End-to-end Security and Privacy Protection for Co-operative Access to Health and Care Data in a Telehealth Trial System for Remote Supervision of COPD-Patients

Martin Gerdes, Rune Fensli

Department of Information and Communication Technology, University of Agder, Norway

Abstract

The security and privacy of personal, health-related data in emerging telehealth and telecare systems is crucial, in particular under consideration of additional requirements. On the one hand optimal usability of the devices and applications provided for the monitoring of the health condition is desirable for the supervised patient. On the other side the different health and care organizations require co-operative access to the common infrastructure for storage, transmission and provision of the data from the patients.

In this paper we analyse the different types of security related issues and requirements of the telehealth trial system developed for a Norwegian implementation of the EU funded United4Health project, and describe a solution concept for functionalities and policies addressing those requirements. Identified design limitations of the security concept and initial results from the trial operation are discussed.

The paper concludes with the general relevance of the proposed security concept also for telehealth systems for remote monitoring of other patient groups by potentially other types of services, and an outlook on expected infrastructure evolutions and corresponding security considerations.

Keywords:

Security, privacy, telehealth, telecare, EHR, NHN, cloud, health information technology

Introduction

The amount of personal, health related data that are collected, transmitted, stored, processed, and provided by data systems connected to the Internet (or in the *Cloud*), is strongly increasing (as indicated e.g. by the increasing adoption of EHR systems [1]).

On the one hand this is driven by telehealth and telecare systems for professional health and care service providers, which typically support the remote supervision of home-based patients. As the average life span of people is increasing, an increased percentage of the worldwide population is affected by ageing-related chronic diseases [2]. Chronic Obstructive Pulmonary Disease (COPD), for example, will be the fourth most common cause of death by 2030, according to a projection from the World Health Organization, only behind ischemic heart disease, cerebrovascular disease, and HIV/AIDS [3, 4]. It will be the fifth most common cause of chronic disability worldwide by 2020 [5]. In order to keep such patients independent and autonomous within their own living environment as long as possible, patient-centric and efficient supervision and care solutions are needed. And in order to secure the future of health and care systems around the globe, such solutions must provide the best balance between high-quality medical support for individual patients and cost for the society. Medical routine supervision and remote follow-up of patients with chronic diseases is one area that has a high potential for efficiency gains, by giving optimal personalized support to patients within their own private environment, while avoiding unnecessary consultations [6].

On the other hand, commercial, cloud based services for end consumers (as e.g. Apple Health, Fitbit, Jawbone UP, Nike FuelBand, Polar, Samsung, Sony; see [7]) are getting momentum. Such services allow to collect certain health and fitness related data (as typically pulse / heart rate, motion / activity, body temperature, blood pressure, etc.) and to illustrate those on gadgets (as SmartPhones, SmartWatches, etc.) and on corresponding vendor-specific Web-based portals.

Personal medical data about health and care conditions are privacy-critical on the one hand, and a functioning health information service infrastructure as a whole is of potentially life-critical relevance on the other hand. Due to that, there are a number of security aspects to be considered when collecting, accessing, transmitting, and providing different types of information via the distributed components of the health infrastructure.

The general focus of this paper is on the privacy protection of patient data within the components of the end-to-end infrastructure of a telehealth and telecare system. The security aspects to be considered when developing of a security concept for the Information and Communication Technology (ICT) solution are manifold:

- The *patient* (or in general the supervised person) must be reliably authenticated.
- The devices (as e.g. dedicated sensors) for the acquisition of medical, health and care related information from the patient must be reliably authenticated.
- The communication between the measurement devices (sensors) and the patient application device (e.g. a tablet-PC) must take place via a secure connection.
- A clearly defined *relation management* must be in place between the patient, the patient application device, and the measurement devices, in order to reliably relate the personal data from the patient (as sensor measurements or other data gathered via the patient application device) to the corresponding patient.

- The access of the patient to the patient application device must be authorized.
- The access of the patient application device (and the applications running on it respectively) to the communication infrastructure must be controlled.
- The transmission of data between the patient application device and any Electronic Health Record (EHR) or Personal Health Record (PHR) service component in the health information infrastructure must be secured (encrypted).
- The access (e.g. from any telehealth or care service provider) to any personal patient data in the health information infrastructure (i.e. stored and processed in any EHR or PHR system) must be controlled.
- If components in a dedicated national health network as the Norwegian Health Network (NHN, [8]) infrastructure are involved, specific authentication and authorization rules for access control might apply.
- The communication between the information access devices of telehealth and other medical and care service providers and the EHR or PHR systems in the health information infrastructure (as in a NHN) must be secured (encrypted).

