Project Title:

Virtual Collaborative Social Living Community for Elderly

Co-Living

Contract no. 60-61700-98-009

AAL-2009-2

Deliverable reference:

D1.3

Date:

27.05.2011

Title:

Specification of ethical, privacy and legal considerations

Responsible partner:

Philips

Editors:

John Bernsen (Philips)

Approved by:

Anders Kofod-Petersen (reviewer)

Piet Offermans (technical manager)

Classification:

Confidentiality: Project External

Dissemination Level: PU

Abstract:

Ambient Assisted Living (AAL) and Co-Living in particular introduce new services and technology to elderly to assist them in their daily life. This report analyses the legal, ethical, privacy and security considerations for the Co-Living system. It presents ethical and legal considerations that should be taken into account during the design of the Co-Living system and it presents privacy and security requirements that the Co-Living system should support. This report does not consider the operational project aspects of, e.g., the Co-Living trials, which are governed by the projects ethical committee and ethical boards at the respective trial locations. This work builds further on existing work in the field of AAL and to a lesser extent also (personal) healthcare. Projects like PERSONA and mPower studied in detail the ethical and legal requirements respectively for AAL. Therefore, this analysis adopted this basis and focussed on the Co-Living specific aspects such as for example the Social Community network (SoCo-net) and outward orientation. Most important legal requirements have a basis in EU directive 95/46/EC regarding privacy of personal data and the implementation of the directive in the member states. Privacy and security requirements find their origin in legislation, common practice and developing trends. The analysis starts with a consolidation of security and privacy requirements from various AAL projects, notably mPower. The consolidated requirements cover most basic confidentiality, integrity and availability requirements. It also includes practical requirements regarding authentication and single sign-on. Novel requirements for Co-Living mainly find their origin in recent trends for patient empowerment Making security and privacy means usable to end-users is an essential ingredient of empowerment. Important requirements are practical consent and policy management, transparency and autonomy. Connecting this to the elderly target group of Co-Living and its SoCo-net concept also defines an important role for delegation. The analysis presents 27 security and privacy requirements for the Co-Living system of which 15 are new or refined, which are to be addressed with innovative authorisation and auditing functionalities.

Keywords: legal requirements, ethical requirements, privacy protection, security requirements

Document History

Issue Date	Version	Change Made / Reason for this Issue
May 10, 2011	0.9	First complete version for review
May 26, 2011	1.0	Final version

Table of Contents

List of Figures

This document contains no figures.

List of Tables

1 Introduction

1.1 Summary

Ambient Assisted Living (AAL) in general and Co-Living in particular introduce new technology to elderly to assist them in their daily life. This report analyses the legal, ethical, privacy and security aspects for the Co-Living system. It presents ethical and legal considerations that should be taken into account when designing the Co-Living system and it presents privacy and security requirements that the Co-Living system should support. This report does not consider the operational project aspects of e.g. the Co-Living trials, which are governed by the projects ethical committee and ethical boards at the respective trial locations.

This work builds further on existing work in the field of AAL and to a lesser extent also (personal) healthcare. Projects like PERSONA and mPower studied in detail the ethical [1] and legal [2, 3] requirements respectively for AAL. This analysis references to these results and focuses on Co-Living specific aspects, such as for example the Social Community network (SoCo-net) and outward orientation. Most important legal requirements come from EU directive 95/46/EC regarding privacy of personal data and the implementation of the directive in the member states.

Privacy and security requirements find their origin in legislation, common practice and developing trends. The analysis starts with a consolidation of security and privacy requirements from various AAL projects, notably mPower. The consolidated requirements cover most basic confidentiality, integrity and availability requirements. It also includes practical requirements regarding authentication and single sign-on. Novel requirements for Co-Living mainly find their origin in recent trends for patient empowerment. Making security and privacy means usable to end-users is an essential ingredient of empowerment. Important requirements are practical consent and policy management, transparency and autonomy. Connecting this to the elderly target group of Co-Living and its SoCo-net concept also defines an important role for delegation. The analysis presents 27 security and privacy requirements for the Co-Living system of which 15 are new or refined, which are to be addressed with innovative authorisation and auditing functionalities.

1.2 Role of this deliverable

The role of this deliverable is to analyse the legal, ethical, privacy and security aspects for the Co-Living system and present the ethical and legal considerations that should be taken into account when designing the Co-Living system as well as the privacy and security requirements that the Co-Living system should support. It is worth mentioning that it does not consider the operational project’s aspects of e.g., the Co-Living trials, which are governed by the projects ethical committee and ethical boards at the respective trial locations.

1.3 Structure of this document

The structure of this document is as follows. Chapter 2 presents the legal requirements for the Co-Living system. Chapter 3 discusses the ethical considerations for the Co-Living system. Chapter 4 provides the privacy and security requirements for the Co-Living system.

1.4 Relationships with other deliverables

The results of this deliverable are input to other activities and deliverables in the Co-Living project:

- WP1 ”End Users Needs Analysis and Requirements Specification”
- D1.1 “Specification of user needs and analysis and design of the innovative social practice-oriented community model”
- D1.2 “Specification of use case scenarios”
- D1.3 “Specification of Ethical, Privacy and Legal Considerations” (this deliverable)

  D1.1 and D1.2 are developed in parallel with D1.3 and results eventually feeding into the Co-Living system undergo an early consistency check with the ethical and legal guidelines. The user studies that provide the basis of D1.1 are mainly governed and guided ethically by the Co-Living ethical committee and local end-user ethical boards. Policies of these boards are to a large extent based on the same principles as in this deliverable.

- WP2 “System Design and Architecture Definition”
- D2.1 “Overall System design”
- D2.2 “Design of SoCo-net and of a security and privacy infrastructure”,
- D2.3 “Design of ICT based services”

  For these deliverables hold that their architecture and design should be in accordance with the ethical and legal guidelines of D1.3. In addition, the privacy and security requirements of D1.3 are input to the design of the privacy and security infrastructure of D2.2.

- WP3, WP4 and WP5

  The deliverables developed in these work packages concern the implementation and integration of the designs in WP2. Therefore these are less directly impacted by ethical and legal guidelines though care should be applied. In addition, one deliverable in particular should be mentioned:

- D5.1 “Specification of security and privacy infrastructure”.

  D5.1 depends on D2.2 and thereby is based on the privacy and security requirements from D1.3.

- WP6 “Pilot Trials and Evaluation”

  The Co-Living ethical committee and the local end-user ethical boards govern the trials. As such, this validates if the design and implementation of the Co-Living system to which this deliverable is input meets the ethical and legal norms for a trial with elderly. Furthermore, execution of the trial with elderly and other stakeholders may result in feedback regarding ethical, legal and privacy aspects.

1.5 Contributors

Table 1: Deliverable Contributors

Partner name	**Contributor name**	**Contributor email address**
Philips	Paul Koster	r.p.koster@philips.com
Philips	John Bernsen	john.ac.bernsen@philips.com

2 Legal requirements

This chapter analyses the legal framework for Co-Living. The focus of this chapter is on the legal requirements for the resulting Co-Living system. The Co-Living ethical committee and local ethical boards of end-user partners handle operational aspects of the Co-Living project such as user studies and trials. The scope is primarily the EU and secondary Norway and the Netherlands being the countries of the end-user partners where the trials will run.

2.1 Legal requirements for AAL and Co-Living

Legal requirements for the Co-Living system are expected to be largely identical to those of other Ambient Assisted Living systems as these operate in a similar context and have comparable objectives and functions. Therefore, the analysis for legal requirements starts with a consolidation of results in this field from other projects that work or have worked on AAL. This is followed by an analysis of Co-Living specific aspects, such as its Social Community Network (SoCo-net) and Virtual Care Team (VCT) concepts, to check for missing legal requirements and to identify aspects that deserve particular attention.

