Journal of Information, Communication and Ethics in Society

Ethical aspects in eHealth - design of a privacy-friendly system

Milica Milutinovic Bart De Decker

Ethical aspects in eHealth – design of a privacy-friendly system

Milica Milutinovic and Bart De Decker
Department of Computer Science, KU Leuven, Leuven, Belgium

Received 8 June 2014
Revised 27 November 2014
26 January 2015
Accepted 5 February 2015

Abstract

Purpose – The medical advances and historical fluctuations in the demographics are contributing to the rise of the average age. These changes are increasing the pressure to organize adequate care to a growing number of individuals. As a way to provide efficient and cost-effective care, eHealth systems are gaining importance. However, this trend is creating new ethical concerns. Major issues are privacy and patients' control over their data. To deploy these systems on a large scale, they need to offer strict privacy protection. Even though many research proposals focus on eHealth systems and related ethical requirements, there is an evident lack of practical solutions for protecting users' personal information. The purpose of this study is to explore the ethical considerations related to these systems and extract the privacy requirements. This paper also aims to put forth a system design which ensures appropriate privacy protection.

Design/methodology/approach – This paper investigates the existing work in the area of eHealth systems and the related ethical considerations, which establish privacy as one of the main requirements. It lists the ethical requirements and data protection standards that a system needs to fulfil and uses them as a guideline for creating the proposed design.

Findings – Even though privacy is considered to be a paramount aspect of the eHealth systems, the existing proposals do not tackle this issue from the outset of the design. Consequently, introducing privacy at the final stages of the system deployment imposes significant limitations and the provided data protection is not always to the standards expected by the users.

Originality/value – This paper motivates the need for addressing ethical concerns in the eHealth domain with special focus on establishing strict privacy protection. It lists the privacy requirements and offers practical solutions for developing a privacy-friendly system and takes the approach of privacy-by-design. Additionally, the proposed design is evaluated against ethical principles as proposed in the existing literature. The aim is to show that technological advances can be used to improve quality and efficiency of care, while the usually raised concerns can be avoided.

Keywords Ethics, Patient-centric approach, Privacy, E-Health

Paper type Research paper

1. Introduction

The advances in the field of medicine and the historical fluctuations in the demographics are contributing to the increase of the average age of individuals in the Western world. The life expectancy is also experiencing a continuous rise. Consequently, an increasing number of individuals require some form of medical care or assistance. These changes are creating a growing pressure on the government's social security or on other insurance companies, as the costs for appropriate care provisioning are increasing.

This work was partially funded by the Mobile Companion (MobCom) project: www.mobcom.org

Journal of Information, Communication and Ethics in Society
Vol. 14 No. 1, 2016
pp. 49-69
© Emerald Group Publishing Limited
1477-996X
DOI 10.1108/JICES-06-2014-0028

Additionally, as the elderly are often not comfortable with moving to the nursing homes or hospitals and wish to stay at their homes for as long as possible, home care needs to be offered. Currently, the non-medical assistance is performed by the guardians of the elderly, who are most often immediate family members. However, the limited birth rate in the recent decades is creating a greying population. The number of available family members that could provide such assistance is therefore becoming increasingly limited. Additionally, the care provisioning comprises a range of aspects, making the requirements and responsibilities of the guardians all the more demanding. On the one hand, the daily tasks need to be provisioned, such as catering or cleaning, but also social contact and companionship. However, organizing care that requires trained personnel, such as nurses, GPs or specialists, is also essential. To decrease the responsibilities of the guardians and to additionally integrate different aspects of the home assistance, eHealth systems are widely considered and extensively researched. They allow the monitoring of the elderly, or patients recovering at home, and possibly provide means of communication with them.

Even though the eHealth solutions have a great potential and provide valuable opportunities for solving the aforementioned problems, the research in this area has not yet fully tackled the accompanying ethical issues. As eHealth systems encompass a new form of communication with the caregivers and management of patients' (health-related) data, the ethical considerations that exist for the traditional healthcare are not sufficient. On the one hand, these changes are advancing the quality of care by offering quick access to most recent health data, possibility of remote check-up and avoiding repeated analyses. On the other hand, new concerns are created related to aspects such as appropriate protection of patient's data and sustentation of the patient–caregiver relationship.

The issue that we focus on in this paper is the protection of patients' data and their privacy. As these systems perform monitoring and manage health-related information, the protection of data and access control are of major importance. To provide assistance to the elderly or patients, communication with the caregivers has to be ensured. This means that caregivers' personal information, such as contact data, needs to be handled by the system. However, knowing a caregiver of a patient can already reveal sensitive medical information about the patient. For instance, knowing which specialist is treating a patient usually allows inferring the medical condition in question. This is one of the examples that illustrates the need to tackle the privacy issues, so these systems can become widely adopted and deployed.

To address the aforementioned problems, we propose a flexible system design which would allow for care provisioning at the patient's home. Additionally, we also aim to offer the patients to connect to their known caregivers and ensure accountability of the actors. The design is deployed with ethical principles in mind, while encompassing practical properties of a diverse system. Services that can be incorporated are health monitoring, connecting the patient to her regular caregivers and family members and commercial services of external providers. We describe the accompanying set of privacy-preserving protocols that would protect the data of the users of the eHealth system, both patients and their caregivers, but would at the same time ensure that necessary data are made available to appropriate care-provisioning entities. What is also important, the described mechanism for privacy protection does not impose limitations on the number of services, or the quality of care that the system offers.

Additionally, the management of patient's data and its access control is based on flexible policies that are defined by the patient or an authorized guardian. They can easily be changed to reflect the changes in the care-provisioning network of a patient. Finally, the proposed system design is evaluated according to the ethical principles outlined in the literature.

2. Related work

There is a significant number of research initiatives focused on eHealth systems designed to assist elderly or stay-at-home patients. The importance of such systems is also illustrated in a number of European initiatives, such as the ongoing GiraffPlus project, epSOS (2008-2013), MobiHealth (2002-2004) and AMON (2001-2002) projects. They utilize information technology for offering better quality of care and improving the patients' autonomy (Scalvini *et al.*, 2013). In the existing proposals, the services that eHealth systems offer usually consist of monitoring health parameters, assessing the measurements and detecting anomalies. The monitoring is performed with unobtrusive wearable sensors or cameras, which offer the possibility to continuously record the health parameters of a patient.

Most research approaches in the field of eHealth systems focus on the development of the monitoring equipment, i.e. the body area sensor network. For instance, different types of monitoring sensors were assessed by Pantelopoulos and Bourbakis (2010). Specific types of sensor readings were also evaluated for their applicability and usefulness. Examples are video technology for fall detection (Tabar *et al.*, 2006), living activities monitoring (Tsukiyama, 2014), posture and gait analysis (Farella *et al.*, 2008; Lo *et al.*, 2005), voice health monitoring (Mehta *et al.*, 2012), sensors for detecting user-indicated alarms (Sarela *et al.*, 2003) or communication and status assessment (Johnston *et al.*, 2000). Integration of mobile phones into the monitoring network was investigated by Pascu *et al.* (2013) and cell phone communication was explored by Alahmadi and Soh (2011) and Jin *et al.* (2009). Utilization of the GPS technology and monitoring the patients outside of their homes was also analysed (Boulos *et al.*, 2007).

