Project no.:	**610658**
Project full title:	**eWALL for Active Long Living**
Project Acronym:	**eWALL**
Deliverable no.:	**D2.4**
Title of the deliverable:	**Ethics, Privacy and Security**

Contractual Date of Delivery to the CEC:	**30.04.2014**
Actual Date of Delivery to the CEC:	**29.04.2014**
Organisation name of lead contractor for this deliverable:	**Stelar Security Technology Law Research**
Author(s):	**Matthias Pocs, Albena Mihovska, Prateek Mathur, Julia Himmelsbach, Liljana Gavrilovska, Octavian Fratu, Alexandru Martian, Sofoklis Kyriazakos**
Participants(s):	**P01, P06, P08, P09, P13**
Work package contributing to the deliverable:	**WP2**
Nature:	**R**
Version:	**1.0**
Total number of pages:	**32**
Start date of project:	**01.11.2013**
Duration:	**36 months – 31.10.2016**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610658

Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	**X**

Abstract:

In the project eWALL we as technical and legal partners analyse privacy and data protection aspects of new healthcare use cases. The project aims to build on regulations and standards to improve the market environment for measuring devices, systems and services. As a first-of-its-kind approach we design privacy protecting technical concepts and a Privacy-by-Design method for the development of eHealth systems. While the (confidential) Deliverable 2.8 focuses on this Privacy-by-Design method this Deliverable investigates the general ethical, privacy and security aspects of the eWALL sensing devices, system, services and applications. The work contributes to the public acceptance of the eWALL results and the standardisation of the Privacy-by-Design method.

Keyword list: confidential and secure electronic data transmission; sensing devices; European Union data protection legislation; legal interoperability; proportionality; fundamental rights; telemonitoring use cases.

Document History

Version	Date	Author	Description
0.11	Feb 20, 2014	M. Pocs (STELAR)	Drafted first ToC for submission to all partners
0.12	Mar 10, 2014	A.Mihovska, P.Mathur (AAU)	Contributed to Section 3
0.13	Mar 12, 2014	A.Mihovska, P.Mathur (AAU)	Contributed to Section 5
0.14	Mar 14, 2014	L. Gavrilovska (UKIM)	Contributed to Section 5
0.15	Mar 14, 2014	O. Fratu, A. Martian (UPB)	Contributed to Section 5
0.16	Mar 14, 2014	A.Mihovska, P.Mathur (AAU)	Contributed to Section 3
0.17	Mar 18, 2014	M. Pocs (STELAR)	Compiled contributions
0.18	Mar 28, 2014	A.Mihovska, P.Mathur (AAU)	Contributed to Section 5
0.19	Mar 31, 2014	L. Gavrilovska (UKIM)	Contributed to Section 5
0.20	Mar 31, 2014	M. Pocs (STELAR)	Compiled early second contributions
0.21	Apr 1, 2014	A.Mihovska, P.Mathur (AAU)	Contributed to Section 5
0.22	Apr 3, 2014	J. Himmelsbach (ATE)	Contributed to Section 3
0.23	Apr 3, 2014	O. Fratu, A. Martian (UPB)	Contributed to Section 5
0.24	Apr 4, 2014	M. Pocs (STELAR)	Compiled second contributions and considered comments of conference call
0.25	Apr 10, 2014	M. Pocs (STELAR)	Finalised document for approval by WP2 leader
0.26	Apr 16, 2014	J. Himmelsbach (ATE)	Optimised by WP2 leader
0.27	Apr 17, 2014	M. Pocs (STELAR)	Finalised for approval by Technical Manager
1.0	Apr 27, 2014	Sofoklis Kyriazakos (AAU)	Final, Approved

Table of Contents

1 Executive Summary

There is a gap for specifying the normative non-technical requirements of ethics and privacy, on one hand, and the non-normative technical requirements of security, on the other. Filling this gap will help the consortium develop an ethically acceptable design approach.

This Deliverable develops a framework preparing the Privacy-by-Design approach. Since ethical values and legal requirements will guide the development of privacy protecting technical concepts throughout the project's lifetime we outlined the normative concepts of consent, independent living, dignity, etc. as well as the relevant concepts of privacy and data protection law. With the help of technical partners we considered the state of the art of security measures such as access control, cryptography and network security. In addition we explored to what extent the security measures fulfil the system requirements of the project eWALL.

2 Introduction

The acceptability of sensor-based eHealth system depends on the risks felt by older adults, caregivers, hospitals, public authorities and policymakers. In healthcare applications risks of sensor networks pose serious problems to the individual who is using the sensor devices because attackers may misuse personal data and harm the data subject. Since healthcare applications of sensor networks and conventional Wireless Sensor Networks (WSN) applications are similar, most of their security threats are equivalent.

Security threats and attacks can be classified as passive and active. For example a passive attack may occur while routing data packets in the network. Attackers may change their destination or make routing inconsistent. They may also "steal" health data by eavesdropping to the wireless communication media. Active attacks cause greater damage than their passive counterparts. For example attackers may find the location of the user by eavesdropping which could lead to life threatening situations. The common design of sensor devices incorporates limited external security features and therefore, makes them prone to physical tempering. This increases the vulnerability of the devices and poses more complex security challenges. Most commonly the attacks in health monitoring are related to eavesdropping and modification of medical data, forging of alarms on medical data, denial of service, location and activity tracking of users, physical tampering with devices and jamming attacks. Also people with depraved intent may use the information for harmful activities. The generic attacks, which can occur in a WSN-based healthcare system, are classified as:

- Data modification — The attacker can delete and/or replace part or all of the information and send the modified information back to the original receiver to achieve some illegal purpose. Health data is the most vital one in this case of attacks. Modifying them may result in system failure and cause severe problems regarding the persons' health.
- Impersonation attack — If an attacker eavesdrops a wireless sensor node's identity information, it can be used to deceive the other nodes by impersonating as a valid sensor node.
- Eavesdropping — In case of open (unsecure) wireless channels, any opponent can intercept radio communications between the wireless sensor nodes.
- Replaying — The attacker can eavesdrop a piece of valid information and resend it to the original receiver after a while to achieve the same purpose in a totally different case.

These risks have ethical, legal and technical dimensions which are addressed by this Deliverable. This Deliverable reports on the ethical, privacy and security aspects in Task T2.4 which is the basis for the Privacy-by-Design method development in that same Task. It specifies the generic and specific system requirements of "Security," "Privacy," "Traceability," and related requirements defined in the Deliverable D2.1 (D2.1 v1.0 pp. 49ff.). Concerning the system architecture we propose security measures for the architectural components of the "Remote Gateway," "Cloud Data Management" and "Security and Privacy Management" foreseen in the Deliverable D2.3 (D2.3 v0.71 pp. 25f.). Whereas security aspects are centred on the technical system, analysing ethical values for eHealth systems will help Privacy-by-Design service providers to assess the risks to fundamental rights of primary users and to develop first technical proposals that mitigate those risks.

3 Normative ethics

In order to counter the risks for elderly using sensor-based eHealth systems we chose to develop and apply technical concepts from privacy and data protection law. Since for new technologies there are no specific legal provisions one has to interpret the legal principles in the light of ethical norms. Concerning eHealth, these values are important because the industry faces the problem of wasted investment into technologies that are later not accepted by the public. By following ethical considerations manufacturers can take the opportunity to create the technical conditions for legal, social and political acceptance and increase the purchase of their products and services.

As theories that prescribe how people ought to act, ethical norms are in particular defined in constitutional law such as the European Charter of Fundamental Rights[1] and in disciplines like sociology and politics. As a yardstick, we take the fundamental rights of the older adults and other related ethical requirements to specify what they mean for privacy and security of sensor-based eHealth systems (see on the concept of legal technology design [20]).

3.1 Fair decision-making

According to paragraph 2 of Article 8 of the EU Charter data must be processed fairly. This is specified by the fundamental right to an effective remedy according to Article 47 of the EU Charter which entitles everyone whose rights and freedoms guaranteed by the law are violated to an effective remedy before a tribunal. Everyone has a right to a fair hearing by an independent and impartial tribunal and to the possibility of being advised, defended and represented. This right includes the need to resolve false system decisions as an anticipated fair trial.