From the several projects working on Ambient Assisted Living the mPower project included an extensive analysis of legal requirements [2]. Since Co-Living builds further on the mPower open source middleware platform, operates in the same legal jurisdictions and shares many other aspects, this strong link is leveraged to derive the legal requirements for the Co-Living system. Co-Living also has aspects and focus points that discriminate it from earlier projects, which may affect the legal requirements. The primary functionality added by the Co-Living system is the virtual Social Community Network (SoCo-net) and novel assistive ICT services targeting outward environments. This is supported by a privacy and security infrastructure to empower users. Like any AAL system sensors play an important role. However, compared to earlier projects, Co-Living integrates these sensors with a collection of collaborative services.

Although the Co-Living system will provide new functionality and services it is unlikely that the project develops new devices or hardware. It is much more likely that off-the-shelf devices such as smart phones and components such as access points, modems and PCs will be used. Such devices must, of course, carry the CE Mark[1]. More information related to laws and regulations applicable for ICT devices, e.g. use of spectrum, safety, EMC compatibility and CE approval, can be found in [2].

A crucial point for Co-Living is that even though certain services may comply with the laws and regulations, these services may not comply anymore when extended in Co-Living or integrated with new functions or other services. The background for this can be found in the fact that the use, processing, storage and communication of data is highly regulated in certain contexts such as for personal data and especially for medical data.

Therefore, for the Co-Living system the laws that regulate the use, processing, storage and communication of data must be taken into consideration. These are discussed in Section 2.2.

Furthermore, several European directives as well as national law about services and access to service apply. While most of these directives are fairly broad and apply to service types that Co-Living will not use, they are part of the legal basis for the Co-Living system, which is amongst others influenced by the elderly target group for which service access is an important topic. These directives are discussed in Section 2.3.

[1] CE Marked products are products that have the CE Mark, the product “trade passport” for the European Union.

2.2 Applicable laws on data protection

This section presents a selection from the European directives and national laws that are applicable to the Co-Living system. More details can be found in the mPower project results [2], which provide the basis for this overview.

2.2.1 European directives and decisions

Personal Data Directive

Directive 95/46/EC (also known as the Data Protection directive) concerns the protection of personal data and employs the principle that personal data should not be processed at all, except when certain conditions are met. These conditions fall into the three categories:

- Transparency,
- Legitimate purpose, and
- Proportionality.

Directive on privacy and electronic communications

Directive 2002/58/EC[2] (also known as the E-Privacy directive) concerns the processing of personal data and the protection of privacy in the electronic communications sector. It builds on directive 95/46/EC and in particular targets the right to privacy in the electronic communication sector and free movement of data, communication equipment and services.

Directive on privacy and electronic communications amendment

Directive 2006/24/EC (also known as the Data Retention directive) amends directive 2002/58/EC by defining (extra) rules on data retention and the security of data. The directive mandates retention of certain communication data of publicly available electronic communications services or of public communications networks for law enforcement purposes.

Standard Contractual Clauses for the Transfer of Personal Data to Third Countries

Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC sets out standard contractual clauses to ensure an adequate level of protection of personal data transferred from the EU to third countries. The Decision requires Member States to recognise that companies or bodies that use these standard clauses in contracts relating to the transfer of personal data to third countries ensure an "adequate level of protection" of the data.

Standard Contractual Clauses for the Transfer of Personal Data to Third Countries - amendment

Commission Decision 2004/915/EC of 27 December 2004 amends Decision 2001/497/EC by the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

[2] Directive 2002/58/EC replaces directive 97/66/EC which is therefore not included in this overview.

2.2.2 National laws

This section introduces applicable legislation in the Netherlands and Norway. Next to generic data protection legislation related also legislation applicable to healthcare is touched. Background of this is the target group of Co-Living, which consists of "healthy elderly with light physical or psychological health problems" [4], may expand the scope of Co-Living towards healthcare.

Legislation applicable to the Netherlands

The Dutch "Law Protection of Personal Details", which is the Dutch implementation of the European Directive 95/46/EC, defines rules and procedures how organisations have to deal with personal details. The Dutch institute CBP is the data protection agency that sees to it that rules are obeyed by organisations and companies. The law defines who is allowed to have access to which data and for which purpose in line with the principles set by the directive: transparency, legitimate purpose and proportionality. Also people are offered certain rights over data held about them such as the right to know what is held about him and the right to have errors corrected.

Applied to Co-Living this means that collection and processing of data must meet the conditions defined by law and that the elderly or assisted person in Co-Living, or his/her legal representative, can exercise some level of control over the information.

The target group of Co-Living consists of "healthy elderly with light physical or psychological health problems" [4], which may expand the scope of Co-Living towards healthcare. In such case the "Law Medical Treatment Agreement" may apply, which mandates that patients be properly informed regarding their treatment, mandates dossier keeping and patient related rights. For privacy the "Law Protection of Personal Details" remains applicable. A special case may be in case of emergency, which allows for exceptions to the general privacy rules.

Legislation applicable to Norway [2]

Personal Data Act

The act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

Personal Health Data Filing System Act

The purpose of this act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy, so as to ensure that medical assistance may be provided in an adequate, effective manner.

Patients' Rights Act

The purpose of this act is to promote trust in the relationship between a patient and a health service. This act gives people the right to make (part of) their patient record unavailable to health personnel. People may even demand that (part of) their patient record is erased.

Health Personnel Act

The objective of this Act is to contribute to safety for patients and quality in the health services and to trust between the patient and both health personnel and health services. The different paragraphs in this act focuses on subjects like requirements on how the health personnel works, how the organisation is structured, specific rules connected to authorisation, professional secrecy, information requirement, duty to inform and duty of documentation.

2.3 Applicable laws on services and accessibility

The following European directives apply for electronic communication networks and services [2]. Since Co-Living services may take the form of commercial electronic services, directive 2000/31/EC may apply to the Co-Living system and is thereby part of the legal basis of Co-Living system and deployments. The other directives have a rather generic nature and broad scope and may not necessarily be specifically applicable to Co-Living.

Electronic Commerce laws

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market has as its purpose to improve the legal security of such commerce in order to increase the confidence of Internet users. It sets up a stable legal framework by making information society services subject to the principles of the internal market (free circulation and freedom of establishment) and by introducing a limited number of harmonised measures.

Framework Directive

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 is about a common regulatory framework for electronic communications networks and services.

Authorization Directive

Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 is about the authorisation of electronic communications networks and services.

Access Directive

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 is about access to, and interconnection of, electronic communications networks and associated facilities.

Universal Service Directive

Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 is about universal service and users' rights relating to electronic communications networks and services.

3 Ethical considerations

This chapter discusses the ethical considerations for the Co-Living system. The Co-Living ethical committee and local ethical boards of end-user partners handle operational aspects of the Co-Living project such as user studies and trials. The scope is primarily the EU. The ethical considerations complement applicable law. In the unlikely case of a conflict applicable law such as presented in the previous chapter has priority over ethical considerations.

3.1 Ethical considerations for AAL and Co-Living

Several European projects related to assisted or independent living have defined their ethical basis. Co-Living builds on the ethical basis provided by these projects.

Companiable, PERSONA, and SOPRANO belong to the projects that target AAL systems like Co-Living. Absent from this list is the mPower project, which provides the middleware platform that Co-Living builds on, and which does have a deliverable on socio-economic, regulatory and policy studies, but which does not consider ethics.

On the one hand, Companiable and SOPRANO are research-oriented projects. This is reflected in the ethical sections of their guidelines, which are mainly on ethical guidelines when doing medical research. Consequently, these projects can provide little input for this analysis as it mainly concerns the ethical aspects to be developed in Co-Living system.

On the other hand, the PERSONA project has development of technology as its major goal. Furthermore, the target group of PERSONA is similar to the target group of Co-Living, namely elderly people although PERSONA may also include people that are less healthy. Both projects aim to increase the quality of life and the independence of living of their target group. Combining this with the universal nature of ethical requirements, which PERSONA also realised, leads to the conclusion that Co-Living can build on many parts of PERSONA [1] for creating the ethical considerations of Co-Living.