As basis for a more detailed analysis of security related requirements, and for the development and discussion of a security concept, we look at the telehealth trial system developed for the EU-funded project "UNIversal solutions in TElemedicine Deployment for European HEALTH care" (United4Health, or just U4H), and especially at the solution developed for the specific Norwegian requirements [9]. The aim to support a close cooperation of professional health and care providers from different organizations, and to involve even informal care providers as relatives, puts specific requirements on the system, in particular with respect to the security of the patient data. Another focus point for the development and evaluation of the U4H trial system has been the usability of applications and services for the different involved user groups (namely patients and care providers), and we address also the specific impacts of security mechanisms on the usability in this paper.

Within the following *Materials and Methods* section we will give a short overview of the U4H trial system and its main use cases. As part of that we will provide a detailed analysis of the security-related requirements within the different architectural domains of the end-to-end (e2e) system. In the *Results* section we will explain the security concept, which has been implemented in the U4H trial system. In the *Discussion* section we will then look at covered security requirements and potential security limitations, and address improvement potential with regards to usability. In the *Conclusions* we will explain the general relevance of the security concept (proposed for the ongoing U4H trial system) for other telehealth and telecare services for the collection and communication of health data.

Materials and Methods

Figure 1 shows the systems architecture of the U4H trial system with its main domains, the Point-of-Care (PoC) environment of the patient, the Health Information Services (HIS) infrastructure, and the infrastructure for the Health and Care Sources, i.e. the different sources of health and care services.

The U4H Trial System

The overall purpose of the U4H trial system is the remote supervision and follow-up support for COPD patients in their home after being discharged from hospital, following a stationary treatment. We will subsequently explain shortly the main functionalities of the system along the different system domains.

Point-of-Care:

A software application on a tablet-PC supports the patient to carry out daily (at least) measurements of his pulse and blood oxygen level (SpO_2). The SpO_2 sensor device communicates the measurement values through a wireless Bluetooth (BT) connection to the tablet-PC. Additionally, the breathing quality of the patient can be measured with a Spirometer device.

The patient application on the tablet-PC provides furthermore a user interface (UI) with questionnaire forms for the daily reporting of COPD-symptoms of the patient.

The data (SpO_2 values, optionally Spirometer values, questionnaire answers) are stored in a local database on the tablet-PC. From there they are used for an information UI for the patient, and are transmitted to the HIS infrastructure.

Within the U4H field trial, each COPD-patient uses the tablet-PC for a temporary period of one month. After that period the device is provided to another patient participating in the field trial.

Health Information Services Infrastructure:

The data from all remotely supervised patients are transmitted and stored in a personal electronic health record system (P-EHR). A dedicated telehealth service provides a Web-based information portal for telehealth and care service providers. This service takes the patient data from the P-EHR system,

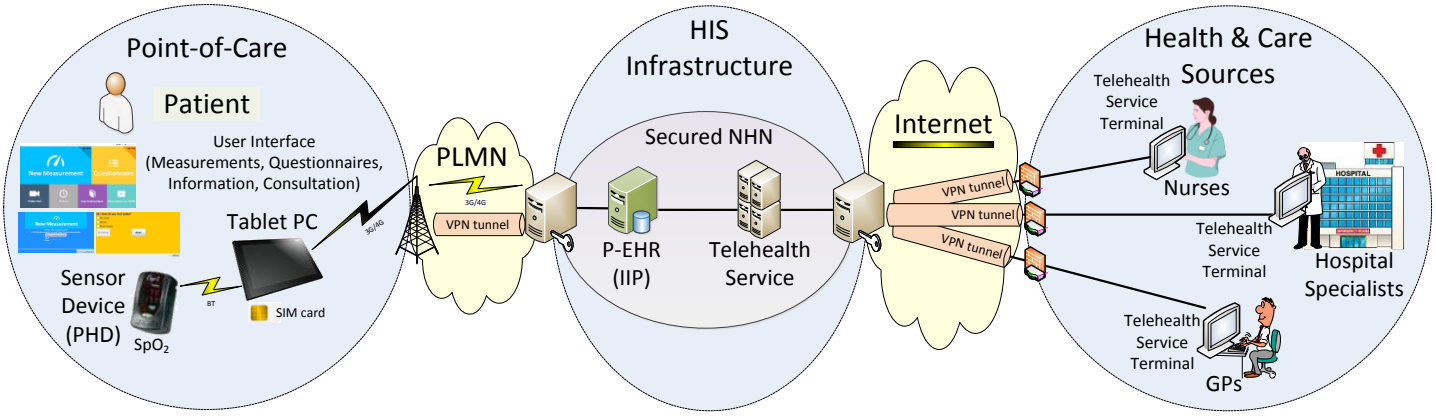

Figure 1- Architecture overview of United4Health telehealth trial system for COPD patients

evaluates the data according to "red (critical) – yellow (attention) – green (normal)" conditions ("Triage"), and provides overview pages with the triage-results of all supervised patients, as well as detailed condition pages with all information from a specific patient, collected during the supervision period.