The existing proposals usually assume a three-tier system architecture. The sensors can be deployed in a single device (Sum *et al.*, 2005), or in a body area network (Jones *et al.*, 2010; Otto *et al.*, 2006; Jovanov *et al.*, 2001). Their readings are being recorded by a personal server and simply relayed to a remote care centre where they are assessed. Examples are proposals by Pantelopoulos and Bourbakis (2010), Jurik and Weaver (2008), Chakravorty (2006), Jovanov *et al.* (2005) and Kim *et al.* (2006). For offering medical care, this implies that the central entity needs to employ medically trained personnel, who would be able to perform the necessary health assessment. However, having a system that allows the patient to connect to her regular caregivers would ease commercial deployment of the eHealth systems and improve their adoption. The central entity of the system would no longer need to employ medically trained personnel and would be offered by a commercial entity. This further allows offering a wider range of services to the patients.

Finally, Markle Foundation's (2008) "Connecting for Health" framework is an effort towards an interoperable health information infrastructure. It focuses on creation, protection and management of personal health records that allow interaction of a network of involved entities. Similarly, we devise a system where information can be exchanged between all relevant entities, supported by their authorizations. However, unlike in the mentioned approach, our focus is a more personalized, home-based system that encompasses patient's preferences and is able to offer continuous monitoring of patient's health status, direct communication with caregivers, scheduling of tasks and usage of non-medical commercial services.

2.1 Ethics in eHealth

With the development of the electronic health care, the ethical issues existent within the traditional health care are broadening. Beauchamp and Childress (2001) propose an ethical assessment framework. It outlines the following four principles:

1. the principle of beneficence;
2. the principle of non-maleficence;
3. the principle of respect for autonomy; and
4. the principle of justice.

These principles can be used to evaluate technologies introduced in the health sector (Whitehouse, and Duquenoy, 2009). However, they are considered to be broad in scope and are also applicable to problems of areas other than health care. Focusing on the healthcare systems, Collste (2008) defines a systematic way of assessing used technologies, based on the following principles:

- doctor–patient relationship;
- responsibility; and
- respect for autonomy.

Making a compliant system and tackling the related issues is especially important, as ethical and legal aspects can be a hindering factor for the eHealth systems' adoption (Liu *et al.*, 2011; Anderson, 2007; Rodrigues, 2000; Hodge *et al.*, 1999). For this reason, the question of ethics in eHealth has been addressed in a number of research initiatives. The need for general guidelines for the eHealth domain resulted in the "eHealth Ethics Summit" hosted by the World Health Organization and held in 2000 (Rippen and Risk, 2000). The result of this initiative is the "eHealth Ethics Draft Code". The code lists the guiding principles, which stresses aspects such as privacy, user consent or accountability.

The issue of privacy is widely recognized, as the novel form of patient–caregiver interaction enabled by the eHealth systems creates new concerns. As suggested in the literature, the privacy concerns can be a great impediment to the acceptance of the eHealth technology (Liu *et al.*, 2011; Anderson, 2007; Tang *et al.*, 2006; Lake Research Partners *et al.*, 2006; Rash, 2005; Goldman and Hudson, 2000). Even though the privacy attitudes differ among users (Steele *et al.*, 2009), the importance of user control over their data was also indicated in the existing studies that investigate patient's attitudes (Essen, 2008), especially in the context of ambient surveillance (Collste, 2011), wireless communication (Ren *et al.*, 2010; Abascal and Civit, 2001) or if invasive video monitoring is utilized. The importance of privacy has been recognized in a number of works (Al Ameen *et al.*, 2012; Varshney, 2007; Cantor, 2006) and proposal by Nordgren (2013) lists it in an "ethical checklist" for eHealth systems.

According to the principle of autonomy outlined by Collste, a person affected by an action should be able to influence it. This principle also implies the protection of privacy

(Collste, 2008). This aspect is paramount to home assistance systems, especially as they handle sensitive and medical information, and it needs to be tackled to achieve wider adoption of these systems. Even though it is widely recognized to be an important problem, not many proposals are offering concrete solutions. Additionally, a general attitude is that privacy imposes obstacles to offering a wide range of services to the users. In our work, we focus on the aforementioned aspects with the intention of creating a system that offers a range of services to the patients. As patient self-management can be a great responsibility (Collste, 2002), allowing for (partial) decision automation and thus respecting the level of autonomy that the patient can take on is important.

Finally, in our proposed system, we follow the principle of "privacy by design", introduced by Cavoukian *et al.* (2010). This means that the privacy is embedded in the design specification, and is not introduced in the system only at the end of the design process, which would impose significant limitations. At the same time, we aim at offering a system that is not limited in the functionality and the services that are offered to the patients. Furthermore, the guidelines of the "eHealth Ethics Draft Code", among others, outline the requirements regarding user consent, privacy and accountability. In this work, we aim to tackle all of those requirements. More concretely, the deployed system offers high level of patient's privacy, it can be governed by patients' consent and the actions taken by different actors are logged, thus ensuring accountability.

3. Privacy-preserving design

In this section, we list the requirements that are posed on a privacy-friendly eHealth system. We then describe compliant protocols that enable privacy-preserving communication between the patients and their caregivers. For every protocol, we also list the goals of the protocol design, we explain and motivate the design decisions and finally represent the attained results.

3.1 Privacy requirements

Taking into account the aforementioned considerations, we list the requirements that an eHealth system needs to fulfil, to meet the legal and ethical requisites and gain a wider acceptance:

- The patient's personal and identifiable information is protected with strict access control policies. The disclosure is governed with the need-to-know principle.
- Non-medical caregivers should not gain access to patient's data, with the exception of explicitly authorized guardians. This is also required by the legislation in many countries (HIPAA, European Patient Rights Legislation).
- The access to the patient data should be logged securely, so that later auditing is enabled. This is important, for possible dispute resolution.
- The policies that control access to the patient's data are flexible and access rights given to a caregiver of a patient can be revoked or expanded. This allows the access control to reflect the patient's care network dynamics.

3.2 Overview of the underlying eHealth system architecture

The existing eHealth proposals are generally based on a three-tier architecture. It is composed of sensors which monitor the health and environmental parameters, a home station which gathers these recordings and a remote centre which provides assistance when necessary. This remote care centre is assumed to employ medically trained personnel to offer assessment of the monitored parameters and medical assistance. However, the drawbacks of this approach are that the care centre needs to employ medical professionals, which would be difficult for a commercially run entity. Moreover, this architecture only allows the connection between the patients and the medical personnel of the central entity, while the patients might prefer to be connected to their regular caregivers, such as their family doctors, specialists or their family members. To extend the possibilities of the eHealth system and the range of services that can be offered through the system, we will base ourselves on a four-tier architecture. This section provides more details on this architecture, on top of which the privacy-preserving protocols are built.

The system architecture is composed of four tiers (Figure 1). Similarly to the existing proposals, the first tier of the system consists of (wearable) *sensors*, which are installed at every patient's home. They monitor health parameters, such as heart rate or blood pressure, and environmental parameters, such as temperature or humidity. The measurements of these sensors are sent to a central indoor station, denoted as the *base station*. It is the controlling unit for the home equipment and is used to deliver all the services to the patient. Namely, it enables the communication of the patient with the rest of the system. It also stores the patient's data, such as sensor measurements, and controls access to it. The principal users (i.e. patients), or their guardians are given administrative rights, which allow them to set the functional and access control policies. These policies are flexible and are used to automatically determine which access is allowed to which caregivers and which caregivers are to be notified in case of emergency situations. Usually, appropriate medical personnel or immediate family members are