There are also differences between PERSONA and Co-Living. For example, PERSONA aims to augment people’s live by a focusing in particular on using the output of body sensors (measuring biological functions such as heart rate, or physical functions such as fall detection or location by GPS) and sensors in the surroundings of people (e.g., presence or pressure sensors in an intelligent carpet) to monitor health, safety and well-being of people and react appropriately. Co-Living shares the aim of PERSONA and the use of sensors and services, but takes a novel approach by focusing on the social community network around the elderly. Co-Living furthermore focuses more on outward environments next to in-house and distributed (web-service) architecture with collaborative services.

More than other AAL projects like PERSONA, Co-Living relies on (electronic) communication with and between elderly to inform and stimulate them to be (more) active, start new activities, and ask them about their health, well-being, relations, desires, etc. This constitutes a lot of data of a personal nature. In some cases this data may be classified as medical data. This data is communicated between persons, systems and services and may be collected and stored on several places by different parties. This data is protected under the appropriate personal data protection laws and when applicable medical data laws. Moreover, since the users of the Co-Living system have to rely on the Co-Living system for their quality of living, and rely on making available all this personal data, data that reveals so much about their person (health, desires, (developing) relations, mobility, etc.), it is all the more important that the Co-Living system is not developed simply adhering to the letter of the law, but also adherent to ethical principles behind these laws. This can also advantageously increase the user’s trust in and acceptance of Co-Living services.

In view of the above, Co-Living follows PERSONA and basis its ethical foundation on article 25 of the European Charter of Fundamental Rights. This article recognises the right of the elderly to live independently and with dignity and states: “The Union recognizes and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.” In addition, Co-Living will adhere to several other declarations, conventions, European Union Treaties and Directives on ethical principles. Appendix A.2 provides an overview of these. The following sections discuss in more detail the ethical principles for Co-Living that follow from the identified applicable sources.

3.2 Ethical principles

The presentation of ethical principles follows the structure adopted by PERSONA [1]:

1. Design principle
   “Include in your present choice, as object of your will, the future integrity of the human being” [1] says that for one’s current actions, one carries the responsibility and one must use precaution not to harm the future integrity of the human being.

2. Human dignity
   Dignity is widely considered part of the substance of the fundamental rights and a universal, fundamental, and inescapable term of reference. As such, no rights may be used to harm the dignity of another person. Therefore, it must always be respected, even where a right is restricted.

3. Human integrity
   Every human being has a right to be acknowledged as an inherently valuable member of the human community and as a unique expression of life.

4. Freedom
   All people have the right to exercise their basic freedoms, such as freedom of thought, conscience and religion, freedom of expression and information, freedom of assembly and of association, freedom of the arts and sciences, freedom to choose an occupation and right to engage in work, freedom to conduct a business.

5. Personal Autonomy
   A person has the right to make choices and take action based on person's own values and belief system. However, this right may conflict with other people's freedom and ethical principles, such as human dignity and integrity and has a lower priority.

6. Privacy
   A person has the right to keep an area of his/her life from other people.

7. Protection of personal data
   Everyone has the right to the protection of personal data concerning him or her.

The above principles apply equally well to the Co-Living system. Actually, the Co-living system aims to involve more actors (relatives, friends, neighbours, care professionals, etc.) than the PERSONA system. These actors form the Collaborative Social Living Community and as such have access to at least some of the information and functions of the Co-Living system. Therefore, it is all the more important that the ethical principles are adhered to, especially the autonomy principle, the privacy principle and the protection of personal data. The involvement of the social collaborative care team requires careful balancing with the autonomy principle and careful service and system design.

3.3 Co-Living ethical guidelines

This section presents the ethical guidelines for Co-Living, which concretizes the ethical principles introduced above. Following the structure from PERSONA [1] it is indicated here how the ethical guidelines apply to the Co-Living system and services.

Respect for human dignity

The Co-Living system must respect the dignity of the users and providers of the services. This provision not only constrains the design of the Co-Living services and the business strategy behind them but also limits the freedom of users and providers. The technology chosen must be respectful of human dignity.

Respect for human integrity

According to the right to respect a person's physical and mental integrity, it is prohibited to turn the body, its parts and/or products into sources of profit. The European Group on Ethics in Science & New Technologies talks about an "electronic body", the body augmented with body sensors, whose integrity could be at risk if these data were used to obtain a profit.

The Co-Living system main goal is to create a Virtual Collaborative Social Living Community which encourages and supports active participation, communication, mutual assistance and self-management of the elderly and where the community consists of the elderly, and people around them of different ages and roles (relatives, friends, neighbours, care professionals, etc.).

As such, the Co-Living system will contain a lot of behavioural data of people, which is also part of a person's physical and mental integrity as his/her (electronic) body.

The Co-Living system must respect the integrity of its users such that the data collected about its users is not directly used for making a profit by any individual though allowing for commercial services driven by the use of personal data (after users have given their consent for the usage in this way).

Responsibility

The responsibility guideline is based on the "design principle". It is the responsibility of the developers of the Co-Living system that the Co-Living system respects the ethical and legal guidelines that protect the (elderly) end-user. Taking this one step further, the Co-Living system may assist in users and organisations of the Co-Living system to behave responsively.

It is the responsibility of the organisations that run Co-Living services to provide a clear identification of who will be overall responsible (organisational, e.g. proper handling of user data) for the Co-Living services and ensuring respect to the ethical and legal guidelines protect the end-users.

Privacy and personal data protection

Privacy and personal data protection must be one of the main concerns of the Co-Living system and services. The user should have control over the services that may undermine his/her privacy and be able to determine when they will be active.

Regarding privacy and personal data protection of the users and stakeholders, the following principles must be followed in the Co-Living System and services and functionality to enable this must be developed:

- *Informed Consent*
  Consent from the data subject is a necessary condition for the processing of the subject's data. As it has been discussed in Section 3.2, this consent is not sufficient when the collection and/or processing of the data may threaten the dignity or integrity of the data subject.

- *Data minimisation*
  Only the minimum number of data required for a certain purpose must be collected.

- *Purpose specification*
  The purpose of personal data must be identified before the collection and processing of the data. The data subject must be informed of this purpose. Each datum must have a purpose and this purpose can only achieved by provision of the data.

- *Relevance of the data*
  The data collected must be relevant to the specified purpose.
- *Proportionality*
  The proportionality principle is also grounded on the relationship between tools to be used and purposes sought.
- *Quality of data*
  Every reasonable step must be taken to ensure that data that are inaccurate or incomplete with regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
- *Destruction of data*
  Once the data is no longer relevant or the purpose has been fulfilled, the data must be either destroyed or blocked.
- *Transparency*
  This principle applies mainly when the devices collecting personal data are not clearly visible to the data subject, as can happen in the Ambient Intelligence paradigm. The data subject must be (made) aware about data is being collected or used even when he/she already has given consent.
- *Protection of data*
  Technological measures must ensure that there is an adequate protection of personal data when it is processed, stored and transmitted. This means that e.g. system operators, network operators (service providers) cannot access the personal data ‘in the clear’ and cannot change it without this being noticed by legitimate users of the system. Legitimate users only have access to data needed for the purpose.

Non-discrimination

All users and stakeholders of the Co-Living system and services must be treated equally unless there is a reasonable justification for a differentiated treatment. The Co-Living system must not discriminate between different kinds of users and must take into account issues of accessibility and design for all. Discrimination based on technology chosen by the user must be justified.

Avoiding harm

All services and exploitation of know-how must comply with the provision that according to the state of knowledge at the moment of offering services these are not known to cause any harm nor is there any reasonable suspicion that they may cause harm to human beings. The selected technology cannot damage or threaten the dignity and integrity of users.