Health and Care Sources:

Health and care professionals from different organizations have collaborative access to the telehealth data (i.e. measurements and questionnaire answers) from patients they are responsible for. This includes specially trained telehealth nurses (potentially located in dedicated telehealth center facilities), medical specialists in the hospital where the patients have been treated before discharge, and also general practitioners (GPs) that take care for the ambulatory care of the patients.

With a telehealth service terminal the health and care service providers get access to the Web-portal containing the overview of patients' status and the history of detailed monitoring data, provided by the telehealth service in the HIS infrastructure.

The U4H trial system also supports video consultation between the patient and the health and care service providers for the remote check-up and follow-up support. The security of the video consultation system is not considered in this paper.

Information flow through the U4H system

When a patient answers the daily questionnaire on COPD-symptoms on the tablet-PC, the answer-values are stored on the tablet-PC, together with an identifier of the patient and the date/time when the questionnaire took place (Figure 2).

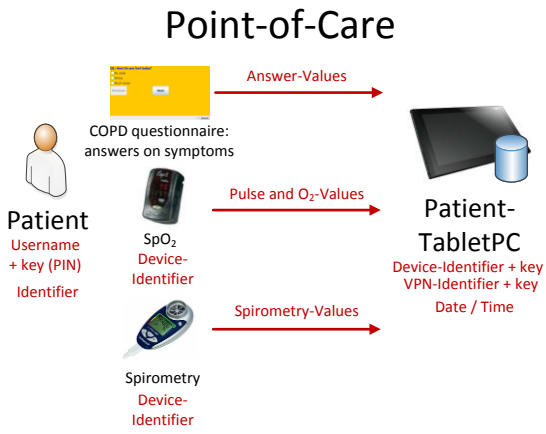

Figure 2- Information Flow in the Point-of-Care

Similarly, pulse and O_2-values from a pulse-oximetry measurement or the measurement-values from a spirometer-measurement are transmitted to the patient-tablet-PC, and are stored there together with the patient-identifier and the date/time of the measurement.

The patient-related information from each distributed patient-tablet-PC is transmitted to a Personal Electronic Health Record (P-EHR) system in the Health Information Service infrastructure (Figure 3). This information includes a patient-identifier, the answer-values from the COPD-symptoms-questionnaires, the pulse- and O_2-measurements-values, and the spirometry-measurements-values, all combined with the date/time of their acquisition, and the device-identifier of the patient-tablet-PC that was used for the acquisition of the information. In the P-EHR service the data is stored in a database, and is made available to the telehealth service.

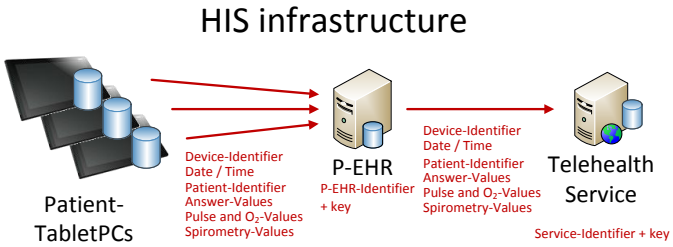

Figure 3- Information flow through the HIS Infrastructure

The telehealth service is the central Web-based access point for the questionnaire and measurement data from all supervised COPD-patients. Also the results from the Triage-evaluation, carried out by the telehealth service and using the raw patient data, are provided via this Web-portal (Figure 4). Different telehealth & care services, hospitals and also general practitioners use telehealth service terminals, which are shared by all staff of the corresponding institution. For example, all telehealth nurses of a telehealth & care service organization might share one terminal, the staff of a specific hospital (or a department respectively), or the staff of a GP office.

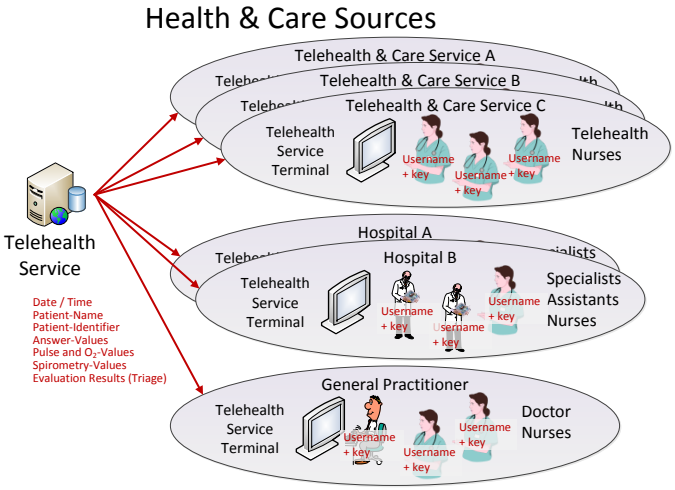

Figure 4- Information Flow to the Health & Care Sources

Analysis of Security Requirements

The fundamental objective of computer security is to protect the confidentiality, integrity and availability of the data and services of the system looked at [10].