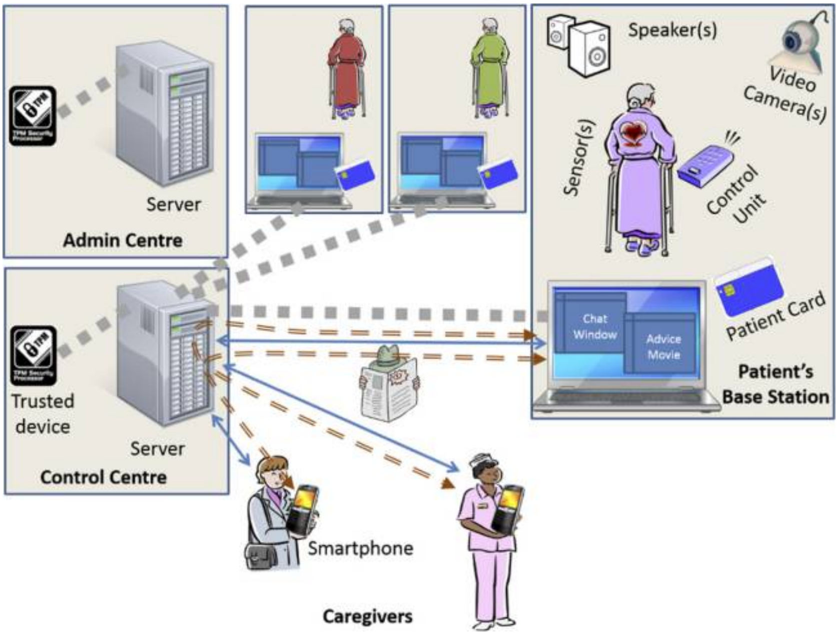


Figure 1.
The global architecture of the privacy-preserving eHealth system with arrows representing communication channels between different entities and dashed arrows representing tunnelled communication

given certain rights regarding data access, unlike commercial service providers, such as a catering provider.

The central part of the system is a *control centre*, which is the third tier of the system. It is a commercial entity and it maintains all the hardware and software components of the system. It is connected to a number of patients' base stations and enables their communication with the patients' caregivers. Furthermore, it is handling the distribution of the indoor equipment, including the base stations, and it offers technical support. However, given the commercial nature of the control centre, all the sensitive medical or identifying data are hidden from it. An important element of the control centre is a *trusted device* – a device with simple functionality, which is trusted to perform specified tasks. For ensuring its trustworthiness, trusted platform module technology can be utilized (Kinney, 2006; Bajikar, 2002). The trusted device is used for decryption and re-encryption of data that need to be exchanged, so that the data are accessible only to authorized entities, while remaining hidden from the control centre personnel or external entities. In addition, the control centre is equipped with a calling module, which is utilized for summoning caregivers in case they are required to assist a patient. The details on how the calling module is utilized are explained in Section 3.3.2.

Finally, the *caregivers* of the patients represent the fourth tier of the system. They are connected to the control centre via a designated software they need to install. Therefore, they can communicate with the patients they are connected with through the control centre. However, even though the control centre facilitates the communication, it should not be able to see the identities of the communicating parties or any data that are exchanged.

To separate the identity management from the commercial system entity, i.e. the control centre, the registration of users is delegated to a separate authority. Namely, all administrative tasks are performed by a separate trusted party, an *administration centre*. Those tasks include initial registration of all users of the system, i.e. verification of their identities and issuing anonymous credentials or smart cards, and invoicing the users for the utilized services. The caregivers who register for using the system obtain an anonymous credential at registration[1]. The credential records their identifying information, but also the level of medical training and their expertise, as this information is relevant for the care provisioning they offer to the patients. This way, when they authenticate with the control centre, they do not need to disclose their identity to prove that they are valid system users or that they are entitled to access patient's medical recordings in the base station.

More details on the architecture of such a commercial, but privacy-aware eHealth system can be found in the work of Milutinovic and De Decker (2013). In this paper, we describe how such architecture can be used to protect all user data, including identities of patients and caregivers, while at the same time ensuring that the authorized individuals can access the data they require for provisioning the care to the patient.

3.2.1 Basic system functioning. This section provides a brief description of the basic functionality of the described eHealth system. First of all, all users who wish to utilize the services of the control centre, both patients and caregivers, are required to register with the administration centre. For the patients, this registration entails proving personal details (such as identity and address) and creating a service-level agreement. This agreement specifies the services the patient wishes to utilize and possible invoicing details. As a result of their registration, the patients obtain a smart card which records their personal details and holds public–private key pairs for encryption and signing and the corresponding certificates. These keys serve to enable authenticity and secrecy of communication with the caregivers. The caregivers who register prove their personal details, while medical personnel additionally provide proofs of medical training and specialization. These data are recorded in an anonymous credential issued to the caregiver and signed by the administration centre. Using the anonymous credentials allows the caregivers to disclose only chosen attributes from it and prove that they are certified by the administration centre.

When the patients obtain the smart card and have the indoor equipment installed, they register remotely with the control centre. The registration is done via the base station using the smart card. The identity of the patient is not disclosed, and a pseudonymous relation with the control centre is established. Upon authentication, the control centre creates a network with a star topology, with the patient's pseudonym representing the central node. The caregivers who subsequently register to connect to the patient will be added to this network as branch nodes (Figure 2). This network is used to maintain the information about the connections between patients and their caregivers, while keeping the identities hidden.

When registering with the control centre, a caregiver uses the anonymous credential to create a pseudonym, which is recorded in a new node of the patient's care network. To ensure accountability, caregivers' personal information (identity, contact and proofs of

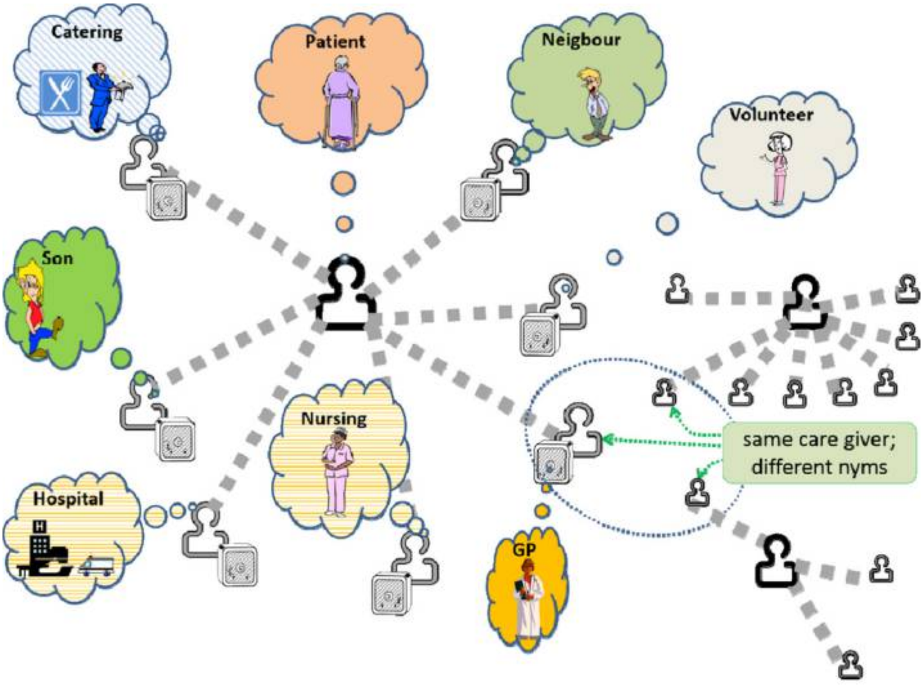


Figure 2.
Patients' networks of caregivers, as maintained by the control centre

Note: The black silhouettes represent patients and grey caregivers, which are all pseudonymous. additionally, caregivers belonging to multiple networks are identified with different pseudonyms in each of them for preventing side-channel information leakage qualifications in case of medically trained individuals) is also stored encrypted with the public key of the trusted device. This information is used to allow authorized entities to authenticate the caregivers before granting them certain rights, or for contacting the caregivers.