The eWALL system will take diverse decisions for the primary users and the secondary users, based on the inputs received from the various sensing and monitoring devices deployed in the home. The system is supposed to play a critical role in assisting and managing various issues and aspects that could help improve the Quality of Life (QoL) of the older primary users. Accordingly, the system has to determine the possible flexibility the user will be offered for accomplishing a given task such as the amount of exercise and amount of food consumed.

Similarly the system is expected to take a fair decision in determining the extent of criticality of a particular issue, and accordingly decide the extent of alarm to be raised, e.g., waiting a few hours, say, till the next morning, or the issue has to be dealt in middle of the night itself. Overall the decision making should be such that the system is unobtrusive on the primary user in his or her day-to-day life. Also, the system should be unobtrusive on the informal secondary user. E.g. the informal caregivers should not be alarmed in the middle of the night if the issue can wait till the next morning.

Having considered the ethical requirement, we can also assess to what extent fair decision-making, justice and effective remedy in eWALL fulfil the user requirements of unobtrusiveness, modularity and flexibility as defined in the Deliverable D2.1 (D2.1 v1.0 pp. 44f.). Fair decision-making promotes unobtrusiveness because it reduces the need for manual follow ups of false reporting by caregivers. It facilitates modularity by ensuring that software and hardware components could be added and/or removed easily according to users' needs and that the system is seen as a framework which allows customisation. In addition, fair decision-making improves adaptation and flexibility because the system adjusts its services according to the users' cognitive and/or physical abilities,

[1] Retrievable from: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

needs (of the primary but also of the secondary users), the ecosystem and particular features of primary user's home.

3.2 Privacy & data protection

According to Articles 7 and 8 of the EU Charter people have the right to protection of their privacy and personal data. The right to privacy entitles everyone to respect for his or her private and family life, home and communications. The right to data protection entitles everyone to the protection of personal data concerning him or her. According to the second paragraph of Article 8 personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The Charter also guarantees that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Paragraph 3 of Article 8 stipulates that compliance with these rules shall be subject to control by an independent authority.

Whereas other international organisations have a longer tradition of dealing with the concept of privacy, the European Union has already specified the notion of data protection in legislative acts such as the Data Protection Directive 95/46/EC. Data protection law is made up of a broadly recognised set of principles: lawfulness, profiling prohibition, data availability, purpose limitation, data security, data subject rights, anonymity, responsibility and accountability. Please see Section 4 Privacy and data protection law for a more detailed analysis of these principles in the eWALL context.

The various stakeholders involved in the project should ensure that all the relevant information gathered through the sensing and monitoring devices and the overall system is not misused and well protected. The right to privacy includes the right to control personal data. That is, the user must be aware of the data and the time period for which they are stored and the people who have access to the information. Further, the user has the right to object to the data processing.

3.3 Consent & autonomy

As mentioned above the second paragraph of Article 8 of the EU Charter personal data must be processed on the basis of the consent of the person concerned or some other legitimate basis laid down by law. There are more specific requirements for consent defined in Article 2 of the Data Protection Directive 95/46/EC (soon Article 4 of the Data Protection Regulation) and by European data protection authorities [33] ("informed" and "explicit" consent). This should aim to obfuscation of functionalities of a technical system. The requirement of consent is an expression of freedoms which are also guaranteed by Article 6 ("everyone has the right to liberty") and the following Articles as well as the freedoms of movement according to the Articles 21, 45, 49 and 56 of the Treaty on the Functioning of the European Union (TFEU).

The system should perform its designated function involving monitoring and sensing of various aspects related to the primary user in a manner such that they are well aware of the functioning of the system in a larger context. The system should preferably inform the user in a suitable manner of the various activities and actions of monitoring and sensing using basic non-technical terminology. An informed consent ensures transparency and that the users are aware of the relevant aspects of the system, such as the system's functionalities and the monitored and stored data, before they start using the system. The users will not only know about the benefits but also about the potential risks, privacy impacts and ethical concerns. The informed consent will be handed out as a written document and must be accurate and understandable to allow an autonomous and voluntary decision by the potential user. If users cannot understand or be fully aware of the content to which they are

expected to consent, e.g. due to dementia, the informed consent has to be signed by the user's guardian. It is crucial, that if the consent is signed, the service provider is not obviated from the liability.

As stated in Section 3.2, the system should not force the primary users to do anything but leave them a fair room of doing a certain activity in their own way. It should not encroach on the freedom of the users. Overall, the system functioning and operation should be such that it benefits the primary user and the other stakeholders, but at the same time it should not trigger a feeling in the primary user that his or her freedom and personal space has been encroached on by the system.

3.4 Rights of the older adults

The Charter of Fundamental Rights of EU includes crucial non-discrimination principles. Article 25 specifically stipulates for older adults that the European Union recognises and respects the rights of the older adults to lead a life of dignity and independence and to participate in social and cultural life. Article 26 relates to persons with disabilities and provides that the European Union recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community. These fundamental rights are an expression of equality right of non-discrimination enshrined in Article 21 of the Charter. Accordingly any discrimination based on any ground shall be prohibited. Beside other fundamental rights, these rights have to be respected by all aspects of the system.

The system operation and design should be well suited to the primary user. There should be some flexibility in changing the way monitoring and sensing units function as per some specific inputs and requirements by the primary users. That is, the specific opinion of the primary user regarding a specific issue or point should be taken into account during the initial deployment of the system. Similarly, the primary users could voice their opinion and even dissatisfaction regarding a specific issue or the overall system to any of the other concerned stakeholders.

Suitable redress mechanisms to address the raised opinions should be obligatory on other stakeholders involved. The system should act as an assistive agent and it should not hinder the older adults from exercising their rights including appropriate inclusion and acceptance by the society, assistance by the neighbourhood if required and harming any existing friendly or familiar contact.

The system should work as a friendly assistive agent with the only goal of improving QoL. The system should not function and operate in any manner that could be discriminating for a given primary user. Discrimination could target ageism-related topics but, following concepts like intersectionality, also other aspects, such as gender, ethnicity, cultural differences, stigmata regarding health status, educational level etc. Effective remedy and justice to the primary user for any dissatisfaction that could arise due to possible perceived and actual discrimination should be ensured by the other stakeholders involved.

The eWALL system is aimed at a wide group of older users with varying needs for assistance. It is to be expected that the eWALL system will be able to provide a great number of applications. However it cannot be expected that all users will profit from having all applications available. Therefore the system should be tailored individually for each user, so that users do not have to deal with applications they do not need.

3.5 Independent living

International and domestic human rights legislation, such as the European Charter of Fundamental Rights, define dignity as an essential human right. In detail Article 1 of Charter states that human

dignity is inviolable and must be respected and protected. Moreover human dignity is the basis of fundamental rights and must be respected even where other rights are restricted. The dignity of older users is not only ensured by decreasing the feeling of being a burden for others and enabling a more independent living, but it is realised in the interaction with the system itself too in order to meet concepts of a "behavioural dignity," i.e. dignity which is realised in the behaviour and social actions. Therefore, the system has to respect the decisions and preferences of the user and must not obtrude decisions or force the users into unwished behaviour. Hence, independent living includes not only independency from other humans but also independency from the system.

The system is expected to assist in the daily routine of the primary user, especially by providing some useful or vital information in regard to certain activities such as meals, medicine and daily exercise. The system is not expected and should not hamper the daily life of the primary user by involving in every action and activity throughout the day. The primary users are older people who face a societal exclusion and loneliness to a significant extent, due to the younger population's feeling of being burdened in handling the issues of their elders.

The older adults do not want themselves to be considered as a burden, and therefore it is necessary that the system only assists them to a certain extent and does not give them a feeling that they are totally dependent on the system for their day to day life. This way their dignity would be maintained which plays a significant role in ensuring good QoL.

