29

Design Requirements for a Patient Administered Personal Electronic Health Record

Rune Fensli[1], Vladimir Oleshchuk[1], John O'Donoghue[2] and Philip O'Reilly[2]
[1]*Faculty of Engineering and Science, University of Agder, Grimstad*
[2]*Business Information Systems, University College Cork*
[1]*Norway*
[2]*Ireland*

1. Introduction

It is anticipated that the patient's access to his/her own medical records and treatment information in the future will play an important role in managing treatment of chronic diseases and protecting patients' health as described by Coulter et al. (2008). Shared access to electronic health records will thus be important for obtaining electronic collaboration, both for the patient and also for the health care professionals.

The patient empowerment approach as defined by Anderson & Funnell (2009) implies that the patient is capable of managing necessary self-selected changes by recording daily control of (their) his/her illness and rehabilitation. The ability to enter daily recordings of clinical data by the patient will be important in future health care services, where remote home monitoring will be a normal procedure in following up hospital treatment. Such recordings and patient details need to be safely stored within the patient's Electronic Health Record (EHR) system, and they should be shared between the patient and the health care providers. When patients are monitored remotely by means of wearable sensors and communication equipments, recorded information of clinical recordings should be automatically incorporated into EHRs. Such functionality will be important for the doctors to make the more informed diagnosis of the patient's (actual) current condition, and solutions like these can be regarded as an important part of the personalized health care concept.

The Markle Foundation (2003) has defined Personal Health Records (PHR) as:

> *"An electronic application through which individuals can access, manage and share their health information, and that of others whom they are authorized, in a private, secure, and confidential environment."*

The American Medical Informatics Association's College of Medical Informatics has in a strategy for adoption of PHR elaborated on technical architecture and described organizational and behavioural barriers needed to be overcome, as described by Tang et al. (2006). They focused on potential benefits both for the patients and caregivers, but presupposed the systems must be easy to learn and easy to use in order to be used on a daily basis.

According to Hurtado et al. (2000), such patient-centric solutions can be defined as:

> *"Systems that enable a partnership among practitioners, patients, and their families (when appropriate) to ensure that procedures and decisions respect patients' needs and preferences."*

The CEN/ISSS eHealth Standardization Focus Group (2005) has finalized a report addressing future standardization and interoperability in the e-health domain, highlighting the importance of obtaining improved access to clinical records and enabling patient mobility and cross-border access to health care. One proposed action is to establish an EU Health Insurance Card containing a medical emergency data set and the use of this card to control access to the patient's medical record.
There are several barriers to overcome in designing shared PHRs, but new solutions for the patient's access to his/her own PHR are emerging within EU countries. However, in designing new solutions for shared PHR systems, functional requirements from the patient's perspective will probably be a key issue, as the patient will have to realise clear benefits from using such tools in his ongoing communication with the health care personnel. This can be comparable to perceived advantages as from using Internet solutions for private purposes like email and the use of social media.

2. Chapter outline

In this chapter, we analyse the security and privacy requirements of the patient's access to his own PHR, focusing also on patient empowerment and self-care. We analyse the European and US National Health Care strategies. Based on scenarios with a patient-centric view in establishing new services, we propose a solution for a Patient administered Personal electronic Health Record (PaPeHR) service, which would include a cross-country certification of health care personnel in order for patients to receive medical assistance when they are abroad. Some emergency access mechanisms should also be included. Finally, we will highlight some design requirements in order to define roles and support patient´s access to shared information within a collaborative health care framework.

3. Security, privacy and trust requirements

In general, the question of privacy will be one of the fundamental requirements for patients, as the actual solutions can be designed in a way that the patient can be confident in being able to take control of his own private information. Privacy can be defined as:

> *"The right of individual to determine for themselves when, how and to what extent information about them is communicated to others";* Agrawal et al. (2002).

As Tang et al. (2006) focused on the ability for the patient to define which part of the information stored in the PHR is to be shared by others, this is in fact a question of privacy regulation in the actual solution. There are several privacy-aware solutions offered on the market, such as the iHealthRecord[1], PatientSite[2], Microsoft HealthVault[3] and Google Health[4]. However, most of those solutions differ on conceptual levels and are based on proprietary standards, making trans-institutional data exchange difficult. When making a decision on which solution to choose, the patient will also have to evaluate the trustworthiness of the company offering a secure solution for life-long storage of life-critical medical information. In many countries you will probably not trust a foreign private

[1] http://www.ihealthrecord.org
[2] http://www.patientsite.org/
[3] http://www.healthvault.com/
[4] http://www.google.com/health/

company; however, you will trust your bank manager when it comes to your net-bank account. In the same manner, you will have to trust your net-health account, and regarding privacy you will be certain that the data storage is preserved in a safe and secure place, where you are the only person managing this account and where only you can control which persons are given access to the information stored.

It is a challenging task to define shared access to the PHR information based on concept of roles defined by Role-Based Access Control (RBAC) which typically are incorporated into the design of EHR-systems used in hospitals and health care services. RBAC is a concept where access to data is restricted to authorized users, and where the actual person's functional role within the organization will determine which part of the information he is authorized to access, as defined by the standard ANSI/INCITS 359-2004 (2004).

Such solutions will first of all require a well defined structure of information in different types, each with different needs of shared access; thus the RBAC solutions have a need of including granulated context aware RBAC. In addition, there should be possibilities of defining generic roles, as typically will be your local doctor or general practitioner, your home nurse (which will be a role shared by many nurses), your spouse/next of kin, persons in your health exercise group etc. Any solution will require the secure identification of all healthcare personnel, and many countries have established a common name-space with a central storage of this public information. However, the secure identification of informal caregivers (voluntary resources) and family members can be a challenging task.

Assuming that the patient is the owner of his/her own PHRs, he/she will need to ensure the integrity of the system; thus he/she will be the responsible person for the data integrity and confidentiality. This (will have the implications) implies that the patient will need to have the administrative privileges of assigning roles and access to the information stored within the PHRs. This will, in fact, be a Patient administered Personal Electronic Health Record (PaPeHR). In such a new concept the challenge will be to design the administrative part of the RBAC interface in a simple and intuitive way, enabling the patient to perform the role of system administrator without making any mistakes. This will be a question of human interface design, but depending on computer skills, probably not all patients can take the responsibility on their own. If a system facilitator is needed in helping the patient with the system setup and assigning roles, this facilitator role should not have access to stored medical information. Technically, this can be solved in a front-end/ back-end solution. However, the facilitator role will be crucial when it comes to privacy issues.

Many proposed solutions only slightly approach security and even less privacy issues. For example, an architecture proposed by Vogel et al. (2006) for distributed national electronic health record system in Austria stated that:

> *"The privacy of patient related data is temporary solved in a way that participating institutions are bound by contract to only access data relevant for specific treatment case"* [page 5].

This is not a technological solution. It is more a question of agreed policy, and should generally not be considered a sufficient protection of patient privacy (otherwise the privacy protection problem would already be solved, since current privacy related legislation requires similar protection of patient data in most countries). Some other approaches focus more on security issues and partly mixing them with privacy issues, and it is important to be aware of the fact that high degree of security does not necessarily protect data privacy.

From the definition of privacy, it is easy to see that perfectly secured data does not necessarily provide protection of patient privacy, as there may not be implemented solutions for the patient's access control. It should be mentioned that in a real-life situation

the above definition of privacy can be ensured by claiming individual may be replaced by any entity (such other individuals or organizations) he/she has sufficient level of trust to. The relaxation was implicitly made in many approaches proposed in the literature, and is described in a global perspective by HiMSS (August 2008). However, it poses another issue associated with correctly assessing trust relations in an ad hoc setting (for example when a patient is abroad on holiday etc.). This is a reason that many proposed frameworks require the availability of a special infrastructure such as for example PKI, digital certificates, health cards, etc., and these may be difficult to implement in cross-border settings. Generally, providing privacy protection is more difficult than providing security of patient data. In some cases it can be contradictory, for example when patient privacy is based on anonymity.

4. Patient empowerment and self-care

In health care services today, there is an increased awareness of patient empowerment. The term "Patient empowerment" implies that the patient should have gained knowledge about his own health and illness, and can be able to make decisions of actual treatment and self care. This is not about "doing something for the patient", but facilitating and supporting patients to understand the consequences of their decisions. There are several relevant papers that describe the understanding of patient empowerment. One example is the WHO report written by Anderson & Funnell (2009) and Coulter et al. (2008) where the situation for patients and decision making is described.