Within this paper we focus in particular on the confidentiality of the patient data when being gathered, stored and communicated through the ICT infrastructure of the U4H trial system. Hence, we address the e2e confidentiality of the patient data from the point-of-care to the health and care service providers. Besides the confidentiality (as basis for the patients' privacy protection) we also address the system integrity.

Potential threats within the different domains of the U4H e2e system and requirements for corresponding countermeasures are identified in Table 1, Table 2 and Table 3 below.

Further security-relevant requirements, as the availability of the ICT system components for any U4H services, and a thorough analysis of possible attacks and risks, are not within the scope of this paper.

Table 1 - Threats and Requirements in Point-of-Care

# no	Threat	Requirement
Req1	Confidentiality threat: wrong person gets access to patient data (e.g. when tablet-PC is handed over from one patient to another)	Access control = authentication and authorization of patient to telehealth applications and personal data
Req2	Misuse of sensor device interface of patient-tablet-PC, to get access to data and services	Secure authentication of sensor device(s) and secure connection to tablet-PC
Req3	Unintended use of applications and services on patient-tablet-PC for purposes not related to telehealth supervision (e.g. installation of any software, access to Internet, etc.)	Patient is authorized for access to a secured desktop environment on the tablet-PC only, that contains the telehealth applications and services, and personal data
Req4	Physical or mental limitations or disabilities of patient limiting the intended use for remote supervision	Enable a high level of usability, in particular of any security related functionalities

Table 2 - Threats and Requirements in the HIS Infrastructure

# no	Threat	Requirement
Req5	Confidentiality threat: unintended access to personal patient data at transmission from patient-tablet-PC to P-EHR system	Encryption of communication between patient-tablet-PC and P-EHR system
Req6	Confidentiality or integrity threat: Misuse of patient-tablet-PC interface of P-EHR system, to get unintended access to data and services or to send false data	Access control = authentication and authorization of patient-tablet-PC at the P-EHR system
Req7	Confidentiality threat: Misuse of service interface of P-EHR system, to get unintended access to data and services	Access control = authentication and authorization of telehealth service at the P-EHR system
Req8	Confidentiality threat: unintended access to personal patient data at transmission from P-EHR system to telehealth service	Encryption of communication between P-EHR system and telehealth service
Req9	Confidentiality or integrity threat: Misuse of P-EHR system interface of telehealth service system, to get unintended access to data and services or to send false data	Access control = authentication and authorization of P-EHR system at the telehealth service
Req10	Compromise national laws and policies for information security ensuring interoperability of services and systems for exchange and storage of health and care data	Enforcement of rules for the deployment of the P-EHR and telehealth service systems within the NHN infrastructure (Code of Conduct, [11], e.g. storage of personal health data within national boundaries of Norway)
Req11	Availability threat: unavailability of patient data when inter-changed between different EHR systems	Unique Patient-Identifier to be used in all EHR- and service systems (cooperating in the HIS infrastructure)

Table 3 - Threats and Requirements at Health & Care Sources

# no	Threat	Requirement
Req12	Confidentiality threat: wrong person gets access to patient data through the telehealth service Web-portal	Access control = authentication of individual person at any cooperating health and care service provider (i.e. medical specialists, GPs, nurses, assistants, etc.) and authorization to access personal patient data only as required for their responsibilities towards the patient
Req13	Confidentiality threat: unintended access to personal patient data at transmission from telehealth service to telehealth service terminal at health care service provider	Encryption of communication between telehealth service and telehealth service terminal

Related Work

According to a report on e-health strategies published in January 2011 by the European Commission (referred from [12]), trust in eHealth systems by both citizens and professionals had been identified as one of, if not the key challenge in all countries. Privacy had been recognized as the most sensitive aspect of eHealth records systems.

Due to their high importance, significant efforts have been put into research studies of different security and privacy aspects of eHealth systems.

Fernández-Alemán et al [13] have carried out a systematic literature review of articles dealing with the security and privacy of EHR systems, most of them addressing standards or regulations related to the privacy and security of EHR data.

Kaletsch and Sunyaev [14] have examined a theoretical foundation of Personal Health Records (PHR) for the deployment in a Cloud environment. Along a few case studies the top-threats for patient's privacy have been identified.

Zhang and Liu [15] proposed a reference model for EHR security, focusing on EHR sharing and integration in healthcare clouds. The model has not been proven in a test or trial system.

Goldman and Hudson [16] study consumer-focused Internet services for online-access and distribution of health information. One finding is, although the Internet appears to offer anonymity and a safe place to seek and share information (what obviously attracts many health care consumers), that many eHealth business models depend on identifying and tracking users for different purposes.