Having considered the ethical requirement, we can also assess to what extent independent living and human dignity in eWALL fulfil the user requirement of unobtrusiveness as defined in the Deliverable D2.1 (D2.1 v1.0 pp. 44f.). Independent living promotes unobtrusiveness by respecting the user's flow of action. Interruption takes place only when it is necessary and should be perceived with the precisely the degree of importance it deserves. The messages from the various eWALL services are prioritised and follow a consistent aesthetic and communication style.

3.6 Health care & access to technology

According to the first paragraph of Article 168 of the TFEU a high level of human health protection shall be ensured in the definition and implementation of all European Union policies and activities. As an expression of solidarity the Charter guarantees in Article 35 the fundamental right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. This right to health care and the European Union's duty to protect human health at a high level includes access of older adults to technology and prevention of digital divide.

The system should ensure that required health and medical assistance is available to the primary user and it is not substituted by the system through any procedure or activity to be undertaken by the primary user, based on the criticality of the particular health aspect. The procedure adopted by the system for addressing a health condition should be in line with the public health policy of the specific country where the primary user is based, and broadly those of the European Union. The primary user should have access to the best possible solutions for the various electronic monitoring and assistance activities, utilizing the accepted technology standards in respect to the various system components. The system should be adaptable to changing needs of the primary users by bringing changes to the applications. Related to this, the primary user should have access to the latest technology related to eHealth monitoring systems. The system should be adaptable and modifiable accordingly, and should not lead the primary user into a digital divide in the long run by lagging behind. Hence, the system should not lead to a widening of the digital divide, that is, social exclusion from digital and information technology, but contribute to the inclusion of older adults

into the information society by providing accessibility for different user groups and their specific needs.

Having considered the ethical requirement, we can also assess to what extent public health policy, solidarity in health care, access to technology and prevention of digital divide in eWALL fulfil the user requirement of adaptation, minimum input, reliability and motivation as defined in the Deliverable D2.1 (D2.1 v1.0 pp. 44f.). Health care promotes the requirements because it is adaptive to the users' needs, requires minimum possible input from the user and the services and interface are reliable to enable trust to the system. It also improves reliability by preferring robust interaction modalities over fuzzier ones and a strategy to prevent and fix errors caused by broken sensors, applications, etc. Usage of the system in accordance with the ethical requirement of health care is also motivating.

3.7 Proportionality & mission creep

When new information and communication technologies interfere with rights and freedoms one must respect the ethical and legal principle of proportionality as defined in national constitutions and the EU Charter. For example, Article 52 of the Charter stipulates that any limitation on the exercise of the rights and freedoms recognised by the Charter are subject to the principle of proportionality and limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Accordingly, the benefits for health care must be balanced with the impact on the rights and freedoms of the older adults. The principle of proportionality includes the prevention of mission creep, also referred to as "function creep," by taking precautions against misuse of technology originally intended for a legitimate use.

As mentioned above, ICT solutions have the potential to support older adults' independence, dignity, inclusion and health. Nevertheless, inappropriate usage can also damage the well-being. Therefore, the system should work primarily to assist the primary user in various activities related to their day-to-day life as part of the ageing population. It should work as an eHealth system and all stakeholders should utilise the system solely for this purpose. Any additional objective to be accomplished through the system would not be desirable. If there is consensus amongst some stakeholders to utilise the system for any additional purpose, it would be obligatory for them to bring all users on board, and ensure that the system's initial purpose of assisting the older adults is not compromised.

In addition the system should only gather personal data, if the data is adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purpose for which the data is obtained. In other words the benefits of the gathered data and the interference with the user's privacy have to be balanced. Moreover the system should not be imposed on older adults or create an "artificial" need for functionalities or the system itself.

4 Privacy and data protection law

Privacy and data protection law is made up of broadly recognised legal principles. This Section analyses the legal requirements for the eHealth sector. Since the legal requirements are too generic to give guidance for engineering the ethical values outlined in the previous section help specify privacy law and develop technical requirements.

4.1 Lawfulness

The principle of lawfulness covers several aspects of legal requirements [34] [30]. From other threats to the health of primary users the medical partners have to distinguish threats to a primary user's life. This is necessary to enforce the balance between the ethical values of health care and privacy. In addition, they have to distinguish threats that will realise immediately from other threats. In such cases there is no time to check lawfulness in advance. The knowledge about the medical history and health-related behaviour can either rest on facts or mere assumptions. Medical partners have to distinguish facts from assumptions before they are allowed to request more data about primary users. In internal and external data sources medical partners have to distinguish according to the degrees of reliability of those sources. One should admit behavioural data as a basis for the threat prediction if medical partners establish a high reliability of data originating in external sources. The medical partners have to distinguish between the data subjects to avoid third parties of being involved in notifications to caregivers, in particular, those in the older adults's social environment. Since independent auditors need to verify whether medical partners meet the legal requirements the manufacturer should assist medical partners in giving the auditor the information he or she needs to check the lawfulness of the data processing.

4.2 Profiling prohibition

The principle of profiling prohibition prevents medical partners from taking system decisions like alarms for granted without sufficient human verification and covers several aspects of legal requirements [34] [30]. Medical partners should avoid confusion of emergencies with false alarms. In particular the manufacturer should enable medical partners to correct inaccuracy factors of behavioural data. They should also enable medical partners to limit the number of false alarms inherent to the automatic decision making of home sensing and behavioural reasoning. In profiling data subjects have a right to know the logic behind automatic decisions that entail adverse effects for them. The manufacturer should enable medical partners to describe the logic of the profiling. Since auditors have to verify that medical partners meet the legal requirements, the manufacturer should enable medical partners to check the number of false alarms in pilot real-life mode. Caregivers have to manually double-check notifications before taking physical measures on primary users. Therefore manufacturers should offer tools assisting in this task. One should draw special attention to how manufacturers can improve the caregiver's ability to tell notifications apart from false alarms.

4.3 Data availability

The principle of data availability covers several aspects of legal requirements [34] [30]. One has to avoid situations where caregivers cannot prevent threats to a primary user's life because of a lack of information. Manufacturers should enable medical partners to make available the data to several caregivers with equivalent tasks. While it is a requirement from the technical domains improving system performance also serve the principle of data availability. Similarly one should also collect

data from all available sources including those about the primary user's social environment and "soft" data, that is, those data which are not necessary in a strictly medical sense. Like the other legal principles outlined in this Section the principle of data availability comes into conflict with the each other principles so that the limitations have to be specified. For this ethical requirements such as proportionality and prevention of mission creep which help to specify the legal principles were previously analysed. Moreover, primary users should not be forced to cooperate with the eHealth system in order for it to capture data. The system should capture data without influencing the behaviour of primary users and failing to manage the data capture if two or more people are present. Concerning data loss it should protect the data, communication channels and user interfaces.

4.4 Purpose limitation

The principle of purpose limitation covers several aspects of legal requirements [34] [30]. One should transform the captured face recognition and other data so that nobody can link them with external databases. They should also be safe from anyone's attempt to link them with the location where the system captures them. Moreover, the system should transform them so that one cannot extract excessive sensitive data about health and lifestyle of the individual from the data. Serving only one purpose the captured face recognition and other data should only be available to the hospital and caregivers in charge. Others, such as central cloud operators, should not be able to use the data for secondary purposes, e.g. to concentrate all behaviour of primary users in a single place. In order to achieve such purpose limitation, one should apply specific technologies and data formats. Medical partners should be able to separate a primary user's data that were collected in earlier captures. The sensing devices, management system and decision making system should be separate from databases that can be accessed by other employees or other institutions. The eHealth system should label the primary user's data with the intended purpose.

4.5 Data security

The principle of data security defines the legal requirement of IT security measures that touch on the privacy and data protection. We can group them using a set of IT-security aspects: authentication and access control, cryptography, platform security, secure communications, Public Key Infrastructure, security management and system integration.

In addition to the requirements from the technical domain of information and network security, the law provides a set of requirements [34] [30]. Although they overlap with the requirements from engineering, one has to treat them separately. This is because the manufacturer's design decisions on the basis of engineering considerations can be different from those based on legal obligations. For example engineers might take business secrets as a reason to implement security while data protection law starts from the fundamental rights of the older adults.

