkeeper.com. (Jun 2014).

[27] Nike, Nike+, https://secure-nikeplus.nike.com/plus/. (Jun 2014).

[28] Adidas, adidas miCoach, http://micoach.adidas.com. (Jun 2014).

[29] FitBit, FitBit, http://www.fitbit.com. (Jun 2014).

[30] LoseIt, LoseIt, http://www.loseit.com. (Jun 2014).

[31] Boulos, M., Wheeler, S., Tavares, C. and Jones, R. (2011) How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *Biomedical engineering online* **10**(1): 24.

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

[33] Jurik, A.D. and Weaver, A.C. (2008) Remote medical monitoring. *Computer* **41**(4): 96–99.

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

[35] Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., Fang, L. *et al.* (2006) ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring. *University of Virginia Computer Science Department Technical Report* **2**.

[36] Anliker, U., Ward, J.A., Lukowicz, P., Troster, G., Dolveck, F., Baer, M., Keita, F. *et al.* (2004) AMON: a wearable multiparameter medical monitoring and alert system. *Information Technology in Biomedicine, IEEE Transactions on* **8**(4): 415–427.

[37] Vance, K., Howe, W. and Dellavalle, R.P. (2009) Social internet sites as a source of public health information. *Dermatologic clinics* **27**(2): 133–136.

[38] Bosslet, G.T., Torke, A.M., Hickman, S.E., Terry, C.L. and Helft, P.R. (2011) The patient–doctor relationship and online social networks: Results of a national survey. *Journal of general internal medicine* **26**(10): 1168–1174.

[39] Chou, W.Y.S., Hunt, Y.M., Beckjord, E.B., Moser, R.P. and Hesse, B.W. (2009) Social media use in the united states: implications for health communication. *Journal of medical Internet research* **11**(4).

[40] Von Muhlen, M. and Ohno-Machado, L. (2012) Reviewing social media use by clinicians. *Journal of the American Medical Informatics Association* **19**(5): 777–781.

[41] patientslikeme, patientslikeme, http://www.patientslikeme.com. (Jun 2014).

[42] Doximity, Doximity, https://www.doximity.com. (Jun 2014).

[43] Sermo, Sermo, http://www.sermo.com. (Jun 2014).

[44] PEW, PEW Research Center Social Life of Health Information, http://www.pewinternet.org/2013/12/30/demographics-of-key-social-networking-platforms/. (Jun 2014).

[45] Scanfeld, D., Scanfeld, V. and Larson, E. (2010) Dissemination of health information through social networks: Twitter and antibiotics. *American journal of infection control* **38**(3): 182–188.

[46] Afzal, M., Hussain, M., Khan, W., Lee, S. and Ahmad, H. (2012) Social Media Canonicalization in Healthcare: Smart CDSS as an Exemplary Application. In *IEEE 14th Intl. Conf. on e-Health Networking, Applications and Services (HealthCom)*: 419–422.

[47] Martínez-García, A., Moreno-Conde, A., Jódar-Sánchez, F., Leal, S. and Parra, C. (2013) Sharing clinical decisions for multimorbidity case management using social network and open-source tools. *Journal of biomedical informatics* **46**(6): 977–984.

[48] Norval, C., Arnott, J., Hine, N. and Hanson, V. (2011) 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): 492–494.

[49] Jawbone, Jawbone Up, https://jawbone.com/up. (Jun 2014).

[50] Garmin, Garmin, http://connect.garmin.com/en-US/. (Jun 2014).

[51] Shine, Shine, http://www.misfitwearables.com. (Jun 2014).

[52] Basis, Basis, http://www.mybasis.com. (Jun 2014).

[53] AgaMatrix, AgaMatrix, http://agamatrix.com/medical-devices/. (Jun 2014).

[54] Lark, Lark, http://lark.com/Samsung/index2.html. (Jun 2014).

[55] Hong, J. and Langheinrich, M. (2014) Privacy Challenges in Pervasive Computing. *Computing Now* **7**(06).