Terry and Francis [17] argue, that acceptance from patients and physicians is the initial requirement for the nationwide transition to EHRs, which depends at the forefront on privacy and confidentiality concerns. They propose an autonomy-based EHR system, giving the patients full control over personal information.

Kluge [18] addresses the risk management of patient health data under consideration of international and global interoperability, and calls for "professional health information organizations", that should lead the development and harmonization of security protocols, and of principles for the certification.

Results

The analysis of security requirements and potential threats has resulted in a security concept and corresponding mechanisms, which we have deployed along the different components in all domains of the U4H trial system.

Point-of-Care Security

Req1 + Req4

At the start of the patient device (switch-on of the tablet-PC), the telehealth application for remote supervision starts automatically, and the patient has to authenticate himself towards his user account with a personal identification number (PIN) assigned to his user name (=account name). Discretionary Access Control (DAC) is carried out, based on the authenticated identity of the patient. All personal data, including all sensor measurements and questionnaire answers, are stored in a database located within the user account of the patient (and are transmitted to the P-EHR system in the HIS infrastructure). When the telehealth supervision of the patient comes to an end, the user account of that patient, including the database with any personal data, is deleted by an administrator, before the tablet-PC is being prepared for another patient.

To improve the usability, the PIN is only 4 digits long. Also it is known to the telehealth nurses, that are in charge for that patient, so that they can remind it to the patient on demand via phone or video conference, e.g. in case the patient has forgotten the PIN.

Req2

Only sensor devices following the Continua alliance specification are supported for the measurements. The communication with the patient-tablet-PC device goes via Bluetooth (BT). The one-time link configuration between the sensor device and the tablet-PC requires a specific Bluetooth device PIN, which has to be configured in the tablet-PC by an administrator. For that a specific administrator account is configured in the tablet-PC, requiring a corresponding administrator password for authentication. Other devices than the linked sensor devices cannot communicate with the tablet-PC.

Req3

A secured desktop environment[1] is installed within the Windows operating system of the patient-tablet-PC, which only contains the applications required for the telehealth supervision of the patient. That environment is automatically started when the tablet-PC is switched on, and prevents the patient (or anyone else) from using unauthorised resources. Only a secret key sequence, known to the administrator, allows switching to the Windows desktop environment.

Health Information Services Infrastructure

Req5

For the communication of the patient-tablet-PC through a public land mobile network (PLMN) infrastructure with the P-EHR system deployed within the National Health Network (NHN) infrastructure, a multi-layered security concept has been developed. For the U4H trial an Information Integration Platform (IIP, [19]) has been utilised as implementation of the P-EHR system.

On link layer, a Virtual Private Network (VPN) tunnel is established between the mobile broadband communication module of the patient-tablet-PC device and a secure access gateway at the NHN[2]. Using the VPN-Identifier of the patient-tablet-PC (refer to Figure 2) and a corresponding symmetric key, stored in the tablet-PC and known to the secure access gateway, the tablet-PC device is authenticated to the gateway. Subsequently, bidirectional encryption of all traffic through the underlying PLMN and Internet infrastructure is established.

On application layer, the HTTPS protocol [20] is utilized for the e2e communication between the telehealth application on the patient-tablet-PC and the P-EHR system (IIP) within the VPN infrastructure of the NHN. The device-identifier of the patient-tablet-PC (refer to Figure 2) and a corresponding symmetric key known to the P-EHR system (IIP) is used for authentication, and for the establishment of bidirectional session encryption. By this, the transmission of all personal patient-related data from the telehealth application to the P-EHR system (IIP) is protected. In a potential future real deployment, asymmetric keys could alternatively be used to establish the session encryption, utilizing a Public Key Infrastructure (PKI). In that case, digital certificates would be issued and validated by a Certification Authority (CA) for the authentication of all patient tablet-PCs and for the P-EHR system (IIP).

Req6

As the communication of any client with the P-EHR system (IIP) via the interface for the patient-tablet-PCs is carried out through HTTPS (refer to the security solution for Req5 above), only authorized clients (authenticated by the correct device-identifier + key pair) can communicate with the P-EHR system (IIP). For that, the P-EHR system (IIP) carries our DAC based on the authenticated identifiers of the communication devices.

[1] For the U4H trial system, the "Secure Exam Browser (SEB)" (http://sourceforge.net/projects/seb/, free under GPL license) is used. It has been developed as Web-browser-environment to carry out online-exams safely, but allows changing any computer into a secure workstation.