According to the legal principle of data security the system must limit user access and types of access on a need-to-know basis. It has to offer user rights for the intended purposes that are workplace dependent both for medical partners as well as auditors. In order to ensure that it is only the medical partners who can obtain knowledge of behaviour and alarms, the system must limit user interfaces accordingly. It should enhance supervised data transfer, especially, to so-called third countries. By splitting up databases among medical partners manufacturers should increase the effort of unauthorised access. They should avoid the possibility of overlapping user rights in central cloud systems and tailor them to the responsibility and task of the medical partner's individual workplace. The system should use state-of-the-art encryption for data storage and transmission as well as a secure data format.

4.6 Data subject rights

The principle of data subject rights covers several aspects of legal requirements [34] [30]. Medical partners have to ensure transparency, that is, revealing who possesses when whose data. Therefore, they should be forced to request the data from a trusted third party. In order to know of the existence of rights, manufacturers should design the system in a way that medical partners have the information ready for the primary users. At all stages of data processing medical partners have to log the following information: employees, their user rights, date/time of process as well as information about access control and data transmission. Concerning data breaches, they have to log the category of data subjects and data categories as well as to count the number of data subjects and number of datasets.

In addition to transparency, medical partners have to ensure participation of data subjects. Manufacturers should support medical partners in accessing, deleting and correcting data in the eHealth system. Of course there is a limit to the participation by data subjects which should be built into the system. In order to handle complaints, the system design should assist medical partners in setting up a complaint management system. Since medical partners have to notify data breaches, watermarks or similar technologies and logging should help medical partners keep the information on unlawful disclosure of behavioural data.

4.7 Anonymity

The principle of anonymity covers several aspects of legal requirements [30]. The system should lower the pixel resolution of face images and other data so that one cannot distinguish one from another. In addition, it should split them up so that medical partners and a third party can only jointly identify a person. Medical partners should take cryptographic or other measures against deanonymisation and assess to what point in time they are effective. In order to anonymise data, the system should collect additional context information and multiple resolutions or other representations of the same datasets. It should avoid content data both during storage and notification of caregivers by using index data where possible and reduce data categories needed for applications.

To the retention periods as short as possible, manufacturers should add policies for the retention of behavioural data. As planned in Annex I, this section particularly explores the period of monitoring of people with mild dementia. Data must be deleted while guaranteeing logging as required by the law. Since some the system captures some data only for intermediary technical reasons, it should delete these by-catch data immediately. Manufacturers should enable medical partners to make the anonymity of primary users conditional upon the extent to which the application in question promotes the health of older adults. Moreover the system should minimise log data. Properties of the eHealth system that can be configured by medical partners should be set privacy-friendly by default.

4.8 Responsibility

The principle of responsibility covers several aspects of legal requirements [34] [32] [30]. To ensure “system protection”, manufacturers should enforce that medical partners can only jointly exercise system administration and use of the system with a trusted third party so that by default no party can identify primary users if not needed. In particular, this protection applies to the programs for pseudoidentifiers and anonymisation. By covering the proper allocation of user rights, encryption, and logging the system should detect irregular activities. It should ensure checking of

software updates. The particular medical partner in charge must have the sole control over the data. Manufacturers should assist them in fulfilling the duty to act responsibly - revealing his or her identity as so-called controller - concerning data transfers. As planned in Annex I, this section particularly explores the choice of relevant entities that will be alarmed in case of an emergency situation with an older person.

The system should log administrative activities. In order to handle privacy compliance, the system design should assist medical partners in setting up a privacy management system. Manufacturers should support the right to be forgotten and ensure effective data deletion beyond the interfaces in the cloud environment, display devices of caregivers and other recipients, etc. In order to prevent unlawful disclosure to the cloud, manufacturers should choose, where possible, a system architecture based on index data instead of access to full data. The system should carry out decentralised decision making.

4.9 Accountability

The principle of accountability covers several aspects of legal requirements [31]. Medical partners have to introduce mechanisms for verification of compliance with the law. Since they also enable medical partners to check the decision making, these mechanisms should reveal hardware, software, development tools and system configuration. Information to be taken into account derives from the manufacturer's public website and other product material. In order to cooperate with data protection authorities and other assessors, sufficiently independent from the medical partner in question, the system should facilitate review inspections and audits.

In addition to policies and audits, manufacturers should ensure that the system remains adjustable. Since they are the basis of possible adjustments required by data protection authorities, manufacturers should guide medical partners in carrying out privacy impact assessments. Concerning their organisation, this guidance should help medical partners oblige their employees to respect data secrecy and provide in-house training.

5 Information and network security

Information and network security is a technical domain which is not dominated by normative disciplines like ethics or privacy. Therefore, we look at security as properties of the technical system instead of starting from measures for the protection of human beings. This Section describes the security measures grouped by technical aspects such as cryptography and access control.

An end-to-end security will be guaranteed in eWALL, based on confidentiality, data integrity, strong authentication and authorisation mechanisms that will be applied both in the Cloud service, as well as the home environment, including gateway and devices. Deliverable 2.1 lists for the eWALL system several requirements: traceability, reliability, security, authorisation, confidentiality, integrity, non-repudiation and auditing. Therefore in the following sections we will analyse these requirements.

One has to distinguish the responsibility to develop these mechanisms which are ensured by the technical and legal partners, on one hand, and to set the specific users and privileges and to enrol the primary user biometrics, on the other. It is the responsibility of the medical partners (that is, the medical partners) to decide on the user registration and primary user enrolment. This is because these tasks depend on the medical partners' internal organisation and their existing ICT procedures for system administrators to register and enrol personnel and primary users which cannot be dictated by other partners. However, in addition to the development of the mechanisms, it is the technical and legal partners' responsibility to give guidance on how to use the authentication and authorisation mechanisms thus improving existing organisational procedures. The technical and legal partners will achieve this in cooperation with the medical partners in preparation of the validation milestones.

The most vulnerable parts in the information security chain are human beings in their capacities as users, operators, designers and similar [11]. Therefore, this Section pays special attention to the security design process and security management. In particular for the application layer one needs to ensure a secure design process.

5.1 Access control

Access control comprises identification and authentication of users as well as authorisation of users to access data and to perform certain kinds of actions on them. In order to ensure security we respect the principle of least privilege and need-to-know principle. Authorisation and authentication will be reinforced using mechanisms such as the biometric feature extraction for secure identification of the primary user (PSKA), restricted access to approved personnel and per-privilege encryption mechanism (CP-ABE).

When considering healthcare systems and applications it is essential to ensure security and privacy of the data during the storage process as well. The access to primary user information, data and statistics must be restricted only to approved personnel in order to provide the required primary user privacy and confidentiality. Since the primary user data and statistics are crucial for medical diagnosis, high level of data integrity should be utilised in order to prevent wrong and miss leading treatments due to deliberate and malicious alterations.

A proficient approach for the data storage process is to use the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) mechanism [5]. CP-ABE provides access policies for the data it manages. It embeds the access policy of legitimate users within the keys so that only the users corresponding to the policy are able to decrypt the cipher text. CP-ABE is public key scheme with enhanced key management. The encryption is done per privilege, not per user. With this mechanism, a certain

user will only be able to access certain data only if the user possesses a certain set of credentials or attributes.

Effective sharing of the key information would ensure authenticity of the user to access the system. The access control could also be designed based on rights. A certain user would only have access to the information to which he or she has a right to access [7]. The overall data could be split into categories based on criticality and sensitivity of information, and accordingly the access rights could be categorised amongst the users.

There should be measures to prevent a collusion attack, that is, combining information bits from a group of users to access the information, since in this way some users would gain information to which they have no legitimate access [4]. The overall system should also be capable of dealing with a denial of service (DoS) attack where it is intended to bring down a system or network. This renders the system or network incapable of meeting service requests from authorised users.