[56] Christian Payne, How activity trackers remove our rights to our most intimate data, http://www.theguardian.com/technology/2014/jun/03/how-activity-trackers-remove-rights-personal-data. (Jun 2014).

[57] Leo Kelion, Samsung reveals Simband and Sami health platform, http://www.bbc.co.uk/news/technology-27612110. (May 2014).

[58] Jemima Kiss, WWDC 2014: Apple reveals 'Health', its new app for tracking fitness and wellbeing, http://www.theguardian.com/technology/2014/jun/02/apple-reveals-health-its-entry-into-fitness-tracking. (Jun 2014).

[59] Fluxtream, Fluxtream, https://fluxtream.org. (Jun 2014).

[60] Avancha, S., Baxi, A. and Kotz, D. (2012) Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)* **45**(1): 3.

[61] Frain, B. (2012) *Responsive Web Design with HTML5 and CSS3* (Packt Publishing).

[62] Google, GoogleHealth, `http://www.google.com/intl/en_us/health/about/`. (Sep 2013).

[63] Microsoft, Microsoft HealthVault, https://www.healthvault.com/gb/en. (Sep 2013).

[64] Free, C., Phillips, G., Watson, L., Galli, L., Felix, L., Edwards, P., Patel, V. *et al.* (2013) The effectiveness of mobile-health technologies to improve health care service delivery processes: a systematic review and meta-analysis. *PLoS medicine* **10**(1): e1001363.

[65] Mechael, P., Batavia, H., Kaonga, N., Searle, S., Kwan, A., Goldberger, A., Fu, L. *et al.* (2010) *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).

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

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

[68] Detmar, S., Aaronson, N., Wever, L., Muller, M. and Schornagel, J. (2000) How are you feeling? Who wants to know? Patients and oncologists preferences for discussing health-related quality-of-life issues. *Journal of Clinical Oncology* **18**(18): 3295–3301.

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

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

[71] Fox, R., Cooley, J. and Hauswirth, M. (2011) Creating a virtual personal health record using mashups. *Internet Computing, IEEE* **15**(4): 23–30.

[72] Google, Google Charts, https://developers.google.com/chart/. (Jun 2014).

[73] Adams, E., Intwala, M. and Kapadia, A. (2010) MeD-Lights: a usable metaphor for patient controlled access to electronic health records. In *1st ACM Intl. Health Informatics Symp.*: 800–808.

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

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

[76] Thomson Reuters Foundation and TrustLaw Connect (2013) *Patient Privacy in a Mobile World A Framework to Address Privacy Law Issues in Mobile Health* (mHealth Alliance, United Nations Foundation). URL `http://www.mhealthalliance.org/images/content/trustlaw_connect_report.pdf`.

[77] Megalingam, R.K., Radhakrishnan, V., Jacob, D.C., Unnikrishnan, D.K.M. and Sudhakaran, A.K. (2011) Assistive Technology for Elders: Wireless Intelligent Healthcare Gadget. In *2011 IEEE Global Humanitarian Technology Conference (GHTC)*: 296–300.

[78] Kale, A., Kaul, S.K., Das, D.P. and Raghunath, S. (2007) A smart system for remote monitoring of patients and SMS messaging upon critical condition. In *3rd IEEE Intl. Conf. on Wireless Communication and Sensor Networks (WCSN'07)*: 141–144.

[79] Triventi, M., Mattei, E., Censi, F., Calcagnini, G., Strano, S. and Bartolini, P. (2009) A SMS-based Platform for Cardiovascular Tele-monitoring. In *World Congress on Medical Physics and Biomedical Engineering, Munich, Germany* (Springer): 295–298.

[80] Watanabe, H., Kawarasaki, M., Sato, A. and Yoshida, K. (2012) Development of wearable heart disease monitoring and alerting system associated with smartphone. In *14th IEEE Intl. Conf. on e-Health Networking, Applications and Services (HealthCom2012)*: 292–297.

[81] HeartResearch, Heart-Research-Australia, `http://www.heartresearch.com.au/arrhythmias.html`. (May 2013).

[82] Three, Three, https://www.three.co.uk. (Jun 2014).