Chronically ill patients experience a greater degree of freedom and are more involved in the treatment with daily monitoring of vital information during hospitalization in their own home, than with the traditional treatment procedures at a hospital. Introducing advanced medical technology in the patient's own home will influence the patient's situation as it makes empowerment and self-management possible as described by Barlow et al. (2002). At the same time, coordinated follow-up and new workflow procedures for the health-care services need to be implemented in order to give the patient satisfactory support by virtual visits in his/her home, which was put in focus by Wootton & Kvedar (2006). However, this support also must be integrated in the self-monitoring of vital signs information performed by the patients, with understandable interpretations of the results.

In an evaluation by Wald et al. (2007) of the physician – patient relationship, it was found that the impact of Internet use with possibilities of collaborative teamwork approach and access to the patient's own health information were effective and contributing to quality of health care. Weingart et al. (2006) evaluated patients who used the PatientSite, and they discovered a steady growth of use after the introduction, by typically younger patients with few medical problems. But to expand the use of patient portals it is important to overcome obstacles for those patients who might benefit most from this technology, as they will probably be the first users of the new system.

In a review analyzing potential benefits and drawbacks of patients' access to PHR, Ross & Lin (2003) found improved communication between patient and doctor, improved patient empowerment and improved education. However, this can require a fundamental redesign of the health care process, with full electronic integration and communication with patient-centric applications for disease management and prevention, as Demiris et al. (2008) are pinpointing. When designing such solutions, the patients will probably expect a quick feedback from the doctor to recorded event situations or messages requesting for advice; thus a reliable workflow and defined response times should be defined according to Fensli & Boisen (2008).

As the health care personnel normally will be using secure solutions within a national health care framework, there is a need to establish secure communication and exchange solutions crosswise health network borders. At the same time, the patient should be able to participate in a training group for patients with the same diseases, as the encouragement from other patients will have a positive impact. This should imply functionality known from social media, with shared training results, questions and answers, blogs. Such functionalities are well known from most weight watcher programmes found on the Internet, but are rarely used within a health care and rehabilitation domain.

Today, many athletes are using a pulse watch during their regular training. This watch enables them to share their achieved results with training partners on the web, and even as a virtual competition. Grimsmo et al. (2010) found that prevalence of atrial fibrillation is increased for middle-aged over-trained athletes, and the next thing they will have to do will be sharing their training records also with the doctor. However, being able to distinguish between different security needs can be a challenging factor for patients in their role as system administrators, defining the actual roles and access to different types of information.

5. European and US national health care strategies

5.1 Core electronic health records

Within a national health network, mechanisms for secure transfer of clinical information are in many countries established between hospitals and General Practitioners (GP), and also with the local municipal health care services, based on different infrastructure principles and secure message exchange.

In Denmark, the Danish eHealth Portal, sundhed.dk (2010), is designed to give the patients on-line access to their personal health data with the medical history from Danish hospitals, including e-Journal and Medicine profile. In addition, the health professionals can get access to a summary of the patient's electronic health record.

In Norway, a patient portal "Min journal" is established by Oslo University Hospital, in close collaboration with a number of hospitals and rehabilitation clinics. A secure electronic ID is used for authentication of the patient, and he/she will have access to secure message exchange with the health care services. The patient will also have an overview of the medical prescriptions and epicrisis from the hospital. Such solutions can be classified as a patient portal approach, with access to the health systems owned by the providers.

In Scotland, the National Health Services (NHS) has established a common Core-Electronic Health record, The Emergency Care Summary; to be accessed by all health care services within the country. However, up until now the patients are yet not given access to this solution as described in the report by The Scottish Government (2006).

Within The UK, the Healthspace portal operated by the NHS enables the patients to view their Summary Care Record (SCR) and to book a hospital appointment as described by the UK National Health Service (2008). Within the HealthSpace portal, patients can manage their own health and lifestyle information. By having an account, the patients can fill in important information about their health details; keep a record of their own medication, daily intake of alcohol, smoking and calorie, and also monitor blood pressure and fitness recordings.

In order to establish a common database of patient information to be shared between health care professionals, several European countries have focused on defining a common shared EHR, summarized by the CEN/ISSS eHealth Standardization Focus Group (2005).

Within several European countries, efforts have also been made to define a core dataset for public health, "Core-EHR", where a minimum common dataset of important clinical information can be securely stored and shared among health care professionals at different administrative levels. In the EU report "Connected Health", the European Commission (2006) has described the term Patient Summary as (p 13):

> *"A clinical document that is stored in repositories with cumulative indexing systems and secure access by authorized people. In order to achieve maximum benefit from this instrument, the structured content of patient summaries should be agreed at an international level, starting from a few generic summaries and gradually developing a series of summaries specific for each clinical context."* (Citation from an eHealth ERA coordination action deliverable)

In the report, three specific topics are considered as prioritized activities, namely a proposal of requirements of interoperability of patient summaries, patient and health practitioner identifiers and an emergency data set incorporated in the patient summary. This summary of important medical information will typically include a summary of patient history, a list of allergies, active problems still under treatment, recent test results and a medication list. In addition, the eHealth action plan as a strategy from the Commission (2004) addressed the question of ePrescribing, in the future this can give possibilities for cross-border prescriptions when patients are abroad on holiday etc.

5.2 Different approaches for patients' access

In the description of how different countries have approached the acceptance, adoption, deployment, operation and support of a national EHR solution, a HiMSS (August 2008) Steering Committee has defined four architectural models to describe how the ownership of the patient records are organized, and whether or not a country allows for EHRs to be accessed by patients.

These four approaches are as follows: 1) A Fully Federated model where the data remain in the source systems; 2) A Federated model where patient data are consolidated with source facility in a clinical document record; 3) A Service Oriented model where patient data are sent to a central EHR by messaging, and where the patient can get access to the events registered in the system, and 4) An Integrated EHR model with a single integrated hospital system where the patients can get access through embedded capabilities. To this list, a fifth model should be added as a privately owned standalone PHR as listed in Table 1.

EHR Approach	National health care strategies
#1 Fully Federated	U.S.
#2 Federated	Netherlands, Wales
#3 Service Oriented	Germany, Denmark, Israel, New Zealand
#4 Integrated EHR	England, Canada
#5 Standalone PHR	None (only private initiatives)

Table 1. Models of approaches to EHR solutions within national health care strategies based on HiMSS (August 2008), with addition of a private standalone PHR solution

In the different strategies to adopt PHR solutions, we have described the range of complexity for a PHR either as a stand-alone application or fully integrated so that patients can view their own information stored in the EHR system at the health care provider. As a minimum requirement, there is a need to export and import data from other systems in a standardized way, and in future solutions there should be seamlessly interoperable systems

as described by Tang et al. (2006). In this paper, they also highlighted the potential benefits for the consumers having a PHR.

Patient's access to their doctor's EHR system has been developed as a web-based service proposed by Cimino et al. (2002), demonstrating that patients gain an improved understanding of their health and that such systems can have beneficial effects on health outcomes where patients and doctors can have a shared workload and a better communication. An e-consent based solution to share the EHR between the patient and health care personnel has been suggested by Bergmann et al. (2007) as a virtual shared EHR and with the use of an e-consent object based on digital signatures for authorized access to the patient's shared her. However, the formal requirements can be difficult to implement in cross-border solutions.

An architecture for a patient-centred shared electronic health record using a Medical Data GRIDs[5] as an open source implementation has been suggested by Vogel et al. (2006). This solution enables the patient to give a fine grained permission to access specific parts of the record. A distributed service using roles defined by the e-Health directory was implemented, and authentication was based on digital certificates. It can also be possible to establish an independent service as a health record data bank, described by Shabo (2006), into which the actual health care providers will have to submit the desired content.

An interesting show-case with two clinical scenarios was developed using a patient-centred approach which demonstrated integration of a PHR to a healthcare enterprise, based on a Cross-enterprise Document Sharing (XDS) profile implemented in a ebXML architecture, as described by Stolyar et al. (2006). In this way metadata were used as index to locate the actual health information stored within a regional health information network.

There is a need to clarify actual standards suitable for integration of information, and how patient-entered data, including vital signs recordings and fitness and lifestyle details can be shared between the patient, his/her relatives, training partners and the health care professionals. In order to adopt a solution to be used in broad scale, it can be beneficial to use open standards in the infrastructure framework, thus different vendors can easily adopt their systems to be used within a national health care data network designed to share information among different applications and clinical tools. The standardization issues are addressed in a joint project on interoperability of eHealth standards organized by NEN (2009), and a final report, M403 Phase 1, was in February 2009 submitted to the European Commission for formal approval.

However, as pinpointed by Kahn et al. (2009) the existing gap between today's PHRs solutions and what integrated services patients say they want and need, is a limiting factor in the adoption. It is also important to keep in mind that Kahn et al. (2009) unveiled that the patients are concerned about security and privacy issues. To summarise, this review reveals that no simple way exists for the patient to gain control of the consent rights given in the EHR approach models #1 to #4. Nor is a proper model for data access in emergency situations proposed.