Precautionary principle

The precautionary ethical guideline is based on the “design principle”. This principle consists of two parts. The first part of the precautionary principle applies to technology and services still not in the market. A new service can only be tested and/or put to the market when there is a reasonable likelihood that the benefits of the service outweigh its risks. For example, the benefits of a given service such as a tracking device must be greater than the possible risk that this service could damage the privacy of users.

On the other hand, this principle applies also to technologies and services that are already in use. There must be a continuous risk assessment of the impact of the service on human beings to detect any actual and potential threat to the safety and fundamental rights of the users and other stakeholders like providers of services.

Because the devices required in the Co-Living system are regular consumer electronics type devices, the safety aspects of the Co-Living system will be not much different from those of consumer electronics devices. However, due to the nature of the information handled by the Co-Living system, adequate attention to the protection of the fundamental rights of users and stakeholders is much more important for the Co-Living system than for regular consumer electronic devices and systems.

Election of users

Involvement of the users must take into account that, from an ethical perspective, not all services are suitable for all users. This requires careful consideration in Co-Living as there is a great variation in mental and physical limitations that elderly may have, which may require a dedicated approach.

Non-instrumentalisation of users and stakeholders

The non-instrumentalisation ethical guideline states that activities where users and stakeholders are involved must be done for their benefit. Furthermore, users and stakeholders must have a clear understanding of the activities they are involved in. Users and stakeholders will not be used as mere tools to achieve a goal.

Respect of the freedom and autonomy of users

This guideline demands finding an appropriate equilibrium between the right of the user to lead an independent life, the constraints to that right caused by the necessity of requiring aid to have an independent life and the respect for other fundamental rights of the person.

Respect for democracy

These ethical guidelines should not only aim to protect the individual but also the society as a whole. Co-Living services, due to the large amount of private data they are in the position to collect, may create a tension with a democratic society if the data so collected can be used for control of individuals. A strong justification is required for those services that may threaten the freedoms of a democratic society.

To operationalise above ethical guidelines during development of the Co-Living system and services one may consult the checklist by PERSONA [1]. For aspects close to the medical field the International Medical Informatics Association (IMIA) Code of Ethics for Health Information Professionals [5] may be considered.

4 Privacy and security requirements

This section specifies the privacy and security requirements for the Co-Living system and services. The privacy and security requirements are consistent with and partially based on the legal and ethical guidelines for Co-Living that have been defined in the previous two sections.

The previous two chapters have argued that Co-Living is much like other AAL projects, in particular the mPower and PERSONA projects. Likely, also the privacy and security requirements will also be similar to those from other AAL projects. This similarity has also been noticed by Jensen et.al., who have derived the “Reusable Security Requirements for Healthcare Applications” [3] from results of the mPower project.

The security and privacy requirements for the Co-Living system take the reusable security requirements [3] as a basis, which are described in Section 4.1. Section 4.2 analyses the Co-Living System to determine additional requirements that are necessary. Section 4.3 specifies the consolidated list of security and privacy requirements for the Co-Living system and services.

This section uses both the terms security and privacy. In general security shall include privacy and whenever security is mentioned here without the explicit mentioning of privacy, this does not mean that it excludes the protection of privacy.

4.1 Reusable security requirements

Jensen et.al., identify that “Systems development neglects privacy – too often, privacy threats could be avoided if” [3]. Their solution is to provide a set of legislation-based reusable security requirements for (developing) health care applications. This set of requirements is derived from results from the mPower project. The authors argue that since the (mPower) AAL platform will handle personal health data to some extent, it “automatically falls under the strict legislative privacy regulations of healthcare applications”. The authors have taken the set of Norwegian laws that implement the European Directives applicable to the healthcare domain and include traceability references to specific sections in this set of Norwegian laws for each reusable security requirement. This set also includes general laws and regulations on privacy, data protection and information security. All reusable security requirements formulated in [3], except one, can be traced to paragraphs in both general (information) laws and healthcare specific laws. The exception is a non-repudiation requirement on patient journals, which requirement can only be traced to healthcare specific laws. Consequently, these requirements are a good basis for AAL and Co-living in the EU.

Table 2: Reusable security requirements [3]

Requirement type	Description
Identification and authentication requirements	Services should identify and verify the identity of all of its human users before allowing them access to their resources.
	Services should identify and verify the identity of corresponding services before they are allowed to communicate.
Authorization requirements	Services should verify the authorization level of users before access to sensitive data can be given.
Integrity requirements	The platform should support integrity protection of sensitive personal data while it is stored.

Requirement type	Description
	The platform should be able to detect unauthorized manipulation of data that is being transmitted.
Privacy requirements	The platform must protect any stored sensitive personal data from unauthorized access.
	Personal sensitive data must be confidentiality protected while transmitted over open, untrusted communication lines.
Security Auditing Requirements	The platform should be able to log security incidents, such as failed login attempts or unauthorized access attempts to services in order to discover and trace system abuse.
	The platform should be able to log activities related to access of sensitive information.
Survivability requirements	Input validation should be performed at time of data reception to reduce threats represented by malicious content and malformed packets.
	Multiple levels of security should be ensured to avoid a single point of failure.
	Data freshness should be controlled to prevent chances of replay attacks.
Non-repudiation requirements	A patient journal should show who has added content, e.g. through electronic signatures.[1]
[1] This requirement is the only requirement exclusively traced back to healthcare laws. All other requirements have been traced back to both general (information) laws and healthcare related laws.	

4.2 Privacy and security analysis

This section analyses and derives requirements for Co-Living in addition to the reusable security requirements of the previous section. The novel approach to AAL taken by Co-Living is characterised by the fact that Co-Living offers a social collaborative network around the elderly, focuses on the outward environments next to in-house, and uses a distributed (web-service) architecture. The Co-Living system relies much more on (electronic) communication with the users to inform and stimulate them to be (more) active, or start new activities and ask them about their health, well-being, relations, desires, etc. Although Co-Living relies less on sensory data than PERSONA, Co-Living does rely on and supports wireless mobility sensors, such as GPS or accelerometers.

In order to analyse further the specific privacy and security requirements of Co-Living, we first present brief descriptions of stakeholders (4.2.1) and assets (4.2.2) of the Co-Living system and services. Section 4.2.3 analyses the requirements for the Co-Living system and services with a particular focus to identify new requirements.

4.2.1 Stakeholders

This section lists the Co-Living stakeholders. Some of the stakeholders require protection, while other stakeholders must be prevented from doing something:

- *Co-Living platform provider*

  This organisation provides the central components of the service-oriented platform. This could for instance include components like a central service repository and PKI facilities. Collection of personal data could be in the form of a central user database (e.g. for PKI or other identity management facilities). Such a central provider might be able to detect with which services a user is registered, which could reveal sensitive information about a person.

- *Service providers*

  Service providers use services and components offered by the Co-Living platform provider to offer services to end-users. Different kinds of organisations could become Co-Living service providers. This not only includes public (health) care organisations, but also commercial companies that provide services to support elderly people in an active lifestyle. Consequently, some of these providers may have direct contact with the elderly people, while some provide just remote online services. Depending on the kind of service they offer, they will receive, store and process possibly very sensitive information. This information is also forwarded to other service providers in order to collaborate and create the social community network.

- *End-users*
  The people that use the services provided by the service providers can also be divided in several groups:

  - Assisted Persons

    The most important group is the group of assisted persons, the elderly people that use the AAL system to support an active and independent life.

  - Friends and relatives

    An important part of the usage by Assisted Persons of the Co-Living system and services consists of communicating with friends and relatives. In addition, these people may provide informal care to the assisted persons, or act as a guardian. Consequently, these friends and relatives will also make up part of the end-users.

  - Care Volunteers

    Care Volunteers are the people that provide volunteer support to the Assisted Persons. They may be connected to the community in which the Assisted Persons are living or the Co-Living services.

  - Care Professionals

    Care professionals are the people that are able to give professional support to the Assisted Persons. They may be connected to the community in which the Assisted Persons are living or the Co-Living services.