[2] For the U4H trial system, a VPN solution from the Norwegian mobile network operator Telenor is being used, called Mobile Data Access (MDA) (http://www.telenorfusion.no/makeit/communication apis/mobiledataaccess/mdatechnicaldetails.jsp)

Req7

Similarly to the communication of patient-tablet-PCs with the P-EHR system (IIP) (refer to Req6), also the communication of any application or service node with the P-EHR system (IIP) utilizes HTTPS. The telehealth service component has to provide the valid service-identifier + key pair (refer to Figure 3) for the authentication towards the P-EHR system (IIP), in order to get authorized for corresponding data access. The DAC mechanism in the P-EHR system uses the authenticated service-identifiers.

In order to protect the privacy of personal patient data stored in the P-EHR system (IIP), an arbitrary patient-identifier is sent from the patient-tablet-PC together with all telehealth data, instead of the patient's name or any identifier that can easily be related to the patient. Only the telehealth service can map the patient-identifier to a specific patient, and hence pseudonymization of the patient data is applied when being communicated from the patient-tablet-PC to the telehealth service, and stored in the P-EHR system (IIP).

Req8

The P-EHR system (IIP) requires communication via HTTPS, in order to authenticate any application or service node, and to authorize incoming requests (refer to Req7). This also establishes bidirectional encryption of the data traffic between the P-EHR system (IIP) and the telehealth service, protecting the data against eavesdropping.

Req9

The HTTPS protocol is used for authentication of the telehealth service to the P-EHR system, and for bidirectional encryption of all messages exchanged between them (refer to Req8). Correspondingly, the P-EHR system uses its P-EHR Identifier + key pair (refer to Figure 3) for the authentication at the telehealth service, and the telehealth service use DAC based on the authenticated P-EHR identifiers to control the access.

Req10

Norway has developed a legally-binding "Code of Conduct for information security in the healthcare and care services sector" [11], defining an information security policy to ensure a secure interoperability of information system from all organizations operating within the National Health Network (NHN).

As the HIS infrastructure components for the U4H trial system, namely the P-EHR system (IIP) and telehealth service, are deployed within the NHN (refer to Figure 1), those components had to be compliant with the code. The code requires (as one example besides many other rules), that the information system components for the storage of any personal health-related data have to be physically installed on Norwegian territory. This excludes for example cloud-based solutions relying on storage systems being located outside Norway.

Req11

A unique patient-identifier, to be defined for all patient devices (as the U4H patient-tablet-PCs), is crucial for the availability of patient data when being inter-changed between cooperating EHR systems and health and care service systems (as the U4H telehealth service) within the HIS infrastructure (see Figure 3).

Such an identifier should be anonymized from other public known identifiers (as the patient name or the social security number), to protect the privacy of the patient data within the EHR systems (see also Req7). The mapping of that anonymous patient-identifier to a specific patient should only be technically available for the patient devices and the health and care services.

Health and Care Sources

Req12

The efficient and secure access to health and care related data from the remotely supervised patient is crucial for the cooperative approach of the U4H trial system. In order to achieve that, a Role-Based Access Control (RBAC) [21] approach has been chosen. Each individual health and care service provider staff uses the telehealth service terminal to authenticate her-/ himself at the common (i.e. shared by all health and care sources organizations) Web-portal of the telehealth service with her / his username + key pair (refer to Figure 4). Based on their authentication, the individual service providers are grouped according to their organization or institution, and get authorized to access personal data of those patients that are assigned for supervision by that organization.

A more detailed definition of access groups also allows distinguishing between specific access rights of different groups within each organization. For example, authenticated doctors can be authorized to perform different operations on the patient data than assistants or nurses.

Req13

The communication between the P-EHR system (IIP) and the telehealth service is secured by using the HTTPS protocol (refer to Req8 and Req9 above). Now, HTTPS is not used for client authentication and access control of the telehealth service terminals (which is done by RBAC at the telehealth service), but only for encryption of all messages between the telehealth service and each telehealth service terminal.

Discussion

The requirements towards the security policies and functionalities of the telehealth e2e system for the U4H trial have been addressed in the system development as described within this document. Compared to most other related work (see above) about security and privacy of eHealth systems and EHR data, we have followed a more practical approach towards the implementation of the proposed security concept. The trial operation will also be analysed with respect to security limitations or issues in the design, implementation or operation of the system.

During the design and development of the U4H trial system, which has followed a User-Centered Design (UCD) approach [22], the dependencies between security and usability became obvious. Usability is critical in particular for patients with physical or mental disabilities or limitations. Long (and presumably more secure) passwords are subject to be forgotten, or are problematic to be entered on the touch screen of a tablet-device for people with motoric difficulties. For telehealth services providers, as the nurses in the U4H telemedicine central (and also for other health and care sources), the efficiency of the system in the daily usage is crucial. The telehealth service terminal is shared by potentially many individual persons within one organization (as a telemedicine central), and the authentication and authorization procedure must not limit the timely access to potentially life-relevant information from supervised patients. Other methods, as e.g. biometric authentication or the use of personal SmartCards, or other devices, as

mobile phones supporting RFID technology [23] or NFC technology [24] for authentication, are subject to be integrated and tested in evolutions of the current trial system.