6. Scenario with remote home monitoring

6.1 Information flow

When defining a framework for information flow, storage and retrieval, it is necessary to focus on the (actual) system users and their responsibility. Putting the patient in focus can

[5] GRID computing is combining resources from multiple of distributed computers

give a perspective where the important information flow and responsibility for the different health care professionals can be identified. A typical scenario may be the situation which is shown in Figure.1, where a patient's vital signs are monitored during his/her outdoor walk. The electrocardiogram (ECG) signals are automatically transmitted to the patients PaPeHR using secure mobile data communication (1).

If an arrhythmia situation is detected, this information can be transmitted to the local doctor/General Practitioner (2) to be prepared and preliminary evaluated by the care coordinator for a quick focus on important findings. This can be timesaving for the doctor's evaluation to determine appropriate interventions. As he may not have necessary cardiology competence, he can forward the arrhythmia event to a specialist at the hospital as a telemedicine referral (3). Depending on the epicrisis received (4), he can both send a message to the home nurse for necessary follow up (5) and inform the patient (6). All the information on the arrhythmia event recorded data, referral, epicrisis and messages should be properly stored within the patients PaPeHR (7).

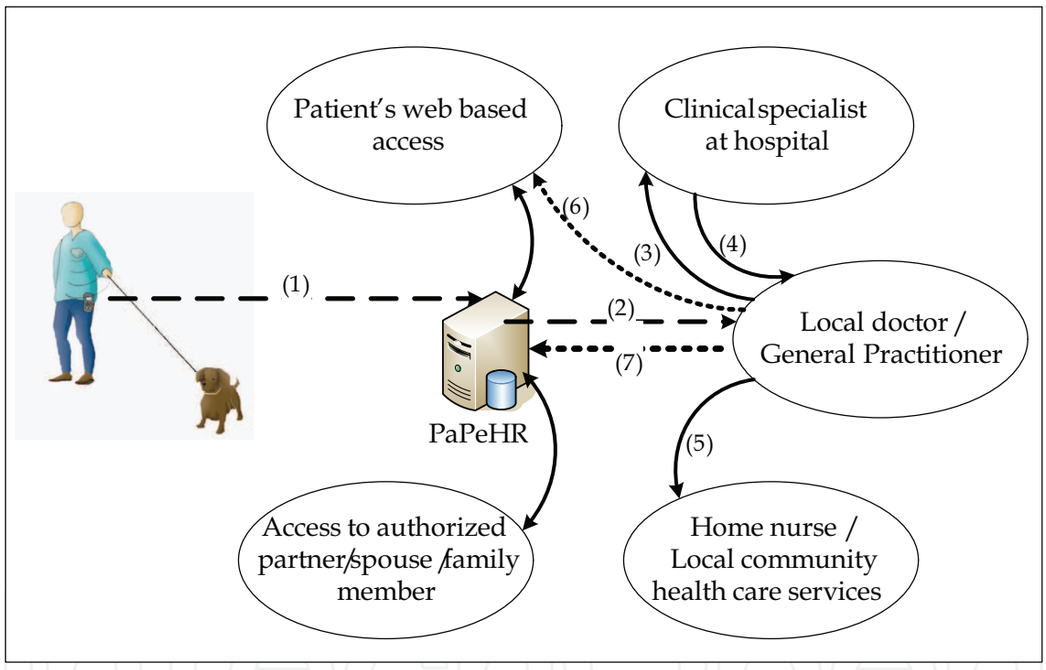

Fig. 1. The principle information flow (1-6) between the patient, the local doctor, the clinical specialist and the home nurse, in response to a detected cardiac event. The patient should also have online access to his own PaPeHR to update actual information and read the feedback from his doctor (7). In addition, the patient should have possibilities to define access to his partner/spouse/family member

Of course, a detailed log will record any access to the stored information, in order for the patient to have an overview of what has been read or evaluated by the health care personnel and other persons given access privileges. As the patient may have consented to allow family members to access actual parts of the information stored, there will be a need of RBAC mechanisms to control the privacy as described in section 3.

The patient should not need to worry about security issues; however, he/she would need to trust the organization or company offering the PaPeHR solution. Preferably, this could be a

well known public service in the country, but it could be anyone offering a reliable and easy to use solution as a trusted third party. This principle is well known for security systems when it comes to offering digital ID's (normally private companies), secure net bank accounts, secure payment solutions, secure storage of private information like family photos, and others.

6.2 Integration of remote monitoring

When patients are monitored remotely by wearable sensors and communication equipments, the automatically recorded information is important for the doctors to make the correct diagnosis of the patient's current situation, and it is an important part of the personalized health care concept as described by Aziz et al. (2008). Several wearable vital signs recording solutions have been developed, with different aspects of how to record and transfer such information. In an overview and an evaluation of different telecom solutions for remote cardiac patients it is suggested by Kumar et al. (2008) that next-generation telecardiology network architecture should incorporate a signal processing module for local analysis of recorded physiological measurements. Preferably, it should only transmit to the doctor detected events where recorded data are out of defined thresholds values. The systems should be able to use multiple wireless interfaces and include location-based services.
Fensli et al. (2005) and Dagtas et al. (2008) have proposed a local signal processing solution and transmission of periodic reports with detected alerts to a central server as an entry point for the professional staff to monitor the recorded data.. Similarly, a remote diagnostic system which integrates digital telemetry using a wireless patient module, a homecare station and a remote clinical station has been developed by Kong et al. (2000). However, none of those solutions discussed how the recorded information at the central server can be stored securely within a patient EHR or PHR framework.
Telemedical solutions have been used in several interesting projects to evaluate patient outcome, and the Airmed-Cardio project described by Salvador et al. (2005) showed the importance of enabling patients with chronic heart disease perform out-of-hospital follow-up and monitoring, where they developed a dedicated platform for necessary measurements and contact between the patients and the health care agents. However, the platform used was not integrated into the patients EHR system. A clear outcome effects of a home-based tele-cardiology service has been verified by Scalvini et al. (2005), where the patients' ECG recordings automatically were transmitted to a receiving station available for trained nurses (telemonitoring), also this solution was a stand-alone receiving database.
In a report on remote monitoring, the U.S. Department of Health and Human Services has described use cases to define possible solutions for information exchange and integration of patient-monitored data into a national health information technology (U.S. Dept of Health and Human Services (2008). This report highlights the importance of a clinician to monitor patient information captured remotely in management of chronic health problems and to diagnose new conditions. Such measurements can include physiologic measurements, diagnostic measurements, medication tracking and activities of daily living measurements. However, common data standards and interoperability are necessary to establish a pathway to incorporate the remotely monitored information into EHRs and PHRs, and they defined a data intermediary into which a remote device could be able to exchange and store information and where privacy controls and restrict data access mechanisms were incorporated. One of the important problems discovered, was a lack of standardized interface and interoperable data, giving restrictions when trying to integrate remote

monitored data into the EHRs and PHRs. In use cases describing exchange of measurements between patients' monitoring device and their clinicians, they described three different roles and functions: *The Clinician* (personnel who clinically evaluate the remote measurements in the EHR and determine appropriate interventions), *Care Coordinator* (clinically-trained individuals who monitor the information received from the patient's device and assist the patient and/or clinician in managing the remote monitoring information) and the *Patient* (including family caregivers who use a remote monitoring device to gather measurements). From the data intermediary, persons with the defined role could be given controlled access to information by a web-based portal, and decision support capabilities should be incorporated to generate alerts and communicate information to the EHR or PHR reaching threshold values in the remote monitored data.

6.3 Daily use of a PaPeHR solution in patient's self care

In the patient's daily use of his/her PaPeHR, he/she should have access to a variety of information like general health status, care plan, medication list, allergies, doctor's journal record documents, medical advises, vital signs recorded, a calendar with scheduled actions and visits to the doctor and health care personnel, in addition to the ability to write a medical diary to follow up the planned treatment and exercises. The vital signs can, upon the doctor's request, be a combination of physiological measurements either done automatically by wearable sensors, or manually by reading the values of the recording instrument and uploading the measurements via web-based interface. Such information can be physiological measurements (e.g. blood pressure, blood glucose, INR-values), diagnostic activities of daily living, drug intake, food, performed exercise (including use of step counters etc.). As the patient normally will have the ability to freely move around, most of the automatic recordings should preferably be based on secure mobile communication solutions. Also manually entered data should be able to be uploaded from a mobile device, and in a web-based solution this should be available from an ordinary mobile phone with secure data transfer.