  - Service Provider Employees

    With Service Provider Employees are meant all people, except Care Professionals that are associated with Co-Living Services (e.g. help desk) or Co-Living platform providers (e.g. system or database administrators). Some of these people may be in the position to access Co-Living information in other ways than offered by the Co-Living services.

All end-users, but especially the assisted persons, will submit many personal data to service providers in order to use Co-Living services. They want the benefits of these services, but no negative effects caused by their sensitive personal information falling into the wrong hands.

4.2.2 Sensitive assets in the Co-Living system

This section lists the sensitive assets that are present in the Co-Living system and that require protection:

- User data

  End-users submit all kinds of personal information while using services. This information can range from simple e-mails and filled-in questionnaires on mobility and health, service membership data to electronic discussions with others in the collaborative network on their health, hope and desires. This data is stored and processed by the service providers and exchanged between service providers. The information can range from simple user profiles containing for example a username and an e-mail address to very sensitive data about the health of the assisted person.

- Sensor data

  Part of the information that is submitted to Co-Living service providers may be gathered by sensors (GPS, accelerometers). This data is not sent to the service provider directly by the sensor, but is usually collected and possibly even processed at some kind of gateway first. The raw sensor data that is transferred from the sensor to such a gateway is a sensitive asset itself, before it becomes “user data”, because of the kind of information that is transmitted.

- Private communications between end-users

  End-users might not only communicate with service providers, but also use the Co-Living system to have communications directly with each other. Since these communications could be of private nature (i.e. discussing personal information), they are a sensitive asset.

- Service membership

  The fact that some person is a member of a certain service may represent sensitive information about that person.

- Social network composition

  The composition of the social collaborative network of an Assisted Person and the identity of people in his/her social collaborative network may also be regarded sensitive information.

- Audit logs

  Audit logs contain information on who accessed or changed what information at which time. From these logs, misuse can be detected, but also cases where a Care Professional or Service Provider Employee has used the emergency override, e.g. by overruling the confidentiality protection of certain data (e.g. position data of a GPS) in an emergency.

The sensitive assets in above list relate both to interests of end-users, e.g. privacy, and providers, e.g. commercial interests like competition, liability and reputation. In addition there are sensitive assets that primarily support the provider interests such as the confidential information or knowledge that drives a particular service.

4.2.3 AAL security and privacy functionality

Examples from other systems may be a source of privacy and security requirements or may serve as a checklist to make sure that no obvious requirements have been missed. To properly scope the analysis, this section touches briefly on functionality offered by AAL projects. For example, the mPower system provides security functions to fulfil basic security requirements such as confidentiality, integrity, and authorisation. Concretely, it offers the following security functions:

- Encrypted storage / transfer;
- Auditing functions (logging functions);
- Audit logs;
- Mechanisms for managing users, roles, access policies (role-based access control);
- Security tokens for granting access to a service;
- Authentication mechanisms (password based and PKI-based, single sign-on).

Appendix A.1 provides a brief overview of security and privacy functionality raised by other AAL projects.

4.2.4 Security requirements analysis

In the Co-Living system, a lot of user and sensor data about or of assisted persons may be shared between stakeholders and may be available in many connected systems and services. To improve the acceptability and trustworthiness of the Co-Living system it requires that its system enable the assisted persons to be in control of his/her data and that this control is supported (enforced) by security functions. For healthcare data protection regulations in Europe sort of mandate this control, e.g. through patient consent.

With the above in mind, we analyse the mPower security functions and whether they have limitations that need to be addressed as Co-Living security requirements.

The analysis is split in several parts. Section 4.2.4.1 describes a set of risks for e-health applications identified by ENISA [6] and analyses the controls the mPower architecture offers and lacks to mitigate these risks. Section 4.2.4.2 describes the authorisation mechanisms that must be present in e-health systems according to Accenture’s Institute for Health and Public Service Value [7] and analyses to what extend these mechanisms are present in the mPower architecture. The input documents used in Sections 4.2.4.1 and 4.2.4.2 both originate from the e-health domain, but are equally applicable to AAL irrespective of certain slight differences. In both sections, extra requirements for Co-Living are formulated whenever a risk is not mitigated sufficiently by the mPower architecture. Section 4.2.4.3 describes some security requirements that have been derived from trends. Similarly, Section 4.2.4.4 derives requirements from common security practices. Finally, Section 4.2.4.5 summarises the findings of these analyses.

4.2.4.1 ENISA risk analysis

ENISA identifies a large number of risks related to e-health systems [8]. These risks have been reproduced in Appendix A.3 together with a selection of the risks that have to be taken into account in this security analysis for Co-Living. The following paragraphs briefly describe each selected ENISA risk, discuss how the mPower platform mitigates it and when this is not sufficient, specify what is required extra for Co-Living. Table 3 summarises the requirements for Co-Living identifying the related risk through a label R##. The numbers refer to the risks as they are presented in Annex II of the ENISA document [8]. That document contains more elaborate descriptions of the risks.

R02 The risk of non-compliance with informed consent legislation

Access to sensitive data without prior consent from the subject of the data may be prohibited by legal regulations. A system that is not protected against such illegal data access could cause privacy breaches that could have legal consequences. An AAL framework could provide mechanisms to capture and enforce the consent of its users to mitigate this risk.

Historically, consent is often addressed non-technically. Also mPower lacks support. For example, it does not have a policy language that is expressive enough to capture consent and does not provide mechanisms to capture and enforce consent explicitly.

The above fuels the requirement that the Co-Living system should have a mechanism to capture user consent policies (in a user friendly manner) and enforce consistent end-to-end application of these policies.

R04 The risk of a confidentiality or integrity breach of processed data

Systems that do not provide adequate protection of data in storage or communication risk that the confidentiality or integrity of this data is breached. Access control is one of the important security mechanisms to mitigate this risk (augmenting basic security means such as encryption).

mPower only supports coarse-grained access control (as well as basic security means like encryption). It provides a mechanism to restrict access to service methods, but no means to restrict access to specific assets. It relies on services to make use of the service method access control mechanism.

What is required for AAL systems like Co-Living is fine-grained access control on multiple levels throughout the system that not only supports controlled access to service interfaces, but also to specific assets such as stored data, sensors and actuators. Fine-grained here also means that data can only be accessed by their owners or by actors that have been given permission to access this data by the data owner.

R13 The risk of unauthorized access to data

The risk that unauthorised individuals gain access to sensitive assets and are able to modify or delete them is related to risk R04 in the sense that such access would be a confidentiality or integrity breach. Therefore, the analysis of how the architectures mitigate risk R04 also applies to risk R13.

R14 The risk that the modification and/or deletion of patient data can be performed by authorized individuals

Authorised individuals may cause a risk by erroneous modification or deletion of data either intentional or unintentional. Considering the target users of Co-Living services, most, if not all of their data will probably *not* be ‘patient data’. Nonetheless, it may be an important optional feature Co-Living services to mitigate the risk R14 for data that is considered important. Therefore, we consider the mitigation of risk R14, but then for more types of data than just ‘patient data’, for the formulation of requirements for optional features.

Risk R14 can be technically mitigated by proper audit logging controls and the capability to label data.

mPower does offer an audit service that allows the logging of auditable events. However, audit entries are without internal structure, which makes evaluation hard and potentially reduces effectiveness. Furthermore, sending audit events is at discretion of individual components with no means to indicate necessity to log audit events, e.g. based on data classification or policy.

What is required for AAL systems like Co-Living is that they should have mechanisms that allow for structured audit log eventing and querying. Optionally, they may have mechanisms to label data e.g. as patient data, and if they do support labelling, support the triggering for auditing in case data with a certain label is accessed or used otherwise, and a mechanism to trigger the logging of specific events through policies, e.g. resulting from captured user consent.