To ensure that only authorized access to patient's data can take place, the creation of the patient's network is performed with strict checks. Admission of a caregiver to a care network of a patient is allowed only if the caregiver has been invited by the patient and has been given an appropriate digital token which proves that. The control centre also verifies that the patient approves the connection after verifying the real identity of the caregiver. When a patient approves the connection, it also assigns the authorizations to the caregiver. These authorizations determine what kind of requests the caregiver can make and which access rights are granted to him. For instance, only medically trained personnel can make requests to inspect the stored health information of the patient. The fine-grained authorizations are stored in the base station. An overview of their access rights is also issued to the caregivers in an anonymous credential. The credentials are issued by the trusted device, on patient's request.

With the authorizations assigned to them, the caregivers can make requests to access the data in the base stations of the patients. They can prove only a chosen subset of their authorizations when requesting access (Section 3.1.1). These requests are relayed by the control centre, where the first level of access control is performed. However, the access control here can only be coarse-grained, as the protocols entail that the control centre cannot learn the specific authorizations or roles of caregivers, for improved privacy. Fine-grained access control is then performed in the base stations, where the information does not need to be anonymized or minimized.

3.2.2 System properties. This section provides the rationale behind the described design – the initial goals and design decisions, and describes the resulting privacy properties:

- *Goals*: The system architecture was created for a commercial provision of the eHealth service. The central entity is supposed to connect the patients to their caregivers of choice and other service providers, but due to its commercial nature, it cannot see any identifying or sensitive data. Therefore, the care networks need to be anonymized as much as possible. In general, data disclosure based on a need-to-know principle is chosen.
- *Design decisions*: To minimize the amount of data that is disclosed to the control centre, it only sees the pseudonyms of all parties. Moreover, if a caregiver is a member of care networks of more than one patient, he is represented with a different pseudonym in each of them. For enrolment in a patient's network, anonymous credential technology is used because of its selective disclosure property. This is necessary, as traditional credential technologies require showing the complete content of a credential to prove its validity. This would disable the users to hide their personal information, while showing only the required attributes. Furthermore, by using anonymous credentials, different interactions of one user with the administration centre and with the control centre remain unlinkable, even if the control and the administration centre collude.
- *Results*: The described design achieves the network anonymization, as none of the parties discloses their identities or other personal information. Furthermore, one

entity is not reusing its pseudonym in multiple networks, so deliberate or accidental data leaks in one network do not affect other patient networks.

3.3 Privacy-preserving mechanisms

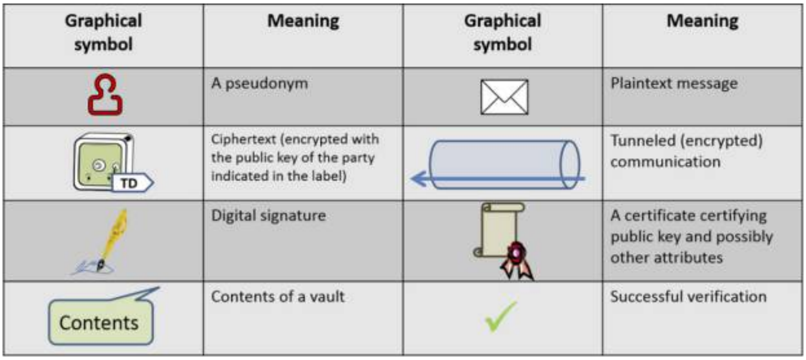
This section describes in detail the protocols for handling caregivers' requests for accessing patient data in the base stations and for contacting a caregiver in case of an emergency. The goal of this protocol design is to ensure that required data are available to authorized parties, but are at the same time appropriately protected. For instance, if the patient is in need of urgent assistance, the system ensures that she is given timely and appropriate care, but emergency procedures do not allow data to leak or allow imposters to defeat the security of the system. Even though the communication between the patients and their caregivers is performed through the system, all commercial parts of the system, such as the control centre, are not able to see the data passing by. Additionally, they are not able to request any data stored in the base stations of patients. The base stations themselves impose strict access control and authenticate the requesting parties.

3.3.1 Controlled access to patient data. This section describes a protocol for privacy-preserving access to patient data. The goals of this proposal, the design decisions taken and the resulting properties are as follows:

- *Goals*: As the base station represents the storing point for the recordings of health parameters and other patient data, the caregivers should be able to make requests to access it remotely. These requests are sent to the base station via the control centre. However, the control centre should not be able to see the specific details of the request or the identity of the caregiver. In case the requested access is granted, the data that being exchanged should also be hidden. Finally, the accountability needs to be provided as well, so that when an attempt at misuse is detected, it allows to deanonymize the perpetrator.
- *Design decisions*: To minimize the data that the control centre sees, the caregivers not only keep their identities hidden, but they also do not disclose their pseudonyms. Learning the pseudonym would allow the control centre to create a profile and analyse patterns of a caregiver's interactions. This may lead to inferring the role of the caregiver and the type of assistance that the patient needs. Therefore, the data that the caregivers disclose are kept to a minimum. In fact, they only need to prove that they are connected to the patient in question and that they have the required rights to make the request. These rights are proven by presenting a high-level overview of a subset of authorization given by the patient. To prove the authorizations, anonymous credentials are used, because of their selective disclosure property. Furthermore, anonymous credentials allow the owner to only prove properties of the recorded attributes, while the attributes remain hidden[2]. Finally, as the control centre cannot identify the caregiver, verifiable encryption[3] of the identifying information is utilized for providing accountability.
- *Result*: With the taken approach, the control centre facilitates the exchange of information from the base stations to the caregivers, while even the pseudonymous identities of the caregivers are hidden. This way, it is not possible to profile the interactions to deduce information about the care that the patient is

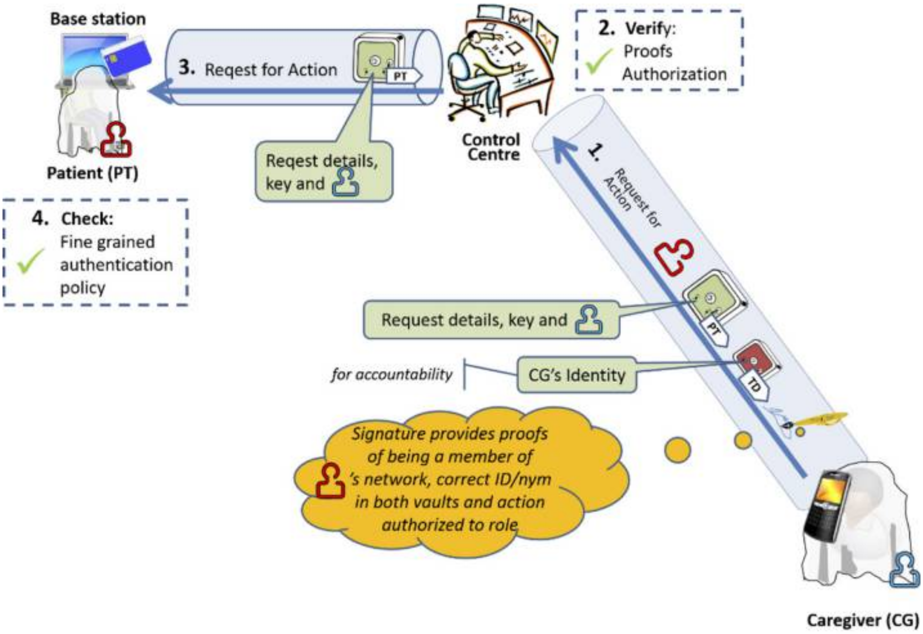
using. Identifying a misuser is still possible through verifiable encryption, which the caregivers utilize to encrypt their identifying information.