When considering the security access of stored data, the acquisition of the data is regularly administrated by complex policies that have the capability to link each part of the stored medical data with the access user's privileges. Therefore, providing easy and efficient access control mechanism that supports complex administrative policies is a challenge that still needs to be tackled. Trust negotiation [27] [2] [15] is an example of such a mechanism. Trust negotiations allow two, initially mutually untrusting, parties wishing to exchange information, to establish a mutual trust relationship. The trust is established through an exchange of digital credentials. The digital credentials represent digital statements of relevant properties of the parties, and may be recommended by trusted entities (i.e., Certification Authorities (CAs)) or other entities which are trusted by the negotiating parties. The required credentials for the negotiation are defined on the fly according to a given negotiation's goals. During the negotiation, each entity chooses the credentials that it is prepared to disclose to the counterpart and under what conditions. Such conditions are expressed by rules called disclosure policies.

The eWALL project will focus on the practical issues, such as the security management and the overhead and scalability of the access control by introducing novel solutions based on concepts like CP-ABE, Single Point of Contact (SPoC) [8], Organisation-based Access Control (OrBAC) [23], Privacy-aware Role Based Access Control (P-RBAC) [22], Trust negotiation based access control [2] [15], etc.

Having considered the state of the art, we need to assess to what extent eWALL access control fulfils the security-related system requirements. They include the following requirements: traceability, non-repudiation, auditing, reliability, identification, authentication, authorisation, confidentiality, and integrity (D2.1 v1.0 pp. 49ff.).

Concerning traceability, non-repudiation and auditing aspects, the access control should store all necessary information regarding the network access (i.e., authentication and authorisation) process of all users/devices, for example, the ID of a user/device and the time of access. This mechanism should be secure enough to bear the challenge of this information as being manipulated. With an access control system traceability is improved because activities of various users can be tracked. While access control does not seem to promote non-repudiation, it facilitates auditing because it helps in determining all users seeking to gain access and information from the system.

With regard to reliability the access control process should provide on the fly identification, authentication and authorisation of the users/devices. Additionally, the access control process should be capable to reliably identify, authenticate and authorise the valid users/devices and detect the malicious ones. Implementation of access control in the overall system promotes reliability because it only admits genuine users.

As to identification, authentication and authorisation the access control process should incorporate mechanisms for reliable user/device identification and proving its authenticity to the given users/ devices. Commonly, these mechanisms rely on digital signatures and digital certificates. Access control improves identification, authentication and authorisation because it identifies the person seeking to enter the system and gain information.

In relation to confidentiality the access control process should provide possibilities for secure exchange and storage of the user/devices credentials and digital certificates, which are required for the network access process. Access control promotes confidentiality by preventing entry of un-authorised users and access to information of the system. This keeps information confidential to the larger public.

Concerning integrity the digital signatures and digital certificates (used for the identification, authentication and authorisation process) are envisioned and designed to be resilient to data integrity attacks. Access control facilitates integrity because it only admits authorised users and thereby assists in preventing any malicious activity to be conducted and the system to be compromised.

5.2 Cryptography

The eWALL platform will support a wide range of cryptographic services including digital signatures, message digests, ciphers (symmetric, asymmetric, stream & block), message authentication codes, key generators and key factories, the standard algorithms.[2]

Utilizing digital signatures with public key infrastructure would ensure the reliability of the sender and receiver based on the integrity checks that are possible on digital signatures using hash functions. It would also prevent possible non-repudiation of any communication. Effective encryption of the data transmitted across the network should be sufficient to the extent that easy generation of plaintext from cipher text (encrypted data) is not feasible [4].

In order to combat the above-mentioned security attacks (see Section 3) the sensor networks must introduce some aspects and features of key establishment and management. Due to the low computational capabilities of the nodes, the requirements for low energy consumption contemporary key distribution management algorithms cannot be utilised. One efficient aspect already introduced in the area of RFID and WSNs is the Physical Unclonable Functions (PUF) [28]. A secure scheme based on PUFs for establishing and managing keys is feasible solution, which can reduce the energy consumption and processing complexity without having a negative impact on the security aspects of healthcare based WSN systems.

Elliptic Curve Cryptography (ECC) represents another promising cryptographic approach recently introduced in the area of WSNs and health monitoring. In comparison to traditional Public Key Cryptography (PKC) algorithms like RSA, ECC offers equivalent security by utilizing smaller key sizes, faster computation, and lower power consumption. The implementation of ECC in WSN can be either done by software or hardware implementations. The advantages of the software implementations include ease of use, simpler upgrading process, flexibility and lower development cost [13] [10]. However, their main disadvantages are the lower performance and limited ability to protect private keys from disclosure compared to hardware implementations. These disadvantages have led several research works to investigate the possibility of efficient hardware implementations of ECC

[2] For example, RSA, DSA, AES, Triple DES, SHA, PKCS#5, RC2, and RC4 as well as the PKCS#11 cryptographic token.

in WSN [21] [9] [18] [24]. Most of these ECC hardware implementations are developed for the Galois Field GF(2m) and provide computation and encryption of the data only in the binary domain.

In order to mitigate man-in-the-middle attacks when using ECC, first it is necessary to enable secure authentication of public keys. Public key authentication is usually achieved by means of a Public Key Infrastructure, which issues certificates and requires users to store, exchange, and verify them. These operations can cause high communication and processing overheads and in scenarios that require real-time data transmission and fast establishment of the secure data channel or similar, can be inadequate for WSN and health monitoring applications. Identity-Based Encryption (IBE) reduces the need for Public Key Infrastructure. It utilises information that uniquely identifies users, that is, communication nodes (e.g., IP address or node ID) for the key exchange and data encryption processes [17] [19]. For large networks with a high number of active nodes, the complexity of the IBE dramatically increases making the encryption process computationally expensive. Hierarchical IBE (HIBE) allows a root Private Key Generator (PKG) to distribute the encryption workload by delegating private key generation and identity authentication to lower-level network entities [25] [35].

The eWALL system box along with the sensor networks that would provide the monitoring and sensing information related to the primary user, largely, in an in-house environment. The sensor nodes usually have a short communication range of 10 to 15 meters. The communication range of the sensor nodes can be adjusted using power control [26]. This way the communication links within the sensor network, and its communication with the eWALL box would be undetectable outside the house, reducing the communication range. This would minimise their proneness to interception and malicious activity.

Similarly, duty cycling the sensor nodes would also achieve a similar purpose, as a connection that does not exist cannot be intercepted or manipulated. The duty cycling of the sensor nodes could be carried out while meeting the requirement of a given monitoring activity. The aforesaid steps for sensor networks would also additionally help in reducing the overall power consumption of the energy constrained sensor networks.

The aspects of cryptography would also depend to a significant extent on the information access that is provided to the primary or secondary user, especially as some of the primary users have experience with modern technology. This is also closely related to whether the access control to information related to the information concerning a given primary user is within his or her control or is decided through a centralised location for all primary users (see Section **Fejl! Henvisningskilde ikke fundet.**). The likelihood of achieving efficient operation would as such require a centralised access control for all the primary users and not a home-based distributed access control. This also relates to the ethical aspects of consent (Section 3.3) and rights of the older adults (Section 3.4). The cryptography and information security aspects also depend on the manner in which Internet is accessed by the eWALL box (WiFi, ADSL, mobile broadband, etc.).

In particular cryptography can be based in a public key infrastructure. Key management is a very important functionality which defines how secret (and shared) keys, which are the important components to perform any security operation, are managed. The key management has the role to handle the associations of different entities which will be used to perform authentication, and later on, to manage user sessions and to perform encrypted communication. Secure communication means that the communication channel is encrypted with a certain key which is obtained in the authentication process. The authentication process itself can succeed when there is some level of security trust between the entities. Normally, the security mechanism which provides trust relies on a Public Key Infrastructure (PKI) in a form of a digital certificate issued by the trusted third party called Certificate Authorities (CA).

Having considered the state of the art, we need to assess to what extent eWALL cryptography fulfils the security-related system requirements such as traceability, reliability and integrity (D2.1 v1.0 pp. 49ff.). Concerning traceability the cryptographic process should be capable to store all required and necessary information regarding the encryption process and the secure communication between the underlying users/devices. This can be done by conventional key infrastructures like IKE/IPsec. Cryptography facilitates traceability because based on digital signatures of genuine users their activity in respect to using the system can be monitored.