R15 The risk of data surveillance and profiling

With large amounts of sensitive data being collected and processed, stakeholders may be tempted to combine all kinds of information about an individual in order to gain extra knowledge. This could impose a threat to the privacy of the individual. This is an example of using data outside of the purposes for which it was originally intended (risk R16) and as such mitigated in similar ways as risk R16, which is discussed below.

R16 The risk of data being used outside the purpose originally intended

This risk is related to risk R02, in the sense that effective consent management and enforcement prevents data from being used outside the original purpose defined in consent statements. This risk is especially relevant to AAL because of the heterogeneous landscape of service providers that exchange all kinds of sensitive data.

Since data is supposed to be accessed to some level, it cannot be completely guaranteed that someone who has access to information will not use it inappropriately. Audit logs can serve as an extra safeguard against inappropriate use by recording who has accessed a certain asset. Access policies can capture the allowed purposes of access to data. Obligations inside policies can be used to define when audit logs should be written. Data-centric rights management techniques can be applied to enforce policies end-to-end, e.g. by transferring policies along with data.

mPower does not support policies that can capture intended purpose.

Co-Living requirements already covered at R02 include the support of access control policies that are used to capture and enforce the intended purpose and user consent end-to-end. Similarly, R14 already presents a requirement for auditing which may be applied to events related to particular (intended) purposes.

R20 The risk of non-compliance with data protection legislation

If a system does not comply with data protection legislation then security breaches may not only impact confidentiality and integrity of data and privacy of individuals, but may also have legal consequences.

mPower has considered data protection legislation while investigating the security requirements [3]. It addresses data protection through encryption means.

4.2.4.2 Accenture information governance foundation for e-health

Accenture describes a number of components that must be included in e-health system architectures in order to ensure data privacy, data confidentiality, data security, data quality and data integrity [7]. These components have been listed in Appendix A.4 together with the selection of components that have to be taken into account in this security analysis for Co-Living. The following paragraphs briefly describe each selected component and specify what is required extra for Co-Living if not yet required or supported by mPower. Table 3 provides a summary of the requirements identifying related components from this section by their code starting with ‘C’.

C1 Patient consent models and mechanisms

According to Accenture, “patient consent should be the prime access control in e-health systems” [7]. This topic is already covered by the analysis of risk R02 in Section 4.2.4.1, which found that mPower does not provide a consent mechanism and therefore proposes a requirement for Co-Living.

C2 Patient-provider relationship based access controls

In healthcare, a patient usually has one or more healthcare professionals responsible for his care. The responsible professionals should have access to the relevant data, while their colleagues that are not involved in the care for that patient should not. This principle also applies to the AAL domain, because e-health may be part of the offered AAL services and specifically to Co-Living, because relationships between assisted persons and their relatives and friends could serve as a basis for access rules. The relationships may be present captured in the SoCo-net and virtual collaborative network of Co-Living.

mPower does not provide a mechanism to incorporate relationships between users into access control rules.

What is required for Co-Living is a mechanism to incorporate relationships between users into access control rules.

C3 Patient access controls

Accenture states that e-health systems should provide patients access to data about them. Appropriate authentication and authorisation mechanisms should be incorporated to support such an interface. It will be rather important that patients can only view data about themselves, not about other patients. This also holds for the assisted persons in Co-Living. The stakeholders in Co-Living should only have access to their own data and the data they have been given permission to access to by their respective owners.

mPower does not provide access control to specific data, only to service methods. Consequently, it cannot restrict users to have only access to their own data.

Consequently, Co-Living requires that stakeholders can only access data they own or that they have been given permission to access by the data owner. This is the same requirement as R04 in Section 4.2.4.1.

C4 Role-based access control models

Accenture suggests role-based access control models as a suitable mechanism to represent job-functions and roles and grant permissions to such groups of users. They stress that very specific permissions, capable of defining rules on access to data, usage of data and access to functionality, must be supported.

mPower does provide a role-based access control mechanism, but its range of supported permissions is limited. It only supports controlling access to functionality on the level of service methods, but does not support e.g. permissions on specific data objects or types. It also does not support role hierarchies.

The Co-Living system does not operate in a regulated healthcare environment, which has well-defined roles by nature and therefore may not require role-based access control per se. However, in some cases role-based access control may be applicable and there is an optional Co-Living requirement that it may support role-based access control.

C5 Patient and provider record sealing

Accenture states that patients, health care professionals and administrators should be able to seal certain parts of a health record, thereby restricting access to these parts beyond the restrictions that are effective on the entire record. In contrast to e-health systems, AAL systems are not built around a notion of a health record as some sort of structured document. The idea of restricting access to parts of data objects may however still be applicable; especially since e-health systems with their health records could be integrated with AAL systems.

mPower does not support permissions on specific data objects, let alone permissions on parts of these objects.

It is not required for Co-Living to support access permissions to particular parts of user data objects. It may be supported as part of other requirements for fine-grained access control policies.

C6 Event audit and alerting

Logging, monitoring and reporting all security relevant events is vital to an e-health system, according to Accenture. This is a requirement that is also found in data protection legislation [7]. It is not a direct requirement for authorisation mechanisms, but is strongly related to it. Audit logs and even notification add an extra layer of security. Organisations and users can keep track of what happens to their data and who has accessed it and possibly act upon this information in case something inappropriate took place.

mPower does offer an audit service, but no means to trigger its use through policies.

What is required therefore for Co-Living is to include a mechanism to be able to trigger the logging of specific events in the audit service through policies.

C7 Data validation

According to Accenture data validation is the set of rules that verify that data conforms to a set of specifications regarding format, quality, integrity, accuracy and structure.

This is already covered by the reusable security requirements.

C8 Code integrity

According to Accenture, the integrity of the code of an e-health system verified by processes that test the source code to eliminate bugs that may result in data loss or data corruption during data storage or transfer.

The Co-Living system does not have a requirement for code integrity functionality, though its development process includes the necessary steps to guarantee its quality.

4.2.4.3 Developing trends in society and research

Law and regulations and industry norms are an important source for security and privacy requirements, but typically have a trailing character with respect to novel developments. Therefore, this section considers developing trends in society and research to derive security requirements that are not covered in the previous sections. Inclusion of such developments as potential requirements fits the explorative and maturing nature of AAL and Co-Living.

4.2.4.3.1 T1 User empowerment

User empowerment is a societal trend that manifests itself in many areas. In online services it allows users to take things into their own hands. In healthcare it allows patients to take an active role in their own care. This empowerment trend also affects security and privacy. In online services it may be recognised in the option users have to indicate their privacy preferences, e.g. for which purposes their data may be used or with whom it may be shared. In healthcare it may be recognised in e.g. electronic health records that have explicit (online) opt-in or opt-out options and that allow the patient to (online) see who accessed their records. Alternatively, it may be seen in personal health records where the patient in detail can specify the sharing policies.

Although a clear trend can be recognised in such examples for user empowerment for privacy and security it is still in flux from a technical and user-interaction perspective [9]. The position of AAL and Co-Living justifies requirements to enable elderly to be in control over the data they share with other parties and over what happens with this data. It is the expectation that this improves the acceptability and trustworthiness of the Co-Living system for the assisted persons.

The above leads to a requirement that the Co-Living system and services shall allow the assisted persons to specify with whom their data is shared and how it is used in a user-friendly way. This requirement shares similarity with R02, C1, R15 and R16.

Similar to a priori control through authorisation, user empowerment also applies to control after the fact by enabling verifying what happened and keeping the responsible parties accountable. In classic solutions this works through logging and auditing of these logs by parties responsible for the system. The latter approach has some intrinsic limitations relating to overhead cost, incentives and trustworthiness. Therefore, more and more modern systems also allow the end-user to have insight in what happened with his data. The exact form is subject of experimentation as effectiveness and usability is an important property to meet user empowerment. Kofod-Petersen and Cassens propose to minimize the asymmetry in information flow where a user is more or less forced to share his data in order to use a service by offering the user the option to require information from the provider on how it used the data [10].