The protocol for requesting and accessing patient's data in the base station is shown in Figure 4 and used symbols are explained in Figure 3. When a caregiver wishes to access data in the patient's base station, he initially creates an appropriate request specifying the access details. Then, a fresh symmetric key to be used for communication with the patient's base station is created. This key, pseudonym of



Graphical symbol	Meaning	Graphical symbol	Meaning
👤	A pseudonym	✉	Plaintext message
TD	Ciphertext (encrypted with the public key of the party indicated in the label)	⇐	Tunneled (encrypted) communication
✒	Digital signature	📜	A certificate certifying public key and possibly other attributes
Contents	Contents of a vault	✓	Successful verification

Figure 3. Graphical symbols used in depicting the described protocols and their meanings


Base station
Patient (PT)
3. Reqest for Action
PT
Reqest details, key and
Control Centre
2. Verify: Proofs Authorization
4. Check: Fine grained authentication policy
1. Request for Action
Request details, key and
PT
for accountability
CG's Identity
TD
Signature provides proofs of being a member of 's network, correct ID/nym in both vaults and action authorized to role
Caregiver (CG)

Notes: Vaults represent data encrypted with the public key of the intended receiver, indicated in the index; the tunnelled links represent encrypted communication channels

Figure 4. Protocol for caregiver's access to data in the patient's base station

the caregiver and the request are then verifiably encrypted with the public key of the patient (represented with a vault in Figure 4). This encrypted information is sent to the control centre, to be relayed to the base station of the patient. The control centre is also presented with a part of the request in plaintext and the verifiable encryption allows it to verify that the request that it sees corresponds to the one that is encrypted for the patient. The caregiver also proves that he holds appropriate authorizations (given by the patient in question), by showing a subset of authorizations contained in his anonymous credential (see Section 3.2.1). Finally, for ensuring accountability, the caregiver is required to verifiably encrypt his identity information (ID_{CG}) from the anonymous credential issued by the administration centre with the public key of a trusted third party. The identity thus remains hidden from the control centre, which is still able to check that correct information is encrypted. The trusted device, however, will only decrypt the vault, thus deanonymizing the caregiver, if it receives a signed legal order from a trusted authority. The complete aforementioned transcript is then signed by the caregiver and relayed to the control centre.

Upon reception of a caregiver's request and the accompanying information, the control centre performs all the noted checks, but also stores the received data in case later auditing is required[4]. If the described checks succeed and the authorizations the caregiver possesses allow him to make the specified request, the signed transcript is relayed to the patient's base station. The base station performs similar verifications as the control centre to verify the validity of the request. In case the request is successfully verified, the base station establishes an encrypted communication with the caregiver. The encryption is done with the received symmetric key. The caregiver can then authenticate and prove his identity over this private channel. As the base station records the fine-grained authorizations that are given to all the caregivers that belong to the patient's network and the access control policies of the patient, it accordingly decides whether the caregiver should be granted access to the requested resource. The subsequent communication is also relayed by the control centre, but is not readable by it, as the utilized symmetric key is only accessible to the caregiver and the patient.

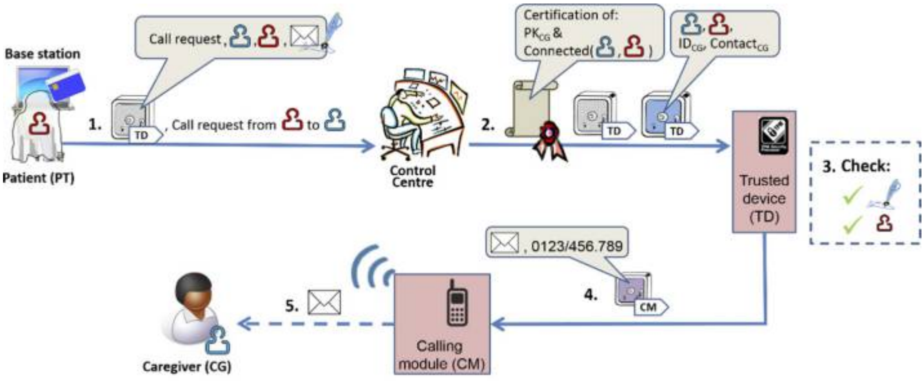
3.3.2 Requesting urgent caregiver's assistance. This section details the protocol that enables patients to contact their caregivers. We first list the rationale and the resulting properties of the protocol:

- *Goals*: When a caregiver needs to be notified that his urgent assistance is needed, a message is sent to him through the system. However, caregiver's contact information must not be disclosed to the control centre, as that would endanger his privacy. Additionally, the responses of a caregiver should be relayed back to the patient, because in case he is not able to accept the task, another caregiver needs to be summoned.
- *Design decisions*: To have the caregivers' contact information available to the calling module, but not disclosed to the control centre or its personnel, this information is stored encrypted. It can only be decrypted by the trusted device, which re-encrypts it for the calling module. The re-encryption is done with strict checks that the request originated from the patient and that only the calling module will be able to access the contact information and the message details. The calling module deletes all the plaintext information after sending the message.

The received response is mapped to the patient's pseudonym, and is relayed back to the patient in an encrypted form.

- *Result*: With the taken approach, the resources of the control centre facilitate informing the caregivers when they need to urgently assist the patient, while not being able to see the contents of the sent messages or the caregivers' contact information. The patients' base stations are also able to receive the caregivers' responses, so that a replacement can be found in a timely manner, when needed.

The detailed protocol is illustrated in Figure 5. If an emergency situation is detected at the patient's site, either through assessment of the sensor measurements or from a patient-initiated alert, a caregiver is required to urgently assist the patient. The control centre's calling module is then used to send the specified messages to provided telephone numbers and then relay the received responses to the patient's base station, keeping them hidden from other parties. The base station of the patient records the policies that determine which caregivers should be contacted in a specific emergency situation – primary and back-up choices. The choice of the caregiver(s) to be contacted is thus performed in the base station based on these policies. The base station initially creates a request (*REQ*) for contacting the specified caregiver and sends it to the control centre. The request notes the pseudonym of the chosen caregiver and the patient, the message to be relayed and is signed by the base station with the patient's signing key. It is encrypted with the public key of the trusted device (*TD*) and is sent to the control centre together with the pseudonym of the caregiver in a *call request*. The control centre relays the request to the trusted device together with the personal information of the specified caregiver, which it stores encrypted with trusted device's public key (cf. Section 3.2.1). The trusted device verifies the signature on the request using the signing certificate of the patient, to make sure that the request does not originate from an unauthorized party. It also checks the stored public key certificate of the caregiver, which records the pseudonym of the patient, to verify that he is indeed a part of the patient's network. The trusted device then uses the encrypted profile of the chosen



Notes: The vault representations denote data encrypted with the public key of the recipient indicated in the index; the envelope represents the specifics of the request and kind of emergency, which are encrypted for the caregiver and hidden from the control centre

Figure 5. Contacting a caregiver in case of an emergency

caregiver to extract the contact information from it. The contact information and the message are then sent to the calling module, encrypted with a symmetric key shared between the calling module and the trusted device. The encrypted request is trusted, as it can only have been created by the trusted device with which the encryption key is shared.

The calling module can also relay the responses to the patient's base station. After sending the message it was instructed to send, the calling module deletes all the information except for the hash of the caregiver's phone number and the pseudonym and the public encryption key of the patient. They are only stored for a limited time frame in which the response is expected. If a response is received from a number, a hash of which corresponds to one of the stored hashes, the module sends the received response to the patient (via the control centre) encrypted with the corresponding public key.