With regards to the general information architecture of the system, other alternatives would have been possible when it comes to the storage, transmission and processing of the patient-related information. Two potential extremes would have been to (1) collect, store and process all information in the PoC environment, e.g. on the patient's tablet-PC, or to (2) transmit all information directly to the Health & Care Sources (Figure 4), and to store and process it there. The main requirement of the telehealth system is to provide the different, collaborating health and care services with secure and efficient access to the patient information. In case of alternative (1), each telehealth service terminal would need e2e on-demand access to the patient-related information on a specific tablet-PC in the PoC environment. This would not be efficient for various reasons, as the unsynchronized data collection by the patient and the information request by the health and care service provider, due to the complex addressing of the data on each distributed patient-tablet-PC, and due to the risk of a specific tablet-PC lacking connectivity or just being switched-off when the health and care service provider requests information from that specific tablet-PC. The required robustness of the system makes it necessary to cope with a (temporary) loss of connectivity, and to retransmit any new patient-related information as soon as connectivity is recovered. Furthermore, the patient application on the tablet-PC shall provide autonomous recommendations to the patient in case of critical conditions, also when communication is not possible. Those requirements need the data to be stored and evaluated also on the tablet-PC, which is not the case in the alternative (2).

Alternative (2) would allow e2e security, i.e. the transmission of encrypted patient-related information from the patient-tablet-PC to the health service provider. In that case, each of the co-operating health service provider devices / applications would have to carry out the evaluation and decision support separately, and the data and information from the patient would either have to be forwarded from one service to another, or would have to be transmitted again, e2e from the patient-tablet-PC to the next health care service(s). Also, the patient-related data and information would not be available for other services in the national health network infrastructure if desired. For those reasons we have chosen a Services Oriented Architecture (SOA) approach with a cloud-technology-based infrastructure in the national health network, consisting of the P-EHR system (IIP) and the Telehealth Service, which provides a central, secure, Web-based access for the cooperating health and care sources. The e2e security in the proposed architecture is realized as secure chain of a few communication legs (Figure 4).

We have not carried out a formal study of vulnerabilities and potential attacks, nor a risk analysis, as this paper focusses on the initial security requirements and the corresponding system design and policies.

Further security related requirements, and also potential vulnerabilities and attacks, will arise with the integration of the P-EHR system (IIP) with other EHR systems or healthcare service components within the NHN, following the goal of system cooperation and integration. The P-EHR system (IIP) interface for the communication with the telehealth service via HTTPS provides for an easy and secure integration also with other services, though the content format of the messages transmitted securely via that interface will have to be adapted to the target system.

The patient-tablet-PC device for the U4H trial is provided and maintained by IT administrators of the trial partners, ensuring compliance with security policies in terms of software installation and configuration. In the deployment of real telehealth systems for large numbers of patients, this might lead to scalability-challenges related to the operation and maintenance (O&M) of the system. Such challenges can e.g. be the manual administration of patient accounts (refer to Req1 above), or the one-time connection of BT sensor devices to each patient tablet (refer to Req2). In future telehealth and telecare systems, it will be desired that also freely-available, off-the-shelf consumer devices can be utilized. In that case, the patients will have to install provided software on their tablet-PCs, or use the by default installed browser application. This bears the risk that - intended or unintended - malicious code gets installed in the patient device. That can potentially open a back-door into a secured national health network. It is therefore necessary to make precautions in the HIS infrastructure, to protect against potential vulnerabilities or attacks from patient devices. One potential option is to incorporate security precautions together with the patients' user credentials into a certified, secured app that would allow the patients to use their own device (as e.g. their personal smartphone). From the HIS infrastructure perspective only such a certified app would be required, instead of a defined and pre-configured mobile medical device.

Conclusion

The proposed security concept fulfils the identified security requirements for the U4H trial system. The system for the U4H trial, which is planned to run until summer 2016, has been developed according to the proposed security concept. The trial will help to identify potential security limitations and vulnerabilities, and further usability limitations (in particular related to security functionalities and policies) might be identified and utilized for improvements of the security concept.

Although the security concept and implementation has been developed for a specific trial system, the use cases and corresponding requirements of the telehealth services for remote patient supervision that are subject of the U4H project, represent typical characteristics of telehealth services. For that reason, the proposed security concept and the results and findings from the trial operation are also applicable for telehealth services for other patient groups, involving potentially other measurement devices, other questionnaires, other patient device types, and also other health and care service providers.

Emerging consumer market devices and applications for the collection of fitness and health related data, and for the transmission, evaluation and illustration on Web-portals, provided by cloud-based services, have similar security requirements as the studied telehealth service within the public health infrastructure. Consequently, the proposed security concept and trial results are also applicable for that type of services.