The reliability of the encryption/decryption process mainly depends on the cryptographic algorithm in use, as well as the length of the cryptographic key. More reliable encryption can be facilitated by algorithms that require higher computational complexity and longer cryptographic keys. Cryptography promotes reliability by means of encryption of the data related to the users.

With regard to identification, authentication and authorisation the cryptographic process should incorporate mechanisms for reliable user/device identification. Commonly, these mechanisms rely on digital signatures and digital certificates. Cryptography improves identification because genuine users can be identified based on the use of digital signatures and private keys. Together with access control genuine users gain access to the system. Whereas cryptography promotes authentication because users can be authenticated based on key matching – digital signatures, it also facilitates authorisation as access based on a genuine user's digital signature by public key infrastructure.

In relation to confidentiality the cryptographic process should reliably store the cryptographic key used for the encryption/decryption process. This key is also known as the "shared secret" between the devices and should be accessible only by them. Cryptography promotes confidentiality because encryption of data prevents unauthorised people to gain access of the system and information.

As to integrity in the cryptographic process, the integrity of the encrypted data should be provided by hashing the user data together with information that is only known to the transmitter and receiver (e.g. the cryptographic key, cryptographic nonce). Cryptography facilitates integrity by preventing unlawful entry into the system and encrypting the information flow.

Concerning non-repudiation despite identification of the user by means of user-specific digital signatures one can only prevent the author from denying to be the author of a message as long as they do not claim that their keys have been compromised. Cryptography promotes non-repudiation by identifying users based on digital signature that are unique to them.

Regarding auditing the cryptographic process should be capable of detecting and storing all unsuccessful attacks performed on the communication link between two given entities in the platform. Cryptography improves auditing by determining the overall activities in the system based on the tracking of the key requests.

5.3 Platform security

According to Annex I, the semantic models of the middleware services must prove data security. In addition we will implement the eWALL platform by paying special attention to the quality of the communication between the home and cloud environments, in particular, to provide security in the connection between the services.

We will provide a safe and secure platform for developing and running applications. It will check data type at compile time and manage memory automatically. This leads to more robust code and reduces memory corruption and vulnerabilities. Bytecode verification prevents hostile code from corrupting the runtime environment. Class loaders will ensure that untrusted code cannot interfere with the running of other applications.

Task T2.3 and Work Package WP4 will specify the architectural components and platform aspects of the eWALL project related to privacy and security, in particular, the distinction between centralised or home administration of access control.

5.4 Network security

While access control ensures authenticity and integrity as well as confidentiality during storage network security focuses on integrity and confidentiality of data in transit.

Recent research in eHealth and Body Area Networks (BANs) has shown that environmental information found in the body of the monitored primary user can be utilised to enable secure communication between the active sensors nodes [29]. The body sensors can extract features from some physiological functions like Heart Rate Variance (HRV) or Electrocardiography (ECG) signals as generic sources for the process of generating a cryptographic key. This approach is known as the Physiological Signal Based key Agreement (PSKA). The PSKA approach can be utilised to provide an end-to-end (E2E) security in eHealth systems (i.e., provide a secure communication channel between the sensors and the back-end medical server or cloud). This approach is also denoted as Physiology-based End-to-End Security (PEES). In PEES the sensors utilise the features of physiological functions to encrypt (hide) the keying material through a cryptographic primitive called the vault. At the medical server or cloud, the vault is deciphered with a diagnostically equivalent physiological signal time-series. This physiological signal time-series is synthetically generated using a generative model that has been parameterised with the primary user's physiological information (e.g., ECG, HRV) [3].

One has to pay particular attention to the BAN when the security is based on a PSKA approach. As recent studies [1] proved when two individuals are in close proximity, the electrocardiogram (ECG) of one person gets coupled to the electroencephalogram (EEG) of the other, thus indicating a possibility of proximity-based security attacks. It was proven that the proximity-based attacks can be successful even without the exact reconstruction of the physiological data sensed by the attacked BAN.

Most of the advances in WSN and BAN security either lack performance (like computational efficiency energy efficiency, reliability and security) or applicability and scalability that will enable and provide implementation on real-world healthcare systems. The eWALL project will focus on providing an advanced security framework, for WSN and BAN communication, by incorporating and developing novel and efficient security solutions based on the notions of PUF and PSKA. This framework will be capable to combat and mitigate the common security problems of applicability, scalability, energy efficiency, low runtime, reliability etc.

Several general security services need to be defined in order to avoid possible security threats: authentication, confidentiality, integrity, non-repudiation, data storage security [16]. The in-house monitoring devices that are considered for use in the eWALL project are either wireless sensors (based on WPAN standards like Bluetooth and ZigBee) or wired sensors. Consequently, these will be the considered situations addressed by the security analysis in this Deliverable.

Authentication service provides a method to corroborate the identity of the entities implied in the data creation or communication (device authentication). It can also provide authentication of the data (data authentication). The authentication requirement that has to be fulfilled is to have the possibility of verifying that that data collected from the sensors is genuine and not forged nor tampered with.

In case of wireless sensors connected to the eWALL system box via Bluetooth, the authentication methods built into the Bluetooth communications allow for the fulfilment of this requirement. Starting with version 2.1 of the standard, Secure Simple Pairing (SSP) mechanisms were introduced in order to improve the security of the communication. SSP uses a form of public key cryptography that can help in protecting against man-in-the-middle attacks.

In case of wireless sensors connected to the eWALL system box via ZigBee, the standard supports both, device and data authentication, using 128-bit keys to implement its security mechanisms. The device authentication procedure is performed by a trust centre. The data authentication is obtained by accompanying each frame with a specific code called Message Integrity Code (MIC), that will be verified at the receiver.

For sensors having a wired connection to the eWALL system box, it can be assumed that this requirement is already satisfied.

Confidentiality is a service aiming to protect data in order to make it impossible to be interpreted by a non-authorised user during communication or storage. The confidentiality requirements that are to be addressed in case of the eWALL project are the following:

1. Data transmitted between the BAN/HAN sensors and the eWALL system box must not be read by unauthorised persons.

In case of wireless sensors connected to the eWALL system box through Bluetooth, the encryption methods built into the Bluetooth standard assure the fulfilment of this requirement. Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher.

In case of wireless sensors connected to the eWALL system box through ZigBee, confidentiality is also assured, as the standard provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices.

In case of the wired sensors, considering the purposes of the BAN/HAN it can be assumed that this requirement is already satisfied.

2. Data transmitted externally to or from the eWALL system box must not be read by unauthorised persons.

In order to satisfy this requirement, transport layer security (like SSL/TLS) for the external communications involving the eWALL system box. When using a secure transport protocol, both communication partners agree on an encryption key to be used in the packets they will exchange. During the negotiation of this encryption key, public key cryptography is used, making impossible for an intruder to discover which key is being used for encrypting the packets.

The public key cryptography techniques used with at transport layer usually require that at least the server authenticates itself by means of an X.509 certificate, issued by a Certification Authority (CA) trusted by the client.

3. Traffic characteristics of the transmissions to or from the BAN/HAN (how many data are sent, how often, from where to where, etc.) must be concealed so that non-authorised observers cannot obtain information about the primary user.

Hiding traffic characteristics (traffic confidentiality) can be provided to a certain extent by the transport layer security. Source and destination addresses cannot be concealed at the transport layer without using a secure network layer protocol like IPsec, but length and frequency of packets can be concealed by periodically sending packets with dummy information that will be encrypted and will not be distinguishable from real packets by a non-authorised observer.

Integrity protects data against non-authorised modification, insertion, reordering or destruction during communication or storage. In case of the eWALL project, the following integrity requirements need to be addressed:

1. Data transmitted between the BAN/HAN sensors and the eWALL system box must not be modified by unauthorised persons.
2. Data transmitted externally to or from the eWALL system box must not be modified by unauthorised persons.