3.4 Flexible privacy policies

The described approach allows to have flexible policies that determine the system functioning. These policies are specified by the patient herself, her guardian or an authorized caregiver and are managed by the base station or the sensors. Sensors' policies are used to determine the boundaries outside of which the measurements are considered to indicate a problem. They can also specify what should be done in such a case. The base station, however, manages a range of policies. Some determine the actions that are taken in case of alerts. For instance, in case of mild disturbance in the health parameters, the base station may give audio or video advice to the patient about the actions that should be taken. Other policies determine which caregivers need to be notified and summoned in case of emergencies detected through the sensor measurements or by a patient-initiated alarm.

Finally, the patient's privacy preferences are also expressed through policies. They are used to control access to the patient's data. These data include: sensor recordings and configurations; caregivers' instructions about actions that patients need to perform (e.g. taking a medication), or their assessment of sensor measurements; and tasks that the patients have specified and that need to be assigned to their caregivers. One example policy is represented in Table I. The possible set of access rights includes:

- Administrative rights (AR), which allow an entity to modify the given access authorizations.
- Write rights (WR) refer to changing the configuration settings or inputting data.
- Read rights (RR), for allowing an entity read-access to the resources of the system (sensor readings or stored information).
- Limited read rights (LRR), which allow an entity to see only limited amount of data. For instance, obtaining only a summary, rather than detailed sensor readings.

All of the access rights may also be conditional. This means that the patient needs to give an explicit permission for each authorized request that is received. For instance, if an authorized caregiver requests for the video to be switched on, the patient is warned and is given the chance to overrule it. Such conditional rights are represented in Table I with an asterisk sign (*) on the authorization. It is also assumed that the patient has read

			Resources			
	Sensors			Caregiver input		Patient input
	Video	Heart rate	...	Assessments	Advice	Patient requested tasks
Patient	{AR}, RR	{AR}, RR	...	{AR}, RR	{AR}, RR	{AR}, {WR}, RR
Relatives						
Guardian	AR, RR*	AR, RR	...	AR, RR	AR, RR	AR, WR, RR
Relative 1	RR*	LRR	...	LRR	RR*	RR*
Relative 2	LRR	LRR	...	/	LRR	LRR
...	...	...	...	...	...	...
Medical personnel						
Specialist	LRR*	WR, RR	...	WR, RR	WR, RR	/
GP	/	WR, RR	...	WR, RR	WR, RR	/
Nurse	/	LRR*	...	LRR	LRR	/
...	...	...	...	...	...	...
Commercial providers	/			/		/

Table 1. A policy of a patient defining access rights of the caregivers

rights to all the data, but in case she is not in a position to perform the task of the administrator, these rights are delegated to her guardian. This is represented with $\{\cdot\}$ notation in the table.

The use of privacy policies ensures the flexibility of the system. The patients are able to easily change their privacy preferences and their authorized caregivers can make changes to other aspects of system functionality. These policies are also extensible and new types of rights can be introduced, when needed.

4. Evaluation and ethical implications

The proposed system is designed with a patient-centric approach. The information managed and stored by the system is controlled by policies. Information flow restrictions are defined as required by applicable legislation, on top of which user-defined policies are applied. These policies express patients' preferences and trust they have in their caregivers. Additionally, the patients tend to be more comfortable with systems running on their side, i.e. in their households (Liu *et al.*, 2011). This would mean that the proposed design would be more attractive than the systems whose main functionality is run remotely. Another requirement identified as important for improving efficiency in eHealth systems is summarization of results before they are analysed by a medical caregiver. The proposed design also allows for this functionality to be provided. Additionally, as this system allows patients to connect to the caregivers they are already familiar with and with whom a trust relationship is established, and as the actions are recorded and can be audited, some important problems of online consultations are avoided (George and Duquenoy, 2008).

In the next subsections, the proposed design is evaluated according to the ethical-assessment frameworks and principles proposed in the literature.

4.1 Collste's ethical assessment framework

The ethical assessment framework put forward by Collste (2008) lists the patient–doctor relationship, responsibility and patient autonomy as main evaluation principles. The following subsections analyse the proposed design from the point of view of the outlined categories.

4.1.1 Patient–doctor relationship. A concern related to the eHealth approach is that the relationship between the patient and his or her medical caregiver would suffer, as the trust, privacy and confidentiality would be threatened. As argued by Collste (2008), the organization of health care and used technology should facilitate the realization of these principles. Accordingly, in the system described in this work, the patients are able to connect to the caregivers they have an established relationship with. Therefore, the issue of care provided by unknown caregivers with no previously established trust relationship is mitigated. The aspect of trust also includes competence. The patients are familiar with the doctors' competence and the system additionally imposes checks on their professional training and limits the allowed actions accordingly. Additionally, the system is offering more information to the (authorized) caregivers, facilitating their decision-making process. The rights of actors, such as access to data and modifications, are further controlled through the system's mechanisms, such as access control.

4.1.2 Responsibility. The data that are communicated for the purpose of care provisioning are controlled by strict regulations. They are defined according to the legislation (system policies) on top of which patient preferences are applied (patient policies). The actions taken in the described system design are recorded (logged) and thus allow for audibility. Therefore, attempts to break one of the rules would be detected and entities willing to act unlawfully could be sanctioned. This means that the need for, and thus a sense of *responsibility* of a caregiver is not lessened through the use of technology. Moreover, the technology is allowing for gathering more concrete evidence for assessing actions taken by the caregivers.

4.1.3 Patient autonomy. The design is aiming to allow a high level of autonomy of patients. They are able to exercise their preferences by choosing their connections and through policies that control actions taken by their caregivers. Additionally, an important property of the described design is that the decision-making by the patients is adjusted according to their level of autonomy. For instance, patients suffering from dementia would not be prompted to give access to their medical data, given that previously unknown entities may count on their insecurity to be granted unrightful access. Together with the system policies about disclosure limitations, which represent the legislative requirements (such as prevention of sending medical data to a cleaning service provider), it prevents unwitting or accidental information leakages.

4.2 Markle Foundation's privacy principles

The Markle Foundation (2008) has outlined principles for a privacy-preserving approach in managing personal health information. The system design described in this work illustrates concordance with this approach. For instance, *transparency* and *purpose specification* are achieved, as the patients in the presented system are aware of their personal health data collection and can *control* it by specifying policies that control access to it. The access control polices also ensure that the *usage of data* is limited to the individuals who are authorized to access it. The *data minimization* is also one of the design principles and the minimal amount of data needed for setting up the care networks is disclosed. Actors in the system can also be held *accountable* if misactions are identified. Additionally, access to the data itself is *secured* from external of internal attacks through cryptographic mechanisms.

5. Conclusions

This paper describes the design and functioning of a privacy-preserving eHealth system that provides medical and domestic care to the elderly and stay-at-home patients. Our proposal is based on a four-tier system architecture that allows the eHealth service to be offered by a commercial entity, while hiding all the private and sensitive data from it. The proposal aims at providing a range of services to the users for ensuring a high level of autonomy. In addition, the patients are able to connect to their regular caregivers, retaining the commitment and trust of an established relationship. The caregivers are also able to get the relevant data they are authorized to see in an easy and timely manner.

Having the eHealth services offered by a commercial entity is an important step towards large-scale deployment of these systems and that is why our proposal is based on that assumption. Also, to be able to offer these systems to the users, privacy protection is of crucial importance. These systems handle medical data, which are highly sensitive and the users would trust the system only if their information is secure. Moreover, even when the patient's medical data are properly protected, information about the patient's health could be inferred indirectly if one knows which specialist is involved in the treatment, or which services are utilized. Therefore, not only the medical data need to be protected, but also the patient's network of caregivers should remain hidden as much as possible.