One important aspect to the patient will be to have a quick response from the health care personnel in case of abnormal recordings. This could be values outside threshold limits, and may indicate an action from the patient or a health care intervention. Thus necessary alert mechanisms should be incorporated with an automated tracking of actions and responses, including a system for escalating the case to a more urgent action if needed. However, automatic escalation may involve giving access to information by other health care personnel as the emergency response team as proposed by Hansen & Fensli (2006). It can be difficult to predict such needs, thus the rescuing team may not be registered with access permissions, and there will be a need to incorporate emergency access solutions as described by Oleshchuk & Fensli (2010).

There may be a need of access from the patient's close relatives/spouse/next of kin/family members, depending on the patient's mental condition and need of help controlling his treatment and follow up. Such assistance can also be the case for patients with dementia, where the question of location tracking by use of global positioning systems (GPS) also will imply ethical issues and legal issues for this specific use of tracking persons. In order for health care personnel to access data of position, there should be an automatic logging of this access, together with a written report describing the need of access in this particular situation.

The patient's use of social media will imply sharing actual experiences with others and supporting and encouraging friends in their coping with illness. Some information can be

freely shared on the web as is the case using Facebook, Twitter or similar media. However, we will recommend defining a secure social portal, where the patient easily can add friends with a proper sign-on for them to get access to the shared information. Thus, this portal can be a front-end of a PaPeHR with secure Internet access, while at the same time the back-end services should be integrated within a secure national health network.

6.4 Special attentions and emergency situations

Several emergency situations can require special attention. In an acute situation the system should automatically detect the change in the patient's situation, and perform an escalation of the access rights for the parties involved (in case of emergency event). As proposed by Ferreira et al. (2009) the "Break The Glass" policies are flexible and allow users to override the defined access policies in a controlled manner. Within health care services such "Blue Light" access situations can occur, but it can be necessary to know the exact location of the patient and a Spatial Role Based Access Control system can be useful as proposed by Hansen & Fensli (2006).

If the patient is able to control the access by others to his PHR-information, this will normally be based on informed consent. In situations where there is a change in the health care personnel normally taking care of the patient, he/she should give new permissions to new persons, either as one-time access, temporarily access (limited time) or as permanent access (shift in the staff). There might also be situations where the patient is transferred to a hospital for treatment, and where he/she will not be able to distinguish between the actual personnel/staff; so the permissions can be given to the hospital as an institution (and not defined persons). Thus it will require some infrastructure to be able to identify and authenticate the actual hospital personnel responsible for the treatment. Such role-based access can be achieved by establishing a Public Key Infrastructure (PKI) using digital IDs, and preferably there will be a public name-space within a secure national health network to identify both hospitals as organizations, as well as all registered authorized health care personnel.

In an emergency situation, the patient may be unconscious and therefore not able to give the required permissions. As such, there should be defined ad-hoc read-only access by authenticated doctors in order to get access to important life-threatening information as the Patient Summary with the medication list. In fact, this could preferably be the patient's Core-EHR, where the patient summary is safely stored within a national health network, as is the case in Scotland electronic patient record system. Furthermore, when the patient is travelling abroad, situations can occur where there is a need of local treatment; thus the access possibilities should be based on an international cross-identification infrastructure to allow cross countries data exchange.

7. Design requirements

Based on the scenario with important aspects of the PaPeHR use, some fundamental basis of requirements can be stated which should be implemented in a future solution. It can be useful to separate the list in functional and non-functional requirements as defined in Table 2 and 3, in which the necessary privacy and security mechanism are defined. As the system should be easy to use for persons with relatively low computer competence, the actual solutions will require a good interface, with universal design and according to use for persons with disabilities. The Web Content Accessibility Guidelines published by W3C

(1999), gives recommendations for how to make the web content accessible for people with disabilities, but will also be useful guidelines when developing web content for all users. In order to evaluate a web site for accessibility, a multi-page resource suite is also published by the Web Accessibility Initiative, W3C (2008).

7.1 Suggested implementations

This approach will protect patient privacy by means of providing control of access to their PaPeHR. Having control of access to his/her own PaPeHR means that the patient would be able to provide access to stored data to any nominated medical practitioner, anytime and anywhere. Therefore only systems with patient-controlled access can be considered as adequately protecting patient privacy. Thus comparing five approaches to EHR system design (presented at Table 1) we purport that at present only a Standalone PHR (Approach #5) gives adequate protection of patient privacy. Three approaches (fully federated, federated and service oriented, see Table 1) implicitly assume that a trust relation with users exist. These three approaches are mostly suitable and designed to secure the EHR solution, and not to protect patient's EHR privacy. This will also be the case for the fourth model (integrated EPR), where the patient's influence on access permissions is not implemented.

The approach based on patient-controlled access can easily be extended to give patients an opportunity to continuously update their health-related data by uploading new data collected privately by body area networks (BAN) or Body Sensors Networks (BSN) on the regular base when monitoring vital signs data in the course of daily activities, for example jogging. It will be more important in the future when such body area networks will wide-spread and can be used for continuous monitoring of patients' health conditions (especially chronic patients), and where the recorded information can be used later by medical practitioners to provide more specific health care and optimize number and time used to visits medical practitioners. It can also be related to lifelong EHR, as defined by Shabo (2006). However, handling of special emergency situations when the patient is unconscious or unable to grant access for some other reason should also be included in such system. In this case a verifiable trusted representative should be able to grant such permission.

In the following section we will describe a solution that enforces patients' control of their PaPeHR. We assume that there is a database (distributed or on a single server) that contains PaPeHRs of patients and which can be accessed via the internet. This patient wants to be able to both download and upload data to the database. The patient will need the ability to control access to these data by granting and revocation of access permissions to his PaPeHR. They want to be able to grant ad hoc access to these datasets from a specific computer, to specific records for example in the case of visit to a medical practitioner aboard, while on vacation.

We assume that a patient can securely log on the web site that is at the front-end of his/her personal PaPeHR system and can be accessed from anywhere where Internet access is available. The patient can use available authentication methods (password, smartcard, token, biometrics, etc.) to be authenticated. Through this webpage the patient can administrate permissions that other individuals can have with respect to his PaPeHR, as described by Tang et al. (2006). The patient can register new users and define their permissions with respect to their PaPeHR (such as read, write, update, print etc). Such users can for example be family members, friends, medical practitioners, etc. In this way the patient serves as a security administrator with respect to their PaPeHR.

Functional requirements	
Situations / activities	**Actual functions and requirements**
Remote monitoring from patient's vital signs data (automatically upload of recorded data)	
• Physiological measurements • Activities of daily living measurements • Automatic detection of alarms	• Secure transfer from the patient's HUB to the intermediary/Gateway for data upload • Data formats according to open standards
Patient entered vital signs data (manually upload of recorded data)	
• Medical diary information • Drug intake and medications • Follow up activities in the care plan • Feelings, behaviour, well-being	• Web-based schema incorporated into PaPeHR • Data formats according to open standards • Directly integrated into the Core-EHR database • Internet-based frontend/secure social media
Patient Privacy	
• The patient should be responsible for his own PaPeHR and permissions given • Define authorization – access to different types of information/persons	• Delegation of access based on roles • Role based delegation to authorized health care organisations (home nurse, hospitals etc) • Incorporate a "blue-light" emergency access
Sealed sensitive information	
• In situations when the patient should not be able to read his doctors evaluation	• The patient can give access permissions to other defined clinicians
Basic Core EHR information according to defined standardized regulations	
• Important info in case of emergencies • Name and address to regularly used health care services in case of more information is needed	• Personalia • Current health status Medication list • Allergies • Regular health care services used
Tele-home-care services	
• Patients self-care • e-Communication with the health care services	• Data formats according to open standards • Secure transfer from the patient's mobile phone with web-based solutions
Secure location based tracking (GPS) of patients position	
• Need of finding patients with dementia not finding their way back home • In case of emergency situations, rescue team will need to locate the patient	• Trusted services authorized only when needed • Automatic logging of events • Written reports describing the actual need of access in each cases
Limited access when change in health care personnel and in emergencies	
• Transferral to another hospital • Staying abroad /on holiday • Unconscious patient	• New limited permissions should easily be given • Cross boarder identification personnel/hospitals • Ad-hock read only permissions to Core-EHR

Table 2. Specifications of functional requirements with important situations and activities, and the corresponding functions and requirements for a future PaPeHR