Extracted from the above is the requirement that the Co-Living system and services shall allow the assisted person to have insight in how his data is used. The assisted person should be able to specify that he requires use to be logged in return for giving permission to use his data.

Continuing the usability perspective, the users of AAL-systems in general and in particular those of Co-Living may have difficulties learning and remembering the use of functions that are seldom used including managing access to their data. For these situations in healthcare and assisted living delegation is an accepted and common concept. This leads to the requirement that the Co-Living system should allow an assisted person to let a delegate or guardian to take care of controlling access and consent and auditing on behalf of the assisted person.

4.2.4.3.2 T2 Service oriented architectures and web services

The Co-Living system is an example of a service-oriented architecture (SOA) with web-services. Characteristic of this approach is that multiple services together compose a larger service where a first service invokes other services. Each of these services may operate on user data or other sensitive resources. The system must support secure and practical authorisation both for direct invocations of services as well as indirect invocations through another service.

The reusable requirements of Section 4.1 include a requirement for both human users and corresponding services to be identified. However, there is only an authorisation requirement for users but not for services.

This leads to the requirement that services should verify the authorisation of other services before access to sensitive data can be given. The authorisation of the other services may be derived from the authorisation of the user of the other service from which the request originated. It may also be a generic authorisation of the other service, e.g., a “read access” for basic, non-sensitive data.

4.2.4.4 Other common security functionality

Finally, security and privacy requirements exist that are common either in the application field or generic for security. This section presents some of these requirements that have not been presented in previous sections.

4.2.4.4.1 O1 Emergency override

In AAL-systems, there is the tension between privacy on the one hand and offering quality assistance promptly on the other hand. It may very well occur that only actors that have not been granted access by the assisted person can give timely assistance of the right quality, because the ones that have been granted access are not available. In such exceptional or emergency cases, it should be possible to grant access control overrides to selected stakeholders.

The requirement for the Co-Living system therefore is that is shall support emergency override for authorisation. Such events shall be stored in an audit log. This requirement is in line with break-the-glass functionality as commonly present in healthcare systems.

4.2.4.4.2 O2 Audit log integrity protection and non-repudiation property

Sensitive information in the Co-Living system can be accessed or manipulated by many actors in addition to the original owner. Although actors may have explicit permission to access or manipulate sensitive information, or may even be granted ‘access control override’ in emergency cases, the user gets assurance from the Co-Living system that his data is used properly, because these accesses are logged in an audit system. However, this assurance is of little or no value if the audit information can be changed easily. Therefore, a requirement for the Co-Living system that auditing information should be integrity protected.

Besides reporting access to sensitive information, it is also important to know which actor had access to the sensitive information. For the same reason as above, it should be difficult to manipulate the identity of the actor that accessed sensitive information. Therefore, a requirement for the Co-Living system is that it should be possible to securely trace back every action on sensitive assets to the person or system component that performed it.

4.2.4.5 Analysis summary

The table below summarises the requirements for Co-Living that were found to be necessary in the preceding sections and that are not supported in mPower nor covered in the reusable security requirements.

Table 3: Extra security requirements for Co-Living

Index number	**Requirements for Co-Living that are not supported in mPower nor covered in the reusable security requirements**
R02 / C1 / R15 / R16 / T1 / T2	a mechanism to capture user consent policies (in a user-friendly manner) a mechanism to capture and enforce intended purpose a mechanism to enforce consistent end-to-end application of policies a mechanism for services to verify the authorization of other services
R04 / R13 / C3	a mechanism that ensures that data can only be accessed by their owners or by actors that have been given permission to access this data by the data owner
R14 / C6 / T1	a mechanism for structured audit log eventing and querying a mechanism to trigger the logging of specific events through policies a mechanism to label data a mechanism to trigger the logging of the modification and deletion of data with a specific label
C2	a mechanism to incorporate relationships between users into access and use policies
C4	a mechanism for role based access control (RBAC)
C5	a mechanism to support access permission to parts of user data
O1	a mechanism to support emergency override for authorization
O2	a mechanism for secure audit logging with integrity protection

4.3 Consolidated Co-Living privacy and security requirements

This section presents the reusable security requirements from Section 4.1 extended with modifications and new requirements (marked *italic*) to cater to specific Co-Living requirements resulting from the analysis in Section 4.2. These privacy and security requirements could be valid for other open service and social network based AAL systems as well.

Table 4: Reusable security requirements [3] extended with specific Co-Living requirements

Requirement type	**Description**
Identification and authentication requirements	Services should identify and verify the identity of all of its human users before allowing them access to their resources.
	Services should identify and verify the identity of corresponding services before they are allowed to communicate.
Authorization requirements	Services should verify the authorization level of users before access to sensitive data can be given.
	Users must have control over with whom their data is shared and how it is used. Supported by T1
	The system should have a mechanism to capture user consent in policies (in a user-friendly manner). Part of user consent may be intended purpose. Supported by R02, C1, R15, R16 and T1
	Services should verify the authorization of other services before giving access to sensitive data. Supported by R15, R16 and T2
	Services should verify the purpose of request before giving access to sensitive data. Supported by R15 and R16
	Services should provide a mechanism that ensures that data can only be accessed by their owners or by actors that have been given permission to access this data by the data owner. Supported by R04, R13, C3 and T1
	The system should provide a mechanism to enforce consistent end-to-end application of consent policies along with the data they govern. Supported by R02, R15, R16 and T1
	Services should provide a mechanism to incorporate relationships between users into access and use policies. Supported by C2

Requirement type	**Description**
	Services may provide a mechanism for role based access control. Supported by C4
	The system should support delegation for access control, consent management and auditing. Supported by T1
	The system shall support emergency override for authorization to selected stakeholders. Such events must be stored in an audit log. Supported by O1
Integrity requirements	The platform should support integrity protection of sensitive data while it is stored.
	The platform should be able to detect unauthorized manipulation of data that is being transmitted.
Privacy requirements	The platform must protect any stored sensitive data from unauthorized access.
	Sensitive data must be confidentiality protected while transmitted over open, untrusted communication lines.
Security Auditing requirements	The platform should be able to log security incidents, such as failed login attempts or unauthorized access attempts to services in order to discover and trace system abuse.
	The platform should be able to log activities related to access *and use* of sensitive information *to provide transparency to end-users.* Supported by T1
	The system should support a mechanism to be able to trigger the logging of specific events through policies. Supported by R15, R16
	The system may have a mechanism to label data. The system may trigger the logging of the modification and deletion of data with a specific label. Supported by R14.

Requirement type	**Description**
	Auditing information must be integrity protected. Supported by O2
Survivability requirements	Input validation should be performed at time of data reception to reduce threats represented by malicious content and malformed packets.
	Multiple levels of security should be ensured to avoid a single point of failure.
	Data freshness should be controlled to prevent chances of replay attacks.
Non-repudiation requirements	A patient journal should show who has added content, e.g. through electronic signatures.
	It should be possible to securely trace back every action on sensitive assets to the person or system component that performed it. Supported by O2
NOTE The specific Co-Living requirements, as well as changes to the reusable security requirements from Section 4.1 are in *italic*.	

References

[1] PERSONA, Ethical and legal issues, policy, guidelines, D4.4.1, 2007.

[2] MPOWER, Socio-economic, regulatory and policy studies, D8.2, 2007.

[3] J. Jensen, I.A. Tondel, M.G. Jaatun, P.H. Meland and H. Andresen, Reusable Security Requirements for Healthcare Applications. ARES '09. March 2009, pp380-385

[4] Co-Living partners, Virtual Collaborative Social Living Community for Elderly (Co-Living), project plan part B, 2010.

[5] International Medical Informatics Association (IMIA), the IMA Code of Ethics for Health Information Professionals. Available from: http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf . Last accessed 2011-05-25.

[6] ENISA, 'Being diabetic in 2011': Identifying emerging and future risks in remote health monitoring and treatment, EFR Pilot, 2009. Available from: http://www.enisa.europa.eu/act/rm/files/deliverables/being-diabetic-2011/at_download/fullReport . Last accessed 2011-05-25.