In this work, we have listed the requirements that a secure and privacy-preserving eHealth system needs to fulfil. These requirements were used as guidelines for the creation of the proposed protocols. They are designed to protect the private information of both patients and their caregivers. We do not focus only on the health-related data, but also on the identities of all users – both elderly or stay-at-home patients and their caregivers. Commercial entities in the system cannot access any sensitive data and disclosure of data is generally kept to a minimum. The protocols allow the authorized caregivers to request and inspect medical information collected by the sensors. They also ensure that in case of an emergency, a caregiver is notified and his attendance is confirmed. Besides data availability and access control, the system provides accountability. This means that if a caregiver tries to gain unauthorized access to the patient's data, it would be detected. Furthermore, the focus is not on the misuse detection, but rather prevention. Strict procedures prohibit attackers – both external and internal, such as unauthorized caregivers or control centre personnel to access the patient's data.

Finally, the proposed design is evaluated against the ethical principles outlined in the literature. It is analysed through the Collste's ethical assessment framework, which lists patient–doctor relationship, responsibility and patient autonomy as main evaluation criteria. Additionally, the privacy principles outlined by the Markle Foundation are mapped onto the described system. The focus of the proposal was respect for autonomy and patient privacy, which are achieved through patient policies. They restrict the access rights given to different caregivers' roles and to individual caregivers. They are also flexible and can be modified to reflect the changes in the patients' care networks and in the eHealth services that the patients utilize. Next to that, patients connect to their regular caregivers, thus retaining the established trust relationships. The sense of responsibility of caregivers is also maintained, as their actions are logged and can be assessed. Therefore, a high level of compliance with established ethical principles is illustrated.

Notes

1. Anonymous credential technology allows the owner of a credential to show only a chosen subset of the recorded attributes and still prove that they have been certified by the trusted issuing authority (Camenisch and Van Herreweghen, 2002).
2. In case traditional credentials were used instead of anonymous credentials, the caregivers would only be able to show the complete list of the authorizations they are granted. This significantly reduces the anonymity set of the caregiver, by comparison of the disclosed authorizations. As the patients' networks already have a limited size, a caregiver would often be uniquely pinpointed.
3. Verifiable encryption is an encryption scheme that allows a party to prove certain properties about an encrypted value without disclosing it. In our system, it allows the caregiver to prove that his identity information is in the vault, without opening it.
4. These data can be used to prove which requests were made, and if it is established that a misuse was attempted, the requesting entity can be deanonymized.

References

Abascal, J. and Civit, A. (2001), "Universal access to mobile telephony as a way to enhance the autonomy of elderly people", *Proceedings of the 2001 EC/NSF Workshop on Universal Accessibility of Ubiquitous Computing: Providing for the Elderly*, *Alcácer do Sal*, *May*, *ACM, New York, NY*, pp. 93-99.

Al Ameen, M., Liu, J. and Kwak, K. (2012), "Security and privacy issues in wireless sensor networks for healthcare applications", *Journal of Medical Systems*, Vol. 36 No. 1, pp. 93-101.

Alahmadi, A. and Soh, B. (2011), "A smart approach towards a mobile e-health monitoring system architecture", *2011 International Conference on Research and Innovation in Information Systems (ICRIIS)*, *Kuala Lumpur*, November, IEEE, pp. 1-5.

Anderson, J.G. (2007), "Social, ethical and legal barriers to e-health", *International Journal of Medical Informatics*, Vol. 76 No. 5, pp. 480-483.

Bajikar, S. (2002), *Trusted Platform Module (TPM) Based Security on Notebook PCS-White Paper*, Mobile Platforms Group, Intel Corporation.

Beauchamp, T.L. and Childress, J.F. (2001), *Principles of Biomedical Ethics*, Oxford University Press, Oxford.

Boulos, M.N., Rocha, A., Martins, A., Vicente, M.E., Bolz, A., Feld, R., Tchoudovski, I., Braecklein, M., Nelson, J., Laighin, G. and Kinirons, M. (2007), "CAALYX: a new generation of location-based services in healthcare", *International Journal of Health Geographics*, Vol. 6 No. 1, p. 9.

Camenisch, J. and Van Herreweghen, E. (2002), "Design and implementation of the idemix anonymous credential system", *Proceedings of the 9th ACM Conference on Computer and Communications Security*, *Kyoto*, *3-6 June*, *ACM, New York, NY*, pp. 21-30.

Cantor, M.D. (2006), "No information about me without me: technology, privacy, and home monitoring", *Generations*, Vol. 30 No. 2, pp. 49-53.

Cavoukian, A., Fisher, A., Killen, S. and Hoffman, D.A. (2010), "Remote home health care technologies: how to ensure privacy? Build it in: privacy by design", *Identity in the Information Society*, Vol. 3 No. 2, pp. 363-378.

Chakravorty, R. (2006), "A programmable service architecture for mobile medical care", *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006, PerCom Workshops*, Sydney, 14-18 March, IEEE, p. 5.

Collste, G. (2002), "The Internet doctor and medical ethics Ethical implications of the introduction of the Internet into medical encounters", *Medicine, Health Care and Philosophy*, Vol. 5 No. 2, pp. 121-125.

Collste, G. (2008), *Ethical, Legal, and Social Issues in Medical Informatics*, IGI Global, Hershey, PA.

Collste, G. (2011), "Under my skin: the ethics of ambient computing for personal health monitoring", in Nagy Hesse-Biber, S. (Ed.), *The Handbook of Emergent Technologies in Social Research*, Oxford University Press, Oxford, pp. 89-110.

Essén, A. (2008), "The two facets of electronic care surveillance: an exploration of the views of older people who live with monitoring devices", *Social Science & Medicine*, Vol. 67 No. 1, pp. 128-136.

Farella, E., Pieracci, A., Benini, L., Rocchi, L. and Acquaviva, A. (2008), "Interfacing human and computer with wireless body area sensor networks: the WiMoCA solution", *Multimedia Tools and Applications*, Vol. 38 No. 3, pp. 337-363.

George, C.E. and Duquenoy, P. (2008), "Online medical consultations: legal, ethical and social perspectives", in Duquenoy, P., George, C. and Kimppa, K. (Eds), *Ethical, Legal and Social Issues in Medical Informatics*, IGI Global, Hershey, PA.

Goldman, J. and Hudson, Z. (2000), "Virtually exposed: privacy and e-health", *Health Affairs*, Vol. 19 No. 6, pp. 140-148.

HIPAA, "Health Insurance Portability and Accountability Act", available at: www.hhs.gov/ocr/privacy/

Hodge, J.G., Jr, Gostin, L.O. and Jacobson, P.D. (1999), "Legal issues concerning electronic health information: privacy, quality, and liability", *JAMA*, Vol. 282 No. 15, pp. 1466-1471.

Jin, Z., Oresko, J., Huang, S. and Cheng, A.C. (2009), "HeartToGo: a personalized medicine technology for cardiovascular disease prevention and detection", *Life Science Systems and Applications Workshop, 2009, LiSSA 2009, IEEE/NIH*, Bethesda, MD, 9-10 April, IEEE, pp. 80-83.

Johnston, B., Weeler, L., Deuser, J. and Sousa, K.H. (2000), "Outcomes of the Kaiser Permanente tele-home health research project", *Archives of Family Medicine*, Vol. 9 No. 1, p. 40.

Jones, V., Gay, V. and Leijdekkers, P. (2010), "Body sensor networks for mobile health monitoring: experience in Europe and Australia", *Fourth International Conference on Digital Society, ICDS'10, St. Maarten*, 10-16 February, IEEE, pp. 204-209.