Non-functional requirements	
Situations / activities	**Actual functions and requirements**
Integration of Core-EHR information with other EHR integrations	
• The Core-EHR should automatically be updated after a doctor's visit or hospital treatment	• Export and import of data to other EHR systems • Indexes to locate more detailed information stored within national health information EHRs
Patient's transparent access to Core-EHR information	
• Update personalia • View medication list etc	• Direct integration with the Core-EHR located within a national health network
Front-end / back-end solution with security	
• Internet-available front-end with secure logon for actual users • Secure back-end service for all health care personnel and institutions	• Separated database solution • Dedicated AAA for secure logon • Access to a national namespace • Transparent service for the patient
Cross country integration	
• Patients mobility and travel abroad still being able to use the PaPeHR • Need of temporary access abroad	• National namespaces should be available • Standardization of access, information, data formats, etc.
Secure authentication	
• All persons given access should be authorized based on secure authentication • Automatic functions without the need of computer skills for the patient to define	• Two-factor authentication based on a PKI infrastructure or similar solution • Establish a digital ID for patients and health care personnel according to national standards
Secure and trusted longitudinal storage of data for a patient's lifetime	
• Based on the patient's privacy issues • The patient must be the "owner" of his PaPeHR and have fully control • Several solutions should compete the market (both private and public)	• Trusted third party services authorized by national authorities • Preferably established within the security of national health networks • Encryption of stored information

Table 3. Specifications of non-functional requirements with important situations and activities, and the corresponding functions and requirements for a future PaPeHR

In the architecture presented in Fig. 2, showing principles of the security design, a patient can log on AAA (authentication, authorization and accounting) server via web-based interface to assign permissions to other users he/she wants to give access to the PaPeHR. To simplify such permission administration we propose to use Role-Based Access Control principles as described by Ferraiolo et al. (2003), Hansen & Oleshchuk (2003) and Hansen & Oleshchuk (2006). In such systems there is a set of predefined roles e.g. *general practitioner*, *cardiologist*, *wife*, *parents*, *children*, etc with permissions defined according to law and regulations. In addition, a patient may prefer to define new roles that can be applied after testing on conformance with secure identification.

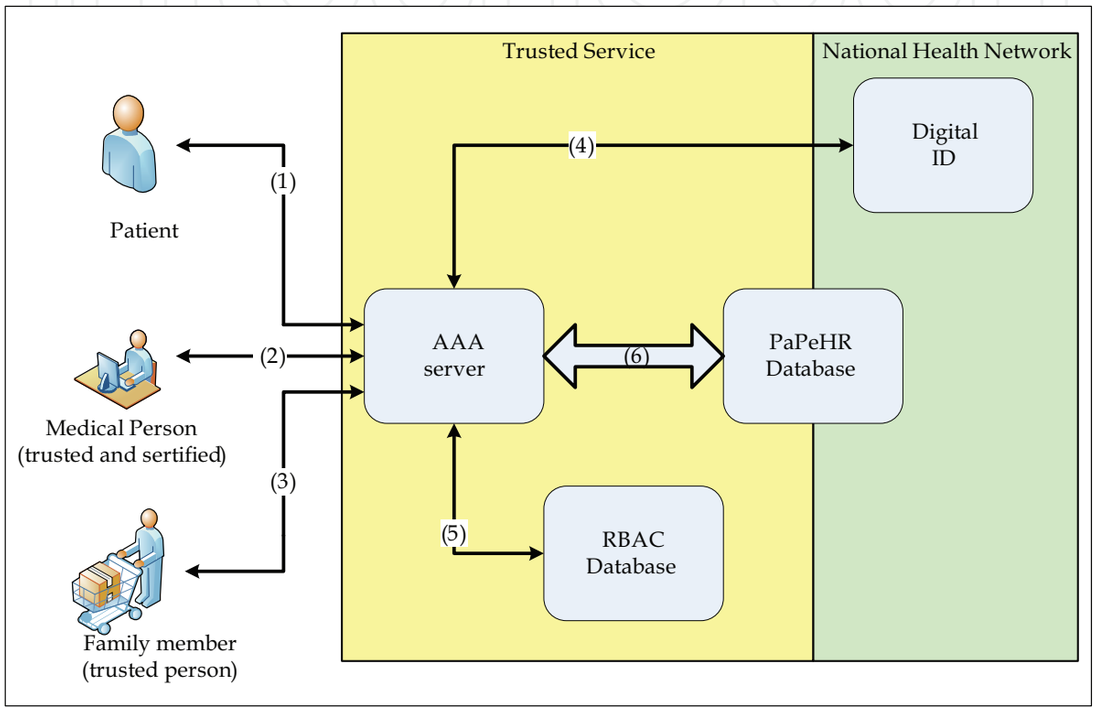

Fig. 2. Patient controlled acces to a PaPeHR, where a front-end Trusted Service is available from the Internet and with a back-end service within a secure National Health Network. The Patient (1), trusted and sertified Medical Person (2) and trusted Family Member (3) can log onto the system. After secure logon according to digital ID permissions (4) and granting the roles and access rights from the RBAC Database (5), the person is given access to the PaPeHR database (6)

As outlined in Fig. 2, the patient (1), trusted and sertified medical persons (2) and trusted family members (3) can log onto the system. After secure logon according to digital ID permissions (4) and granting the roles and access rights from the RBAC Database (5), the person is given access to the PaPeHR database (6).

By registering new users the patient will define the authentication method of these new users and their permissions and constraints with respect to his/her personal PaPeHR. It can be done by assigning corresponding roles such as MD, family member etc. The set of role templates should be pre-defined and available on AAA server. However, roles with critical permissions (for example, right to prescribe medications) should be assigned only to authorized personnel. This will be done by verifying user identity in Health personal

namespace before the role will be assigned. Roles associated with limited set of permissions may be assigned on the base of the patient's trust to this user.
By registering a new user the patient selects user name and password, and their delivery method (delivered personally by the patient, via SMS to new user's mobile phone, by email, etc). After registration and role assignment all users are able to access the patient's PaPeHR directly via the Internet after authentication and according to assigned roles. Note that currently in a majority of the solutions protection of patient privacy is based on the assumption of trust by patients that their data will not be misused. However, the experience from real life shows that it is not the case (see for example a list of privacy related accidents in Appendix A in a description of Hippocratic Databases by Agrawal et al. (2002)). Therefore an approach based on patient controlled access described in this section can be considered as a sound solution that gives real privacy protection.
It should also be possible to have a dedicated role that can be used only to administrate access to the patient's PaPeHR on behalf of the patient. It can be assigned by the patient to any trusted person for some period of time (for example, due to the patient's health conditions). This administrative access should only have access to the AAA service defining permissions in the RBAC Permission Database, and not to the content stored within the PaPeHR database.
However, as the patient's PaPeHR should be securely stored for a lifelong period, integration with health care services is preferable; the PaPeHR solution should not be a stand-alone database but integrated into the national health care service. There should be a seamless integration of the patient's Core-EHR, transparent to the user, with actual access permissions.
Based on those assumptions, we recommend system architecture as shown in Fig. 3, where the Personal National Electronic Health Record (PNEHR) is securely established within a national health network service as an encrypted database. This database should consist of two different but integrated parts: the Spine/Core EHR and a database containing the raw data uploaded from the remote vital signs recording equipments. In principal, this model is based on the architecture for the English National Health Services, where the PRIMIS+ (2009) service (Primary Care Information Services) is established with defined standards for recording and exchange of health data.

7.2 Remote home monitoring

A remote Electrocardiography (ECG) monitoring system has been developed, and designed to be integrated into the PaPeHR framework as proposed by Fensli et al. (2005). The principles for a secure infrastructure with transfer of the patient's recorded information and mechanisms for exchange of information between health care professionals need to be established, in order to make the necessary interpretation and patient intervention as a response to the recorded vital signs information with detected arrhythmia events.
We will focus on how the patients can define and control access to share the recorded information with health care professionals, both on a daily basis and as ad-hoc access in case of emergencies. This solution should be an integrated part of the patient's PaPeHR and integrated in a shared "Core-EHR" solution where security and privacy issues are well defined and implemented. When measuring vital sign information, this should preferably be according to an international standard data format, and not as of today with mostly proprietary data formats used in the different products available on the market. If the remote monitoring system is measuring ECG signals, there exist several international

standards. However, their capability of being used in a telemedicine context differs. For a near real-time ECG recording solution, it should be possible to record files containing a defined duration of the ECG signal sequence, and transfer these files from the patient worn HUB or mobile Hand Held Device (HHD) to the PaPeHR system.