The same considerations that were discussed in case of confidentiality apply also in case of integrity, since the security protocols provide both services at the same time.

Non-repudiation service protects against unilateral or mutual data repudiation. The system must be designed in such a way that it is not possible for a data sender to repudiate the transmission of primary user data.

By satisfying the authentication requirements, the main non-repudiation requirements are also satisfied.

Data storage security service is necessary in order to protect stored data against any unauthorised use. Depending on the security level desired for specific applications, it may be necessary to fulfil some of the following requirements:

1. No data collected from the sensors is allowed to be stored locally in the BAN/HAN. This will imply that once the primary user data is collected by the eWALL system box, it is immediately forwarded to a higher level.
2. If the security level is lower, data collected from the sensors is not stored locally in the BAN/HAN, except for temporary storage for later transmission. This situation may appear for applications that need to process larger amounts of data from several sensors from the BAN/HAN at the eWALL system box level, and in this situation it is necessary to use secure temporary storage: once the data is processed, all tracks must be completely and securely removed from the BAN/HAN. This requirement must be addressed by the eWALL system box, since it is not related to communications security.
3. A log of data collected from the sensors has to be stored in the BAN/HAN.
4. A log of data transmitted externally to or from the BAN/HAN must be kept locally.

The last two requirements must also be addressed by the eWALL system box, since it is not related to communications security.

Concerning communication protocols one of the aspects that have to be taken into account is the design of communication protocols to be used for transferring the primary user's data from the BAN/WSN to the back-end medical server or cloud. The protocol has to be designed in such a way that the primary users are able to reveal only selected information about their identity and hide the rest. The information collected through the BAN has to be sanitised according to privacy policies agreed by the primary user before being transmitted to the back-end medical server or cloud. This process of sanitisation has to be done in such a way that enough data is preserved to keep the information useful from a medical perspective, while preventing it to be directly linked to the identity of the primary user [12].

Having considered the state of the art, we need to assess to what extent eWALL network security fulfils the security-related system requirements such as traceability, reliability and integrity (D2.1 v1.0 pp. 49ff.). Concerning traceability the network security process should be capable to store all

required and necessary information regarding the encryption process and the secure communication between the users/devices in the network. This can be performed by conventional key arrangement and exchange protocols like IKE/IPsec. Network security promotes traceability based on the source of the user requesting information from the system.

The reliability of the network security depends on the key exchange protocol, cryptographic algorithm in use, and the length of the cryptographic key. More reliable key exchange protocols and cryptographic algorithms can achieve improved reliability. Network security improves reliability by preventing any eavesdropping on information in transit.

As to identification, authentication and authorisation the network security should incorporate mechanisms for reliable user/device identification and proving its authenticity to the given users/ devices. Commonly, these mechanisms rely on digital signatures and digital certificates. Network security does not seem to promote identification, authentication or authorisation.

With regard to confidentiality the network security process should reliably store the cryptographic key and the digital certificates used for the encryption/decryption process. Network security improves confidentiality by securing the information in transit to be accessible by unauthorised person.

Concerning integrity in the network security process, the integrity of the encrypted data should be provided by hashing the user data together with information that is only known to the transmitter and receiver (e.g. the cryptographic key, cryptographic nonce). Network security facilitates integrity by preventing any eavesdropping and access by unauthorised people.

In relation to non-repudiation the network security process should store information regarding all encrypted data transmissions, in terms of transmitter and receiver ID, time of the transmission, cryptographic algorithm in use, etc. Apparently, network security does not improve non-repudiation.

Regarding auditing the network security process should be capable of detecting and storing all unsuccessful attacks performed in the network. Network security promotes auditing because the network components monitor the entire data flow.

5.5 Secure development life cycle

Secure development life cycle (SDLC) mandates to examine every development progression of a component of the larger system in respect of its compliance with the security and privacy requirements and specifically relates with the overall system that would be running the system. In order to break common vulnerability classes we will cover session management, injection attacks, cross-site scripting, and race conditions. Four broad aspects of SDLC are [14]:

1. Security by design: The software should be designed in a manner such that it is inherently protected and resistive to attacks. This specific aspect therefore relates to the Deliverable 2.8 and highlights the immense significance of Privacy by Design, especially as privacy and security are related entities.

   The overall system will comprise many components. Design and development of the component should be carried out, modelling the security threats it may encounter. The component should be tested and verified to meet the modelled threats.

2. Security by default: As the security of a system will always be open to some possible scrutiny and threats the software development should be such that its operation is inherently

secure. This relates to aspects such as duty cycling of sensor nodes and their power control stated in Section 5.2 as these steps make the sensor nodes secure by default.

3. Security in deployment: The more unobtrusive the overall operation of the software and the system as a whole will be the less likely it is to have a security threat and problems to a reliable operation.
4. Communications: As this is a significant aspect the system security covers the system should communicate possible security threats and possible steps to circumvent it for all the users of the system that are likely to be impacted.
5. Change management: There should be sufficient flexibility in the development of the system so that it is able to address any security threat or vulnerability that may appear in future. This basically requires the system to be sufficiently secure to the expected standards for eHealth systems today, and adaptable to meet any future requirement, especially if a security requirement is mandated by health agencies in the area of operation in reference to the location of primary/secondary user.

5.6 Security management

Security management comprises a number of aspects: human resources security, physical and environmental security, risk assessment methodology, system maintenance, information security incident management as well as business continuity management. In order to ensure these aspects we will follow the principle of separation of duties.

Concerning the human resource security one has to reduce the likelihood of information to be misused by the personnel having the authorised access to the overall system and the information. It also relates to a possible theft of information by a third party from them. A certain previously agreed human resource security policy has to be enacted. All personnel related with the system are required to abide by the policy. The policy has to state explicitly the terms and conditions by which the personnel must abide, especially, in terms of protecting and safeguarding critical information regarding any entity of the overall system. For ensuring the highest order of security and privacy compliance it is also required to designate certain personnel as security managers to ensure smooth operation of the system in respect to appropriate compliance with security and privacy aspects.

Concerning physical and environmental security access to the eWALL box of the primary user should be protected from any possible damage due to an accident or other damage caused by improper use. This is apart from the protection of the device and overall system access protected by passwords/digital signatures and login details. Similarly the cloud infrastructure should be safely housed so as to prevent any possible damage due to a mishap. Additionally, there should be appropriate physical access control on the entry to the premises housing the cloud infrastructure.

Apart from the eWALL box the various sensors and devices to be used for monitoring primary user activities should be designed such that they are not susceptible to any damage due to improper and careless handling and likely damage due to a mishap. As some of the stakeholders in the system might access the information by hand held and mobile devices it necessitates extra security and privacy measures especially to prevent the theft of the device. As well as the network security steps to ensure reliable access of Internet by the mobile device.

Concerning the risk assessment methodology the various threats and the vulnerabilities, to which the overall system and specific components might be prone, should be carefully considered throughout the formation of the system as stated earlier in SDLC (see Section 5.5). Periodic reassessment of the system’s capability to meet changing security threats is necessary. This could be done by a

regular monitoring of advances in the relevant technology and discussions on lacunae on existing technology appearing in public domain.

For other measures of security management Task T2.3 and Work Package WP4 will specify the architectural components and platform aspects of the eWALL project related to privacy and security.

6 Conclusion

Having analysed the ethical, legal and security dimensions of the eWALL system, we specified the generic and specific system requirements of "Security," "Privacy," "Traceability," and related requirements defined in the Deliverable D2.1 (D2.1 v1.0 pp. 49ff.). In addition we proposed security measures for the architectural components of the "Remote Gateway," "Cloud Data Management" and "Security and Privacy Management" foreseen in the Deliverable D2.3 (D2.3 v0.71 pp. 25f.).

Whereas the legal principles of privacy and data protection law provide high-level requirements, the ethical norms such as consent, independent living, dignity, etc. help to specify them for the specific sector of eHealth products and services. Moreover we considered the state of the art in IT security concerning access control, cryptography and network security to be able to evaluate to what extent the eWALL system is secure. The analysis of the security aspects is also a first step in filling the gap between technical and normative requirements for an ethically acceptable design approach. This way the Deliverable prepares the development of a Privacy-by-Design approach at later stages of the project eWALL.