Jovanov, E., Milenkovic, A., Otto, C. and De Groen, P.C. (2005), "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation", *Journal of NeuroEngineering and Rehabilitation*, Vol. 2 No. 1, p. 6.

Jovanov, E., Raskovic, D., Price, J., Krishnamurthy, A., Chapman, J. and Moore, A. (2001), "Patient monitoring using personal area networks of wireless intelligent sensors", *Biomedical Sciences Instrumentation*, Vol. 37, pp. 373-378.

Jurik, A.D. and Weaver, A.C. (2008), "Remote medical monitoring", *Computer*, Vol. 41 No. 4, pp. 96-99.

Kim, H., Jarochowski, B. and Ryu, D. (2006), "A proposal for a home-based health monitoring system for the elderly or disabled", *Computers Helping People with Special Needs* Springer Berlin Heidelberg, Heidelberg, pp. 473-479.

Kinney, S.L. (2006), *Trusted Platform Module Basics: Using TPM in Embedded Systems*, Newnes, Oxford.

Lake Research Partners, American Viewpoint, and Markle Foundation (2006), "Survey finds Americans want electronic personal health information to improve own health care", available at: www.markle.org/downloadable_assets/research_doc_120706.pdf (accessed 12 November 2014).

Liu, L.S., Shih, P.C. and Hayes, G.R. (2011), "Barriers to the adoption and use of personal health record systems", *Proceedings of the 2011 iConference*, *Seattle, WA*, *8-11 February*, *ACM*, pp. 363-370.

Lo, B.P., Wang, J.L. and Yang, G.Z. (2005 May), "From imaging networks to behavior profiling: ubiquitous sensing for managed homecare of the elderly", *Adjunct Proceedings of the 3rd International Conference on Pervasive Computing*, *Munich*, *8-12 May*, pp. 101-104.

Markle Foundation (2008), *Connecting for Health Common Framework*, Markle Foundation, New York, NY.

Mehta, D.D., Zanartu, M., Feng, S.W., Cheyne, H.A. and Hillman, R.E. (2012), "Mobile voice health monitoring using a wearable accelerometer sensor and a smartphone platform", *IEEE Transactions on Biomedical Engineering*, Vol. 59 No. 11, pp. 3090-3096.

Milutinovic, M. and De Decker, B. (July 2013), "Comprehensive eHealth system design for privacy protection", Technical Report (CW Reports), Department of Computer Science, KU Leuven, Vol. CW643.

Nordgren, A. (2013), "Personal health monitoring: ethical considerations for stakeholders", *Journal of Information, Communication and Ethics in Society*, Vol. 11 No. 3, pp. 156-173.

Otto, C., Milenkovic, A., Sanders, C. and Jovanov, E. (2006), "System architecture of a wireless body area sensor network for ubiquitous health monitoring", *Journal of Mobile Multimedia*, Vol. 1 No. 4, pp. 307-326.

Pantelopoulos, A. and Bourbakis, N.G. (2010), "A survey on wearable sensor-based systems for health monitoring and prognosis", *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, Vol. 40 No. 1, pp. 1-12.

Pantelopoulos, A. and Bourbakis, N.G. (2010), "Prognosis – a wearable health-monitoring system for people at risk: methodology and modeling", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 14 No. 3, pp. 613-621.

Pascu, T., White, M., Beloff, N., Patoli, Z. and Barker, L. (2013), "Ambient health monitoring: the smartphone as a body sensor network component", *InImpact: The Journal of Innovation Impact*, Vol. 6 No. 1, pp. 62-65.

Patient Rights in the EU (2008), "A general overview of the national patient rights legislation in Europe", available at: http://europatientrights.eu/

Rash, M.C. (2005), "Privacy concerns hinder electronic medical records", *The Business Journal of the Greater Triad Area*, April, pp. 4-6.

Ren, Y., Pazzi, R.W.N. and Boukerche, A. (2010), "Monitoring patients via a secure and mobile healthcare system", *Wireless Communications, IEEE*, Vol. 17 No. 1, pp. 59-65.

Rippen, H. and Risk, A. (2000), "e-Health code of ethics", *Journal of Medical Internet Research*, Vol. 2 No. 2.

Rodrigues, R.J. (2000), "Ethical and legal issues in interactive health communications: a call for international cooperation", *Journal of Medical Internet Research*, Vol. 2 No. 1, p. e8.

Sarela, A., Korhonen, I., Lotjonen, J., Sola, M. and Myllymaki, M. (2003 April), "IST Vivago®-an intelligent social and remote wellness monitoring system for the elderly", *4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, *Birmingham*, 24-26 April, pp. 362-365, IEEE.

Scalvini, S., Baratti, D., Assoni, G., Zanardini, M., Comini, L. and Bernocchi, P. (2013), "Information and communication technology in chronic diseases: a patient's opportunity", *Journal of Medicine and the Person*, Vol. 12 No. 3, pp. 1-5.

Steele, R., Lo, A., Secombe, C. and Wong, Y.K. (2009), "Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare", *International Journal of Medical Informatics*, Vol. 78 No. 12, pp. 788-801.

Sum, K.W., Zheng, Y.P. and Mak, A.F.T. (2005), "Vital sign monitoring for elderly at home: development of a compound sensor for pulse rate and motion", *Studies in Health Technology and Informatics*, No. 117, pp. 43-50.

Tabar, A.M., Keshavarz, A. and Aghajan, H. (2006), "Smart home care network using sensor fusion and distributed vision-based reasoning", *Proceedings of the 4th ACM International Workshop on Video Surveillance and Sensor Networks, Santa Barbara, CA, 23-27 October, ACM, New York, NY*, pp. 145-154.

Tang, P.C., Ash, J.S., Bates, D.W., Overhage, J.M. and Sands, D.Z. (2006), "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption", *Journal of the American Medical Informatics Association*, Vol. 13 No. 2, pp. 121-126.

Tsukiyama, T. (2014), "Ambient sensor system for in-home health monitoring", *AMBIENT 2014, The Fourth International Conference on Ambient Computing, Applications, Services and Technologies*, Rome, 24-28 August, pp. 47-50.

Varshney, U. (2007), "Pervasive healthcare and wireless health monitoring", *Mobile Networks and Applications*, Vol. 12 Nos 2/3, pp. 113-127.

Whitehouse, D. and Duquenoy, P. (2009), "Applied ethics and eHealth: principles, identity, and RFID", *The Future of Identity in the Information Society*, Springer Berlin Heidelberg, Heidelberg, pp. 43-55.

About the authors

Milica Milutinovic is a Doctoral Researcher and a Teaching Assistant at the Computer Science Department of the KU Leuven University, Belgium. She is a member of the research group iMinds-DistriNet. She has obtained her bachelor's and master's degree at the University of Belgrade, Faculty of Electrical Engineering. Her research interests are security and privacy, with special focus on privacy-preserving identity management. In particular, she is investigating privacy solutions for systems deployed in practice, such as electronic health or value-transfer systems.

Bart De Decker obtained his master's degree in engineering and his doctorate degree in applied sciences (computer science) from the Katholieke Universities Leuven (KU Leuven), Leuven, Belgium, in 1981 and 1988, respectively. He is currently Professor of Computer Science at the KU Leuven and Vice-Chair of TC11 (Security and Privacy Protection in Information Processing Systems) of IFIP. He is also a member of ACM. He has authored or co-authored more than 200 reviewed scientific publications. His main research interests are ICT security, privacy and anonymity. Bart De Decker is the corresponding author and can be contacted at: Bart.DeDecker@cs.kuleuven.be