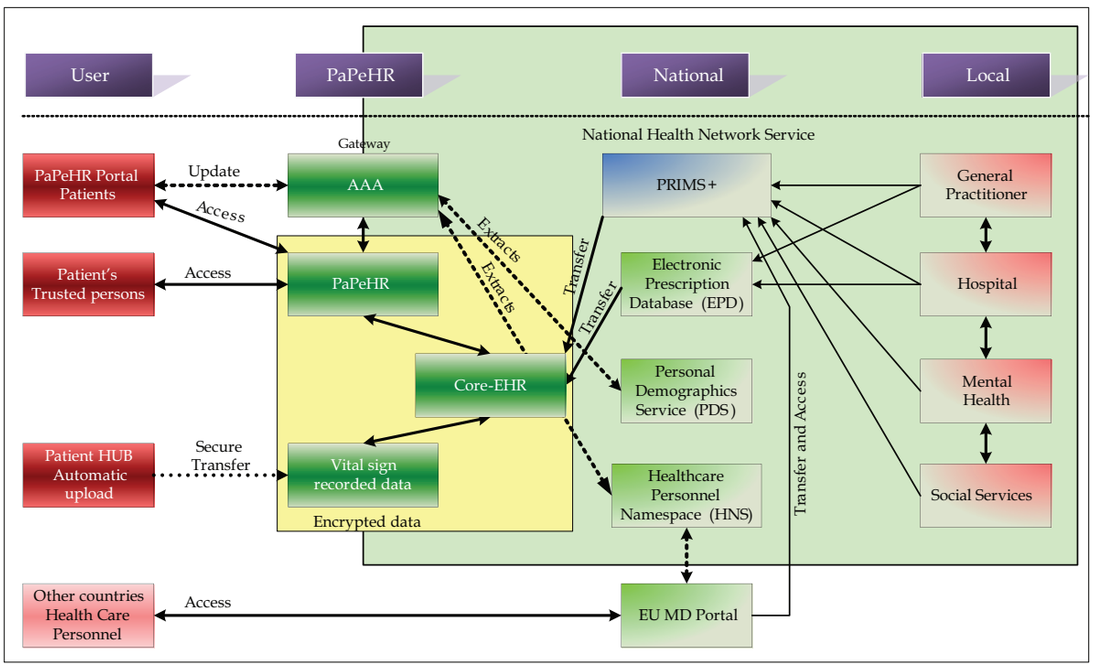

Fig. 3. Principles for a Patient administered Personal electronic Health Record (PaPeHR) service implemented within the framework of a National Health Network. In order to give emergency medical assistance for patients travelling abroad, an EU MD portal is proposed as a standardized gateway into the actual national framework

In the European drafted standard CEN ENV 1064, known as the Standard Communications Protocol for Computer - Assisted Electrocardiography (SCP-ECG), CEN/TC 251 Working Group IV (2006), specifications are given for transferring ECG reports and data from a vendor's ECG recorder to a central management system. In the specification and structure of the data content, it has the intention of being a general and interoperable standard. It is, however, not intended to be used for long-term ECG recordings as an ambulatory "Holter recorder" as may be the case for remote home monitoring solutions. The standard describes a binary file structure, and compression algorithms are used for the ECG signal representation. Because of the file compression methods used in the SCP-ECG format, the file size is relatively small, and could easily be sent from one hospital to another as a secure message within a National Health Network.

The described standard for medical waveform format encoding rules, MFER, is defined as an ISO standard, ISO/TS 11073-9201:2007 (2007). This format was developed as a universal standard description format for medical waveforms to be used for several defined types of Vital Signs. The standard describes different waveform types (electrocardiogram, sound, pulse, monitoring, magneto cardiogram, electroencephalogram etc.) which make this format open and flexible. It uses a binary format with a compact code in the header section, which gives relatively small file sizes. In the supplementary description at Level 2, tags

representing waveform-related information, such as measurements, are defined to implement necessary beat annotations. It is possible to define long-term series of ECG recordings, thus this standard can be used for remote home monitoring solutions. Ideally, within a telemedical application to remotely monitor vital signs information, both actual standards SCP-ECG and MFER should be supported.

Integration of patient-entered data of daily measured vital sign information or automatically recorded information as a remote ECG recording solution, are today not defined within the Core-EHR framework. Such solutions can be established as an addendum to the Core-EHR and stored in a separate database which can be directly linked to the patient's Core-EHR. In such a solution the security and privacy issues should be combined, and necessary access to the information should be defined.

Recorded vital signs data can represent a huge amount of raw data for temporary storage to be accessed by the clinician. His signed evaluation of the data together with selected data samples should be extracted from the temporary storage and stored within the Core-EHR database for long-time storage. A remote ECG recording solution has been developed by Fensli et al. (2005), using a wireless ECG recording sensor attached to the patient's chest and communicating within a closed Body Area Network to a wearable hand held receiver or HHD. Arrhythmia detection algorithms implemented in this HHD will perform a continuous evaluation of arrhythmias, and upload detected events to the patient's vital signs database. In order to establish a secure mobile communication channel from the HHD at the patient, such solutions can be dependent of the actual services available by the telecom operator. A secure VPN channel can be established from the device either by implementing VPN software within this mobile terminal or by using encryption algorithms stores in the SIM card. This will give a secure transfer of recorded data from the HHD to an intermediary or Gateway implemented at the edge of a National Health Network. From this gateway, the transmitted recordings can be polled by a data server storing the database of recorded Vital Signs, as shown in Fig. 4.

7.3 Patient's role as administrator

Within a PaPeHR solution, a challenging task for the patient will be to fulfil the role as system administrator, as this will include assigning access rights to other persons. There is a lack of scientific publications describing how the patient can be able to manage the required tasks, and how those systems should be designed in order to give an intuitive way of performing necessary tasks. In many countries, the use of net-bank accounts is widely adopted. However, those systems are for single users with full permissions, and you will normally not be able to give access privileges to other persons unless you share the same net-bank account with your spouse or have similar solutions defined by your net-bank.

There are several difficulties to overcome. First of all, based on principles from the RBAC approach, patient/user should be able to define/configure suitable roles with needed privileges. Roles can be your local doctor, your home nurse, your private physiotherapist, spouse/next of kin, close friends etc.

As the PaPeHR will contain different types of data, it can be difficult to have sufficient overview. In addition, it should preferably be used common names of the different parts of information that can be understandable to the patient. As medical records use many Latin words, it is challenging to use more common names familiar to the patients with a normal vocabulary.

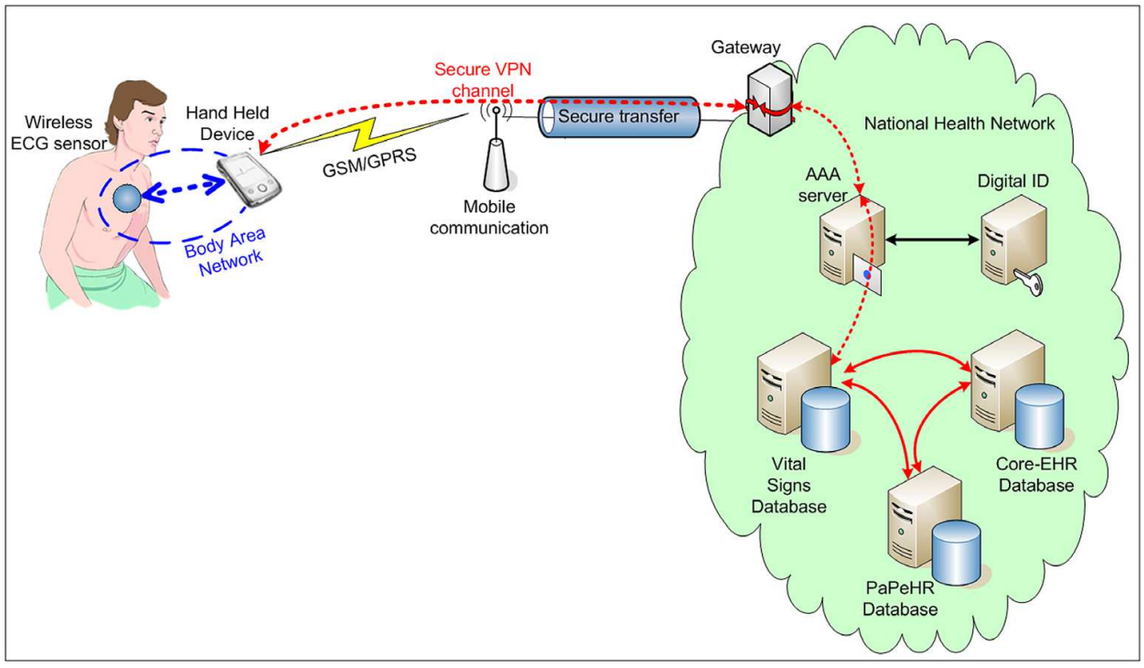

Fig. 4. Principles for secure transfer of real-time recorded ECG signals from a wireless sensor at the patient's chest to a Hand Held Device (HHD) where incorporated arrhythmia detection algorithms will store detected events. The files are transmitted via secure VPN channel to a Gateway at the edge of a National Health Network, where a Data Server can poll for the transmitted files, thus the files can be stored in a Vital Signs database, which is directly linked to the patient's PaPeHR database and also to the Core-EHR database

The problem of having an understandable format in medical documents within the PHR was also focused on in the study by Kahn et al. (2009). Access can be defined as denied, read only, permissions to write etc; however, normally no information should ever be deleted or changed after it is signed, as will be the cases for ordinary EHR solutions used within the health care services.