Bibliography

[1] P. Bagade, A. Banerjee, J. Milazzo, and S.K.S. Gupta, "Protect your BSN: No Handshakes, just Namaste!," in *Proc. 2013 IEEE International Conference on Body Sensor Networks (BSN)*, May 2013, pp.1-6.

[2] S. Bahtiyar, M. Çağlayana, "Trust assessment of security for e-health systems," *Elsevier Journal on Electronic Commerce Research and Applications*, November, 2013.

[3] A. Banerjee, S. Gupta & K. K. Venkatasubramanian, "PEES: Physiology-based End-to-End Security for mHealth," *The Wireless Health Academic/Industry Conference* November 2013.

[4] M. Barua, Xiaohui Liang, Rongxing Lu & Xuemin Shen 2011, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference* pp. 970.

[5] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy'07, May 2007.

[6] European Commission *'Communication on eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century'* COM (2012) 736 final.

[7] N. Dong, H. Jonker & J. Pang 2012, "Challenges in eHealth: From Enabling to Enforcing Privacy" in eds. Z. Liu & A. Wassyng, Springer Berlin Heidelberg, pp. 195-206.

[8] L. Fan, W.Buchanan,O. Lo, C, Thuemmler, A. Lawson, O. Uthmani, E. Ekonomou, A. Khedim, "SPoC: Protecting Patient Privacy for e-Health Services in the Cloud," In proc. of eTELEMED 2012, Feb. 2012, pp. 99-104.

[9] H. Houssain, M. Badra & T.F. Al-Somani, "Hardware implementations of Elliptic Curve Cryptography in Wireless Sensor Networks," *International Conference for Internet Technology and Secured Transactions (ICITST 2011)* Dec. 2011.

[10] S. Khajuria and H. Tange, "Implementation of Diffie-Hellman key exchange on wireless sensor using elliptic curve cryptography", in *Proc. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE '09)* pp. 772–776.

[11] EA. Kiountouzis, SA. Kokolakis, "Information systems security: facing the information society of the 21st century" London: Chapman & Hall.

[12] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. De Decker, and H. Vangheluwe, "Privacy-Preserving Telemonitoring for eHealth," in *Proc. of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, DBSec 2009*, Montreal, Quebec, Canada, July 2009. Lecture Notes in Computer Science 5645, Springer 2009, pp. 95-110.

[13] C. Lederer, R. Mader, M. Koschuch, J. Großschädl, A. Szekely, and S. Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks," *Information Security Theory and Practices WISTP 2009* pp. 112-127.

[14] S. Lipner, "The trustworthy computing security development lifecycle", *ACSAC '04 Proc. 20th Annual Computer Security Applications Conference* IEEE Computer Society Washington pp. 2-13.

[15] Y. Ma, J. Liu & W. Liu, "Security and privacy issues in electronic health network," *Wuhan University Journal of Natural Sciences* vol. 18 no. 6 pp.523-529, Dec. 2013.

[16] R. Marti, J. Delgado, & X. Perramon, "Security specification and implementation for mobile e-health services," *2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004. EEE '04*, March 2004, pp.241-248.

[17] L.B. Oliveira, et al., "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Elsevier Journal on Computer Communications* vol. 34 no. 3 pp. 485-493.

[18] G. Panic et al., "Design of a sensor node crypto processor for IEEE 802.15.4 applications," *IEEE International SOC Conference (SOCC 2012)* Sept. 2012.

[19] H. K. Patil & S. A. Szygenda, "Security for Wireless Sensor Networks using Identity-Based Cryptography," *CRC Pres,* Boca Raton, FL, USA, Oct. 2012 p. 232.

[20] M. Pocs, "Will the European Commission be able to standardise legal technology design without a legal method?," *Computer Law & Security Review* 28 (2012) pp. 641-650.

[21] J. Portilla, A.O. Marnotes, E.de la Torre, T. Riesgo, O. Stecklina, St. Peter, and P. Langendörfer, "Adaptable Security in Wireless Sensor Networks by Using Reconfigurable ECC Hardware Coprocessors," in *International Journal of Distributed Sensor Networks* 2010 doi:10.1155/2010/740823.

[22] N. Qun, E. Bertino, J. Lobo, C. Brodie, C-M. Karat, J. Karat, A. Trombeta, "Privacy-aware Role-Based Access Control," *ACM Transaction Information and System Security*, July, 2010, pp.24-3.

[23] G. Russello, C. Dong, and N. Dulay. "A Workflow-Based Access Control Framework for e-Health Applications," *Advanced Information Networking and Applications Workshops*, 2008, pp.111-120.

[24] W. Shi & P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *International Journal of Distributed Sensor Networks* vol. 2013 Article ID 730831, 2012, pp. 7-14.

[25] G. C. Silverberg, "A Hierarchical ID-based cryptography," *Proc 10th Conf on the Theory and Application of Cryptology and Information Security* 2002.

[26] C. Song, M. Liu, J. Cao, Y. Zheng, H. Gong & G. Chen 2009, "Maximizing network lifetime based on transmission range adjustment in wireless sensor networks," *Computer Communications* vol. 32 no. 11 pp. 1316-1325.

[27] AC. Squicciarini, E. Bertino, A. Trombetta and S. Braghin 2012, "A Flexible Approach to Multisession Trust Negotiations," *IEEE Trans. Dependable Sec. Comput.* pp. 16-29.

[28] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Key Generation," *Proceedings of the 44th Design Automation Conference*, June 2007.

[29] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine 2010* vol. 14 no. 1 pp. 60–68.

[30] ARTICLE 29 Working Party on Data Protection (WP29), "Working Document on the processing of personal data relating to health in electronic health records (EHR) (WP 131)," Brussels 2007.

[31] ARTICLE 29 Working Party on Data Protection (WP29), "Opinion 3/2010 on the principle of accountability (WP 173)," Brussels 2010a.

[32] ARTICLE 29 Working Party on Data Protection (WP29), "Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169)," Brussels 2010b.

[33] ARTICLE 29 Working Party on Data Protection (WP29), "Opinion 15/2011 on consent (WP 187)," Brussels 2011.

[34] ARTICLE 29 Working Party on Data Protection (WP29), "Working Document 01/2012 on epSOS (WP 189)," Brussels 2012.

[35] F. Zhang et al., "Ancestor Excludable Hierarchical ID-Based Encryption Revisited," *7th International Conference (NSS 2013)* June 2013.

Abbreviations

ADSL	Asymmetric digital subscriber line
BAN	Body Area Network
CA	Certification Authority
CP-ABE	Ciphertext-Policy Attribute-Base Encryption
DoS	Denial of service
E2E	End to end
EC	European Communities
ECC	Elliptic Curve Cryptography
ECG	Electrocardiography
EEG	Electroencephalogram
eWALL	eWall for Active Long Living
HAN	Home area network
HIBE	Hierarchical IBE
HRV	Heart Rate Variance
IBE	Identity-Based Encryption
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
OrBAC	Organisation-based Access Control
PEES	Physiology-based End-to-End Security
PKC	Public Key Cryptography
PKG	Private Key Generator
PKI	Public Key Infrastructure
P-RBAC	Privacy-aware Role Based Access Control
PSKA	Physiological-signal-based key agreement
PUF	Physical Unclonable Functions
QoL	Quality of Life
RFID	Radio-frequency identification
RSA	Rivest, Shamir und Adleman
SDLC	Secure development life cycle
SPoC	Single Point of Contact

SSL	Secure Sockets Layer
SSP	Secure Simple Pairing
TFEU	Treaty on the Functioning of the European Union
TLS	Transport Layer Security
v	Version
WiFi	WLAN products that are based on the IEEE 802.11 standards
WLAN	Wireless local area network
WPAN	Wireless personal area network
WSN	Wireless Sensor Networks
WP29	ARTICLE 29 Working Party on Data Protection