Security-related usability improvements can be expected from authentication mechanisms for patients and healthcare personal making use of biometric or Internet-of-Things (IoT) technologies (using RFID or NFC), and are subject for further studies.

Further impacts on the security requirements will arise from the expected integration of consumer health devices and services with the public telehealth services, and from the in-

creased integration and cooperation of EHR systems for various health and care services within the public HIS infrastructure.

Acknowledgments

We thank all project partners and students for their contributions and support during the development and implementation of the trial system.

References

[1] Hsiao C-J, Hing E. Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices, United States, 2001-2013: US Department of Health and Human Services, Centers for Disease Control and Prevention, National Center for Health Statistics; 2014.

[2] Christensen K, Doblhammer G, Rau R, Vaupel JW. Ageing populations: the challenges ahead. The Lancet. 2009;374(9696):1196-208.

[3] Barnes PJ. Chronic Obstructive Pulmonary Disease: A Growing but Neglected Global Epidemic. Plos Med. 2007;4(5):e112.

[4] Mathers CD, Loncar D. Projections of Global Mortality and Burden of Disease from 2002 to 2030. Plos Med. 2006;3(11):e442.

[5] Lopez AD, Shibuya K, Rao C, Mathers CD, Hansell AL, Held LS, et al. Chronic obstructive pulmonary disease: current burden and future projections. European Respiratory Journal. 2006 February 1, 2006;27(2):397-412.

[6] Rialle V, Duchene F, Noury N, Bajolle L, Demongeot J. Health "Smart" Home: Information Technology for Patients at Home. Telemed J E-Health. 2002;8(4):395-409.

[7] Bumgardner W. Where are Wearable Fitness Trackers Going for 2015? 2014 [22.04.2015]. Available from: http://walking.about.com/od/measure/fl/Wearables-2015.htm.

[8] Norwegian Health Network (NHN). Available from: https://www.nhn.no/english/Pages/default.aspx.

[9] United4Health. FP7 EU project United4Health 2013. Available from:
Umbrella project: http://www.united4health.eu/;
Norwegian project: http://www.united4health.no/.

[10] Guttman B, Roback E. An introduction to computer security: the NIST handbook: DIANE Publishing; 1995.

[11] ehelse.no. Code of conduct for information security (The healthcare and care services sector), 5 June 2014. Available from:
https://ehelse.no/Documents/Normen/Norm%20for%20informasjonssikkerhet%205%20%20utgave.pdf (norwegian),
https://ehelse.no/Documents/Normen/Code%20of%20Conduct%20v4.pdf (english).

[12] Mahony H. Trust remains key barrier to eHealth: euobserver; 2011 [22.04.2015]. Available from: https://euobserver.com/digital/31958.

[13] Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013 6//;46(3):541-62.

[14] Kaletsch A, Sunyaev A. Privacy engineering: personal health records in cloud computing environments. 2011.

[15] Zhang R, Liu L, editors. Security models and requirements for healthcare application clouds. Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on; 2010: IEEE.

[16] Goldman J, Hudson Z. Virtually exposed: privacy and e-health. Health Affairs. 2000;19(6):140-8.

[17] Terry NP, Francis LP. Ensuring the privacy and confidentiality of electronic health records. U Ill L Rev. 2007:681.

[18] Kluge E-HW. Secure e-Health: Managing risks to patient health data. Int J Med Inform. 2007 5//;76(5–6):402-6.

[19] Trinugroho YBD. Information Integration Platform for Patient-Centric Healthcare Services: Design, Prototype and Dependability Aspects. Future Internet. 2014;6(1):126-54.

[20] IETF. HTTPS = HTTP Over TLS (RFC2818, http://tools.ietf.org/pdf/rfc2818.pdf).

[21] ANSI. Role Based Access Control. American National Standard for Information Technology: Information Technology Industry Council; 2004. p. 56.

[22] Smaradottir B, Gerdes M, Fensli R, Martinez S. User Interface Development of a Tablet Application for Remote Monitoring of COPD-symptoms - A User-centred Design Process. International Conference on Advances in Computer-Human Interaction (ACHI); Lisbon , Portugal2015. p. 57-62.

[23] Bouet M, Pujolle G. RFID in eHealth systems: applications, challenges, and perspectives. Ann Telecommun. 2010 Oct;65(9-10):497-503. PubMed PMID: WOS:000282178600004. English.

[24] Morak J, Kumpusch H, Hayn D, Modre-Osprian R, Schreier G. Design and Evaluation of a Telemonitoring Concept Based on NFC-Enabled Mobile Phones and Sensor Devices. Information Technology in Biomedicine, IEEE Transactions on. 2012;16(1):17-23.

Address for correspondence

Address: Jon Lilletuns vei 9, 4879 Grimstad, Norway

eMail: Martin.Gerdes@uia.no