In Fig. 5, we have implemented a role-based interface for assigning actual persons to the required roles. As can be seen, the patient, after choosing the Access folder, can define persons being assigned to the actual roles. In this case, the patient can look up his/her doctor by entering the first name and surname, and by selecting the correct doctor from the list. It will be necessary to use digital ID's for secure login, and it can be defined a second step for the login procedure using onetime passwords transmitted to the mobile phone.

8. Discussions and conclusion

First of all, the use of patients' portals to access personal medical information and the ability to have electronic communication with health care services will obviously increase in the future, with the intention of providing the patient with higher degree of empowerment and better self-care. In order to give acceptable privacy to the patient, such solutions should preferably be based on the model of a standalone PHR; while at the same time should seamlessly integrate the access to a Core-EHR solution. The different models for a national Summary Care record or Core medical record system should be established with necessary

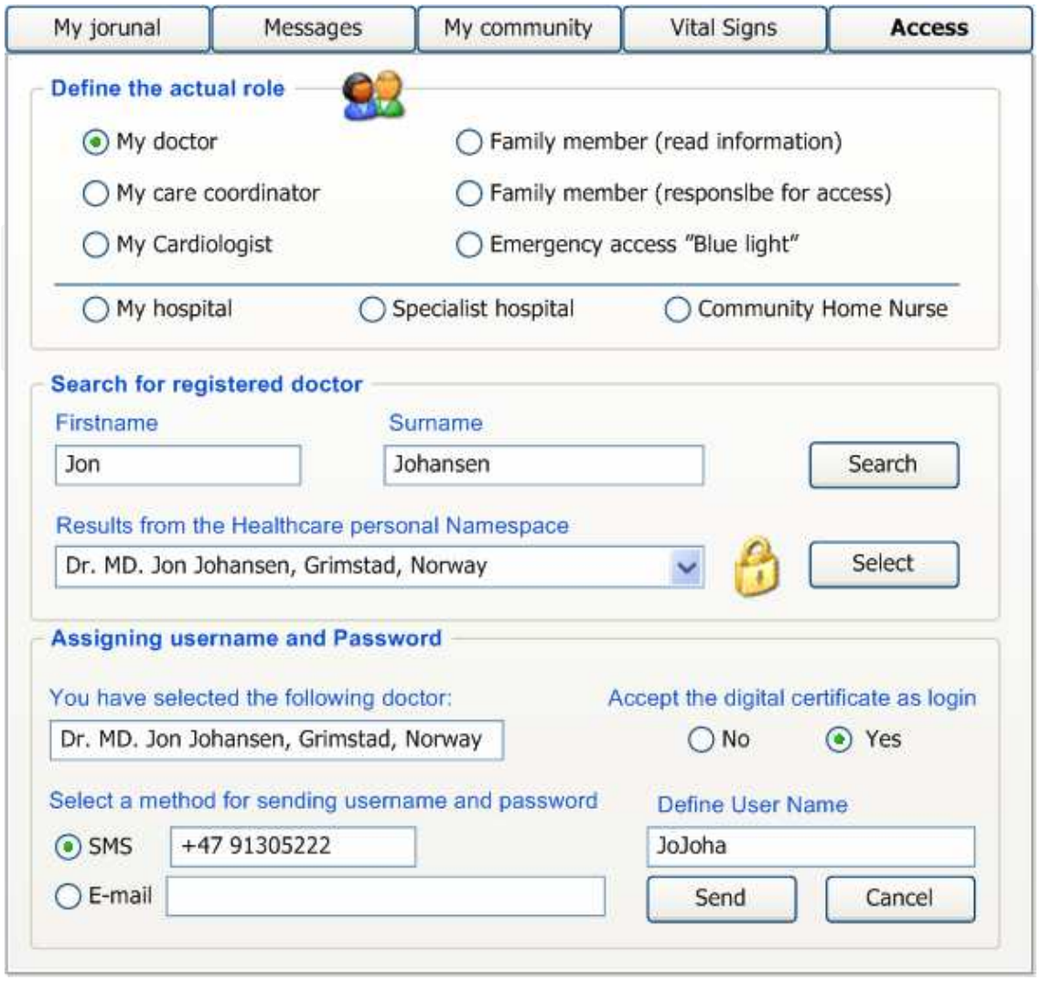

Fig. 5. Example of user interface for assigning access rights based on pre-defined roles, where the patient can select a registered doctor from the National Healthcare Namespace, and give him privileges as "My doctor". It should be incorporated possibilities for use of one-time secure password solutions, where a randomized password is sent to the person's defined mobile phone or to a defined E-mail address

security measures within the framework of a national health network. There are several models of EHR approach; however, it should be established an EU MB Portal where each national authority will be responsible for accreditation of medical personnel and with a cross-country namespace lookup.

Ongoing European initiatives focusing on interoperability and standardisation are important to obtain cross-border implementations. This can give opportunities for using open standards when developing new solutions, and there should preferably be several competing solutions available on the market offered by trusted third-party companies or organizations, where the patient can choose which PaPeHR solution he/she will use with the necessary confidence and trust.

Solutions for remote monitoring of vital signs data should not be developed as stand-alone applications, but integrated into the patient's PaPeHR system. As the amount of raw data can reach huge levels of stored information, those recordings should be stored in a separate

database. From this temporarily database, the clinicians can do necessary evaluations and calculations/simulations/trend analysis/parameter estimations, and actual extracts of important findings should be imported and stored directly in the Core-EHR together with the medical epicrisis. The vital signs data should also be recorded according to defined international standards in order to exchange of data and integration into different EHR systems. Thus open viewers to show recorded and stored data should be developed and implemented into all EHR systems.

There are several challenges to overcome in the design of a Patient administered Personal electronic Health Record, and functionality requirements should be thoroughly explored in further research studies. However, the most delicate issue will probably be the question of how the patient will be able to fulfil the task as a system administrator, in managing roles and access privileges to all the persons (health care personnel and spouse/next of kin/ family members and friends/training partners, etc.) who should have different kinds of authorization to the information stored and to being able to add actual records of new information.

Taking into account the probable use of a facilitator helping the patient to perform those functions correctly, the human computer interaction in design of such new solutions should be focused on in future research projects. This focus is essential in order to develop an easy to use solution which can give the patient a feeling of usefulness helping him/her to better overcome the disease treatment and follow-up. If the obstacles we have pinpointed are overcome in a well designed solution with sufficient functionality, we believe that patients will quickly adopt the use of a secure health-care net account in the same way as electronic banking.

9. References

Agrawal, R., J. Kiernan, et al. (2002). Hippocratic databases, VLDB Endowment.

Anderson, R. M. and M. M. Funnell (2009). Patient empowerment: Myths and misconceptions. *Patient Education and Counseling*.

ANSI/INCITS 359-2004 (2004). Information Technology - Role Based Access Control. I. C. f. I. T. Standards: 56.

Aziz, O., B. Lo, et al. (2008). From computers to ubiquitous computing by 2010: health care. *Philos Transact A Math Phys Eng Sci* 366(1881): 3805-11.

Barlow, J., C. Wright, et al. (2002). Self-management approaches for people with chronic conditions: a review. *Patient Educ Couns* 48(2): 177-87.

Bergmann, J., O. J. Bott, et al. (2007). An e-consent-based shared EHR system architecture for integrated healthcare networks. *International Journal of Medical Informatics* 76(2-3): 130-136.

CEN/ISSS eHealth Standardization Focus Group. (2005). Current and future standardization issues in the eHealth domain: Achieving interoperability. Executive Summary. Retrieved 10 06, 2008, from ftp://ftp.cenorm.be/PUBLIC/Reports/eHealth/eHealthStandardizationExecutive%20summaryFinalversion2005-03-01.pdf.

CEN/TC 251 Working Group IV (2006). prEN 1064: 2005 (SCP-ECG) - Amendment

Cimino, J. J., V. L. Patel, et al. (2002). The patient clinical information system (PatCIS): technical solutions for and experience with giving patients access to their electronic medical records. *International Journal of Medical Informatics* 68(1-3): 113-127.

Commission, E. (2004). Commission Communication on "eHealth - making healthcare better for European citizens: An action plan for a European eHealth Area". COM(2004) 356 final.