[7] Accenture, Information Governance: The Foundation for Effective eHealth, 2009. Available from: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_100473_InfoGovPoV_Final.pdf . Last accessed 2011-05-25.

[8] ENISA, 'Being diabetic in 2011': Identifying emerging and future risks in remote health monitoring and treatment, Annex II: The Risk Analysis Report, EFR Pilot, 2009, Available from: http://www.enisa.europa.eu/act/rm/files/deliverables/enisa_being_diabetic_2011_Annex2.pdf . Last accessed 2011-05-25.

[9] M. Wegdam, D.J. Plas, Empowering users to control their privacy in context-aware systems through interactive consent, Freeband, Dn3.21, 2008. Available from: https://doc.novay.nl/dsweb/Get/Document-86792 . Last accessed 2011-05-25.

[10] Anders Kofod-Petersen, Jörg Cassens, Proxies for Privacy in Ambient Systems, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol 1, No 4, 2010

A.1 Security aspects in AAL projects

Table 5 presents an overview of security aspects identified in various AAL projects in recent years. The Purpose of this survey is to get a quick overview to determine if any obvious aspects were missed in the security and privacy requirements analysis.

Table 5: security aspects in AAL projects

Category	Title	Brief description	Project
identification	username/password	User proves identity using something he knows (e.g. password)	OASIS
	token/certificates	Users/devices/services prove their identity using something they have (e.g. hardware RFID token or digital certificate)	SOPRANO
	biometrics	User proves identity using something he is (biometrics)	PERSONA, SOPRANO
	single sign-on (SSO)	User proves identity to various services once per session using federated identity management.	MPOWER
authorization	access control lists (ACL)	Authorization to access a resource is granted/denied using an ACL or access to a resource is granted/denied based on permissions linked to the role of the subject using RBAC	PERSONA
	delegation	User/service is authorized to act on behalf of another user	REMOTE
	context aware policies	The context of the access request is taken into account upon making an authorization decision	(MPOWER)
	secure transfer	Sensitive data that is transmitted over an untrusted network is protected to preserve confidentiality and integrity	MPOWER
	secure storage	Sensitive data that is stored in the system is protected to preserve confidentiality and integrity	MPOWER
configuration	expert	An expert (administrator) configures default security and privacy settings and policies of the system. Also performs key management of the various parties in the system.	OASIS
	user and consent control	The user applies predefined policies/settings to new data/situations. The user can provide, withdraw and change consent for authorization (like delegation) and his data usage control. A user-friendly interface is available to perform this.	OASIS
	policy negotiation	The user-service or service-service can negotiate the policies that need to be applicable in an interaction.	REMOTE
tracking	store logs and event reporting	The system logs all access (requests) to sensitive data and other security/privacy related actions such as authentication attempts. Events that are conflicting or unusual are reported for audit.	MPOWER

A.2 Applicable declarations, conventions, treaties and directives

Persona [1] presents all declarations, conventions, European Union Treaties and Directives on ethical principles that apply to the PERSONA AAL system. Those that apply to Co-Living are reproduced below:

- *Universal Declaration of Human Rights adopted by the General Assembly of the United Nations on 1948; in particular, Articles 1, 2, 3, 12, 22, 25 and 27.*
- *Universal Declaration on the human genome and human rights adopted by the General Conference of UNESCO in 1997; in particular, Articles 5 and 13.*
- *Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects adopted by the General Assembly of the World Medical Association in 1964 as modified in Tokyo in 2004; in particular Articles 10, 11, 15, 16, 17, 20, 21 and 22.*
- *Declaration of Principles of the World Summit on the Information Society of 12 December 2003; in particular Articles 19, 24, 29, 30, 31, 35, 51, 56, 57, 58, 59.*
- *Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe in 1950, as amended by Protocol No. 11 in 1998; in particular Articles 5, 13 and Article 1 of Protocol 12.*
- *Convention on Human Rights and Biomedicine adopted by the Council of Europe in 1997; in particular Articles 1, 5, 6, 7, 8, 9 and 10.*
- *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted by the Council of Europe in 1981; in particular Articles 1, 6, 7, 8, 9, 10, 11.*
- *Charter of Fundamental rights of the European Union, proclaimed by the European Parliament, the Council and the Commission on 2000; in particular Articles 1, 3, 7, 8, 21, 25, 26, 35, 45.*
- *Treaty on European Union; and in particular Article 6.*
- *Treaty establishing the European Community; in particular Articles 152 and 153.*
- *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on e-Health - making healthcare better for European citizens:*
  An action plan for a European e-Health Area COM (2004) 356 final.
- *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*
- *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;*
- *Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
- *Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use.*

A.3Risks identified by ENISA

ENISA identified 21 security risks in the area of personal tele-health [8]. Of these 21 risks, Table 6 lists the ones that can be mitigated in the design phase. Therefore, these risks have been taken into account in the derivation of the security requirements for Co-Living in this document. The other risks can only be mitigated in the deployment or operational phase, by e.g. proper training, proper selection of server capacity, and consequently are not applicable for this document. These risks are listed in Table 7.

Table 6: ENISA risks [8] applicable to Co-Living

R02	The risk that the system is not compliant with informed consent legislation
R04	The risk that the confidentiality or the integrity of the data processed could be breached
R13	The risk that unauthorized individuals might gain access, modify and/or delete the patient's data
R14	The risk that the modification and/or deletion of patient data can be performed by authorized individuals
R15	The risk of data surveillance and profiling
R16	The risk of collected data being used inappropriately or for other purposes different than those they were initially intended for
R20	The risk of non compliance with data protection legislation

Table 7: ENISA risks [8] not applicable to Co-Living

R01	The risk that the patient might not follow the instructions to do with equipment use, treatment and medication
R03	The risk to compromise one's credentials
R05	The risk that the availability of the service could be compromised
R06	The risk that the devices or hub could be overloaded
R07	The risk of damaging the equipment
R08	The risk of natural threats that could damage the system due to its use in unprotected and/or outdoor environments
R09	The risk of malfunction and breakdown of the system
R10	The risk that the patient's garment and/or IT equipment could be stolen
R11	The risk the devices might be used unprofessionally
R12	The risk that the measurement devices could be used by unauthorized people
R17	The risk that the patient might misinterpret the data
R18	The risk that the misinterpretation comes from a mistake made by medical staff
R19	The risk of human error in cases of emergency
R21	The risk of an inadequate provision or unavailability of medical services

A.4Security components identified by Accenture

Accenture identifies a number of components that must be included in e-health system architectures in order to ensure data privacy, data confidentiality, data security, data quality and data integrity [7]. These components are listed in Table 8.

Table 8: Security components for e-health identified by Accenture

Data Privacy	*C1 Patient consent models and mechanisms*
	C2 Patient-provider relationship-based access controls
	C3 Patient access controls
	Effective data security and data handling policies
Data Confidentiality	*C4 Role-based access control models*
	C5 Patient and provider record sealing
	Identification and authentication
	Anonymization and pseudonymization
Data Security	Message integrity and communications security
	C6 Event audit and alerting
	IT security audit
	Network integrity
Data Quality	Error correction
	C7 Data validation
	System and interface certification
	Standards driven architecture
Data Integrity	*C8 Code integrity*
	System hardening
	Interoperability governance
	Standards-driven architecture and standards management

The components in *italics* in Table 8 are the components that have been taken into account in the security analysis Section 4.2.4.2. These components are identified through a code Cx here.

A.5Glossary

Table 9: List of terms, abbreviations and acronyms

AAL	Ambient Assisted Living
EMC	ElectroMagnetic Compatibility
EU	European Union
GPS	Global Positioning System
ICT	Information & Communication Technology
PKI	Public Key Infrastructure
SoCo-net	Social Community Network
VCT	Virtual Care Team