Coulter, A., S. Parsons, et al. (2008). Where are the patients in decision-making about their own care? *World Health Organization*.

Dagtas, S., G. Pekhteryev, et al. (2008). Real-Time and Secure Wireless Health Monitoring. *International Journal of Telemedicine and Applications* Article ID 135808: 10p.

Demiris, G., L. B. Afrin, et al. (2008). Patient-centered Applications: Use of Information Technology to Promote Disease Management and Wellness. A White Paper by the AMIA Knowledge in Motion Working Group. *Journal of the American Medical Informatics Association* 15(1): 8-13.

European Commission (2006). Connected Health: Quality ans Safety for European Citizens. Report of the Unit ICT for Health in collaboration with the i2010 sub-group on eHealth and the eHealth stakeholders' group: 36.

Fensli, R. and E. Boisen (2008). How to evaluate human factors of wireless biomedical sensors. Identifying aspects of patient acceptance based on a preliminary clinical trial. *International Conference on Health Informatics, HEALTHINF*, Funchal, Madeira-Portugal.

Fensli, R., E. Gunnarson, et al. (2005). A wearable ECG-recording System for Continuous Arrhythmia Monitoring in a Wireless Tele-Home-Care Situation. *Proceedings. 18th IEEE Symposium on Computer-Based Medical Systems*, Dublin, Ireland.

Ferraiolo, D. F., D. R. Kuhn, et al. (2003). Role-Based Access Control. *Computer Security Series*.

Ferreira, A., D. Chadwick, et al. (2009). How to Securely Break into RBAC: The BTG-RBAC Model. *2009 Annual Computer Security Applications Conference (ACSAC)*, Honolulu, Hawaii, USA, IEEE.

Grimsmo, J., H. Arnesen, et al. (2010). Changes in cardiorespiratory function in different groups of former and still active male cross-country skiers: a 28–30-year follow-up study. *Scandinavian Journal of Medicine and Science in Sports* 20(1): e151-e161.

Hansen, F. Ø. and R. Fensli (2006). Method for Automatic Escalation of Access Rights to the Electronic Health Record. *MIE 2006 The 20th International Congress of the European Federation for Medical Informatics*, Maastricht, Netherlands, IOS Press.

Hansen, F. Ø. and V. Oleshchuk (2003). Application of Role-Based Access Control in Wireless Healthcare Information Systems. *Scandinavian Conference on Health Informatics*, Arendal, Norway, Agder University College.

Hansen, F. Ø. and V. Oleshchuk (2006). Location-based Security Framework for use of Handheld Devicces in Medical Information Systems. *4th IEEE Conference on Pervasive Computing and Communications Workshop (PerCom 2006 Workshops*, Pisa, Italy, IEEE Computer Society.

HiMSS (August 2008). Electronic Health Records: A Global Perspective. A Work Product of the HIMSS Enterprise Systems Steering Committee and the Global Enterprise Task Force.

Hurtado, M. P., E. K. Swift, et al. (2000). Institute of Medicine (IOM) Committee on the National Quality Report on Health Care Delivery, Board on Health Care Services. Envisioning the National Health Care Quality Report. Washington DC, National Academic Press.

ISO/TS 11073-9201:2007. (2007). Health informatics — Medical waveform format — Part 92001:Encoding rules (MFER). Retrieved 15 October, 2008, from http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fTS+11073-92001%3a2007.

Kahn, J. S., V. Aulakh, et al. (2009). What It Takes: Characteristics Of The Ideal Personal Health Record. *Health Aff* 28(2): 369-376.

Kong, K. Y., C. Y. Ng, et al. (2000). Web-Based Monitoring of Real-Time ECG Data. *Computers in Cardiology* 27: 189-192.

Kumar, S., K. Kambhatla, et al. (2008). Ubiquitous Computing for Remote Cardiac Patient Monitoring: A Survey. *International Journal of Telemedicine and Applications* Article ID 459185.

Markle Foundation (2003). Connecting for Health. The personal health working group final report.

NEN. (2009). E-HEALTH-INTEROP. Retrieved 04,09, 2010, from http://www.ehealth-interop.nen.nl.

Oleshchuk, V. and R. Fensli (2010). Remote Patient Monitoring Within a Future 5G Infrastructure. *Wireless Personal Communications*: 1-9.

PRIMIS+. (2009). What is PRIMIS+. Retrieved 06.09, 2010, from http://www.primis.nhs.uk/index.php/about-us.

Ross, S. E. and C. T. Lin (2003). The Effects of Promoting Patient Access to Medical Records: A Review. *Journal of the American Medical Informatics Association* 10(2): 129-138.

Salvador, C. H., M. P. Carrasco, et al. (2005). Airmed-Cardio: A GSM and Internet Services-Based System for Out-of-Hospital Follow-Up of Cardiac Patients. *IEEE Trans Inf Technol Biomed* 9(March): 73-85.

Scalvini, S., S. Capomolla, et al. (2005). Effect of home-based telecardiology on chronic heart failure: costs and outcomes. *Journal of Telemedicine & Telecare* 11(S1): 16-18.

Shabo, A. (2006). A global socio-economic-medico-legal model for the sustainability of longitudinal electronic health records. Part 1. *Methods of Information in Medicine* 45(3): 240-5.

Stolyar, A., W. B. Lober, et al. (2006). A Patient-Centered Health Record in a Demonstration Regional Health Information Network. *The 1st Distributed Diagnosis and Home healthcare (D2H2) Conference*, Arlington, Virginia, USA.

sundhed.dk. (2010). The Danish eHealth Portal. Retrieved 04.09, 2010, from https://www.sundhed.dk/profil.aspx?id=11062.105

Tang, P. C., J. S. Ash, et al. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association* 13(2): 121-126.

The Scottish Government. (2006). Your Emergency Care Summary: What does it mean for you? Retrieved 04,09, 2010, from http://www.scotland.gov.uk/Publications/2006/08/16152132/0.

U.S. Dept of Health and Human Services (2008). Remote Monitoring. Draft Details Use Case. http://library.ahima.org/xpedio/groups/public/documents/government/bok1_036413.pdf#page%3D1, Office of the National Coordinator for Health Information Technology: 34.

UK National Health Service. (2008). HealthSpace. Retrieved 10 04, 2008, from https://www.healthspace.nhs.uk/.

Vogel, R., F. Wozak, et al. (2006). Architecture for a Distributed National Electronic Health Record System in Austria. Retrieved 10.05, 2008, from http://www.europacs.net/Extended%20abstracts/Integration%20of%20PACS%20RIS%20and%20EPR/Raimund%20Vogel%20Full_Paper_DistEHR_RVo_EuroPACS2006.pdf.

W3C. (1999). Web Content Accessibility Guidelines 1.0. Retrieved 04,09, 2010, from http://www.w3.org/TR/WAI-WEBCONTENT/.

W3C. (2008). Evaluating Web Sites for Accessibility: Overview. Retrieved 04,09, 2010, from http://www.w3.org/WAI/eval/Overview.html.

Wald, H. S., C. E. Dube, et al. (2007). Untangling the Web—The impact of Internet use on health care and the physician–patient relationship. *Patient Education and Counseling* 68(3): 218-224.

Weingart, S. N., D. Rind, et al. (2006). Who Uses the Patient Internet Portal? The PatientSite Experience. *Journal of the American Medical Informatics Association* 13(1): 91-95.

Wootton, R. and J. C. Kvedar (2006). Home Telehealth: Connecting Care Within the Community, RSM Press.

Biomedical Engineering, Trends in Electronics, Communications and Software

Edited by Mr Anthony Laskovski

ISBN 978-953-307-475-7
Hard cover, 736 pages
Publisher InTech
Published online 08, January, 2011
Published in print edition January, 2011

Rapid technological developments in the last century have brought the field of biomedical engineering into a totally new realm. Breakthroughs in materials science, imaging, electronics and, more recently, the information age have improved our understanding of the human body. As a result, the field of biomedical engineering is thriving, with innovations that aim to improve the quality and reduce the cost of medical care. This book is the first in a series of three that will present recent trends in biomedical engineering, with a particular focus on applications in electronics and communications. More specifically: wireless monitoring, sensors, medical imaging and the management of medical information are covered, among other subjects.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Rune Fensli, Vladimir Oleshchuk, John O'Donoghue and Philip O'Reilly (2011). Design Requirements for a Patient Administered Personal Electronic Health Record, Biomedical Engineering, Trends in Electronics, Communications and Software, Mr Anthony Laskovski (Ed.), ISBN: 978-953-307-475-7, InTech, Available from: http://www.intechopen.com/books/biomedical-engineering-trends-in-electronics-communications-and-software/design-requirements-for-a-patient-administered-personal-electronic-health-record

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen