Deliverable D5.4

Report on Standardization

Authors: Ziad NEHME

Workpackage: WP5

Total Number of Pages: **22**

File: Deliverable 5.4 Care4Balance V2

Executive Summary

This deliverable describes the standardization concerning the Care4Balance system. It details the standards used and to be used for the different components of the C4B system.

Document Revision History

Date	Version	Author	Summary of changes
12/02/2015	0.1	Ziad NEHME	Initiation of the document

Contributors

First Name	Last Name	Company	Email
Ziad	NEHME	PERVAYA	ziad.nehme@pervaya.com

Table of Contents

Introduction

This document lists and discusses the standards, recommendations and ethical features. They are based on the fact that the Care4Balance platform does not manage healthcare data but caregiving information and telecare data only.

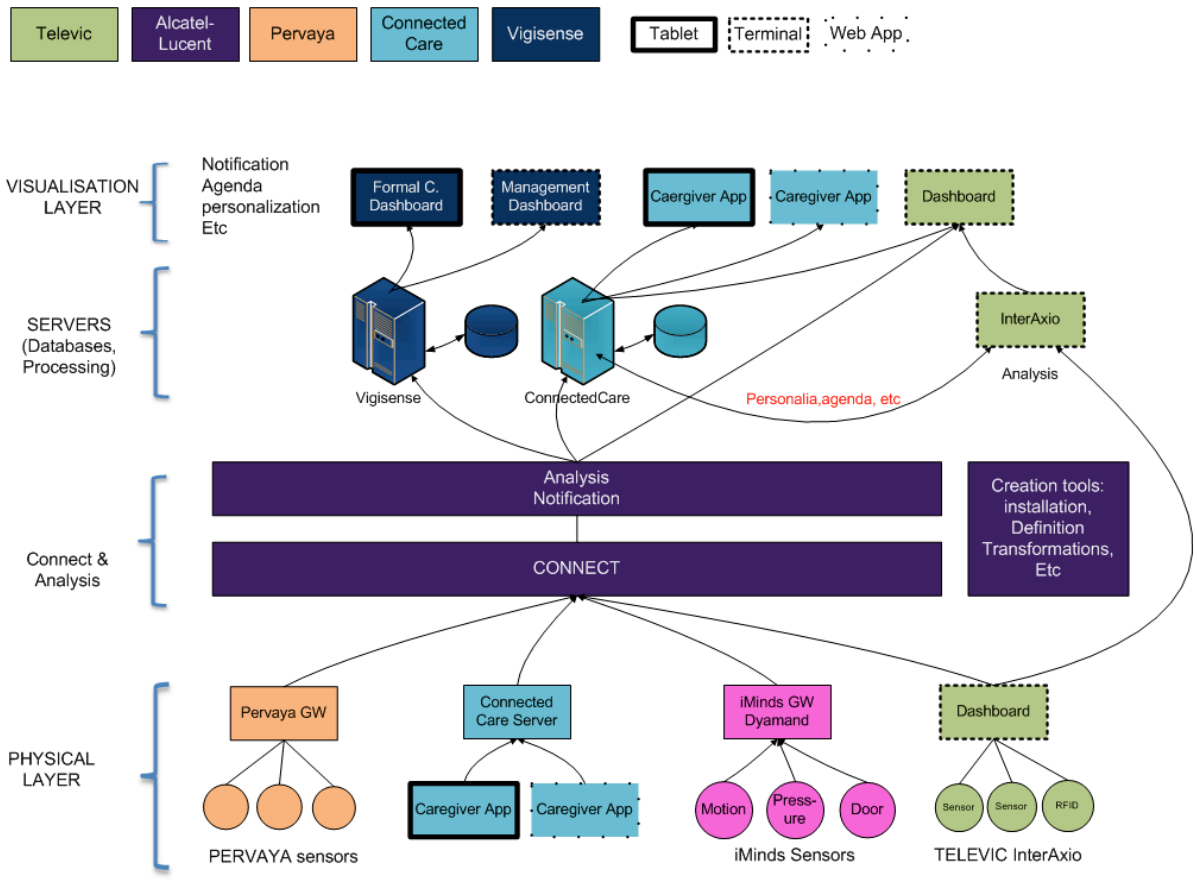
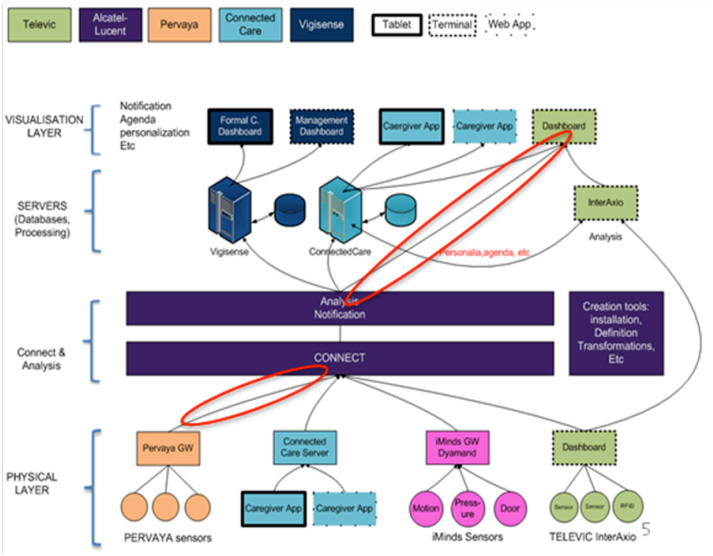
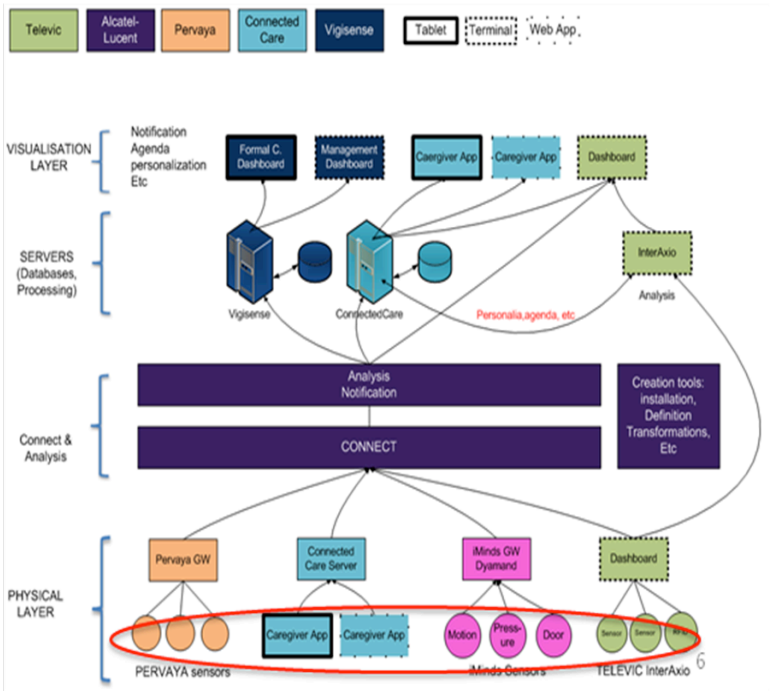


Figure 1: Logical wire diagram



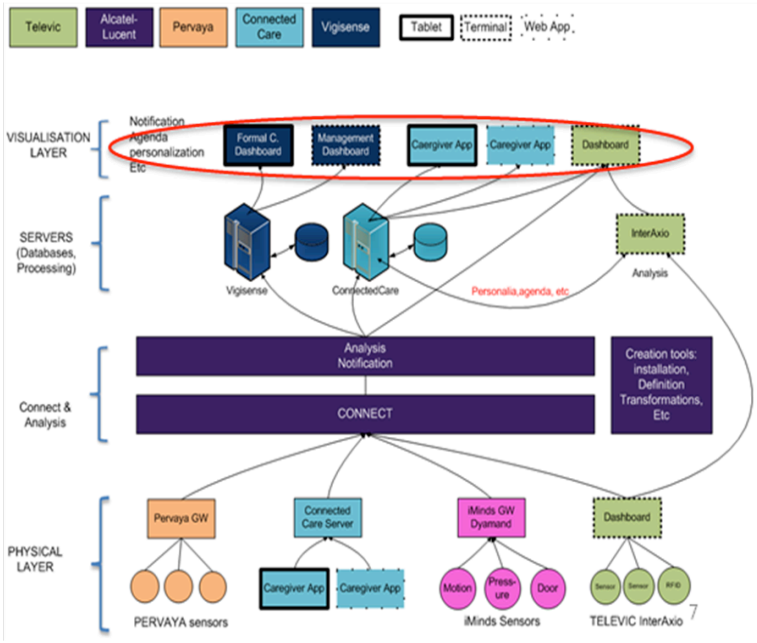
Integration Profiles

- Continua Health Alliance
- DLNA: Digital Living Network Alliance



Sensors & Actuators

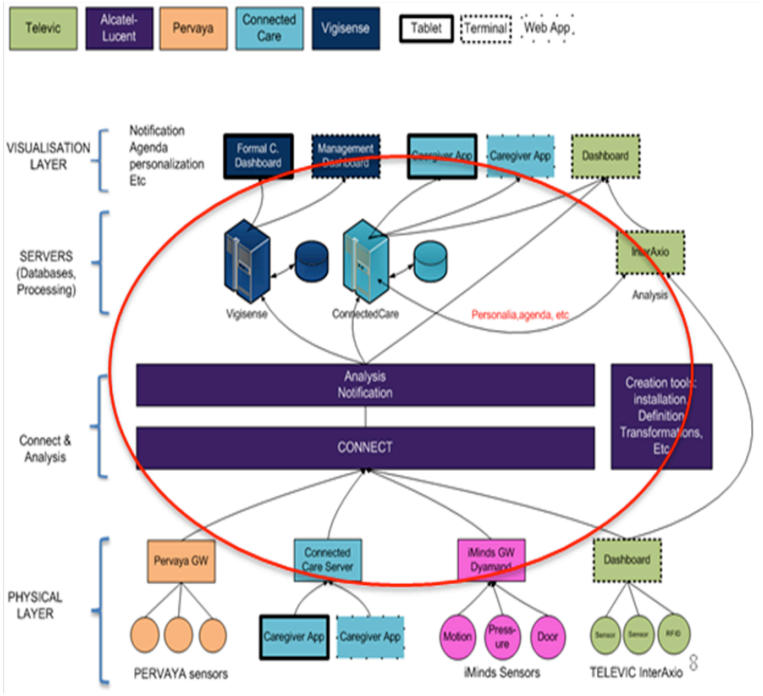
- Sensors & actuators
  - Safety
    - EN 41003: Particular safety requirements for equipment to be connected to telecommunication networks and/or a cable distribution system
    - EN 50364: Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 300 GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications
    - EN 60335: Safety of electrical appliances and machines for household environment and similar purposes
    - EN 60950: Information technology equipment - Safety
    - EN 61000: Electromagnetic compatibility (EMC)
  - Electromagnetic compatibility
    - EN 50130-4: Alarm systems - Part 4: Electromagnetic compatibility - Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
    - EN 55014: Electromagnetic compatibility - Requirements for household appliances, electric tools and similar apparatus
    - EN 55022: Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
    - EN 55024: Information technology equipment - Immunity characteristics - Limits and methods of measurement



User Interfaces: Usability, Ergonomics, Design for All

- EN ISO 14915: Software ergonomics for multimedia user interfaces
- EN ISO 9241: Ergonomics of Human System Interaction
- ETSI EG 202 116: Human Factors -- Guidelines for ICT products and services "Design for all"
- ETSI EG 202 416: Human Factors (HF) -- User Interfaces -- Setup procedure design guidelines for mobile terminals and services
- IEC/TR 62678: Audio, video and multimedia systems and equipment activities and considerations related to accessibility and usability
- ISO 20282: Ease of operation of everyday products
- ISO/IEC 10741-1: Information technology -- User system interfaces -- Dialogue interaction -- Part 1: Cursor control for text editing
- ISO/IEC 25051 (former 12119): Software product Quality Requirements and Evaluation (SQuaRE) -- Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing
- ISO/IEC 24786: Information technology -- User interfaces -- Accessible user interface for accessibility settings
- ISO/IEC 25010 (former 9126): Software engineering - Product quality
- ISO/IEC Guide 71: Guidelines for standards developers to address the needs of older persons and persons with disabilities
- ISO/IEC TR 13818: Information technology -- Generic coding of moving pictures and associated audio information
- ISO/IEC TR 19765: Information technology -- Survey of icons and symbols that provide access to functions and facilities to improve the use of information technology products by the elderly and persons with disabilities
- ISO/IEC TR 19766: Information technology -- Guidelines for the design of icons and symbols accessible to all users, including the elderly and persons with disabilities
- ISO/TR 22411: Ergonomics data and guidelines for the application of ISO/IEC Guide 71 to products and services to address the needs of older persons and persons with disabilities

Specifications and standards for operator models



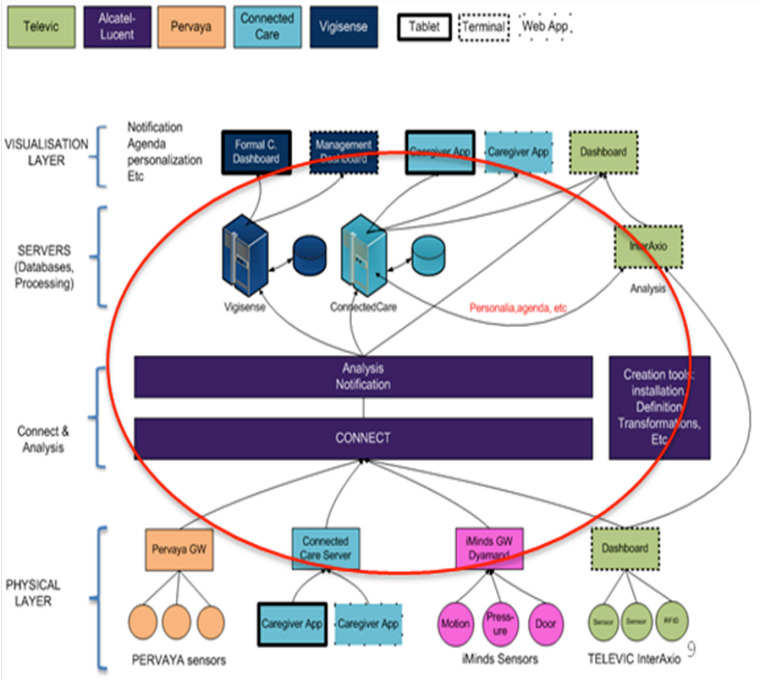
Quality management systems for AAL

- DIN SPEC 77002: Ambient Assisted Living (AAL) - Requirements for AAL services
- DIN SPEC 91280: Ambient Assisted Living (AAL) - Classification of Ambient Assistant Living services in the home environment and immediate vicinity of the home
- DIN SPEC 91300: Guide for the development of a business model for home related services
- VDE-AR-E 2757-2: Service staying at home - Requirements for suppliers of combined services
- VDE-AR-E 2757-3: Staying at home service - Criteria for the selection and installation of AAL components
- VDE-AR-E 2757-4: Staying at home service - Quality criteria for providers, services and products of Ambient Assisted Living (AAL)
- VDE-AR-E 2757-100: Ambient Assisted Living (AAL) – Guideline for the development of AAL products

Other

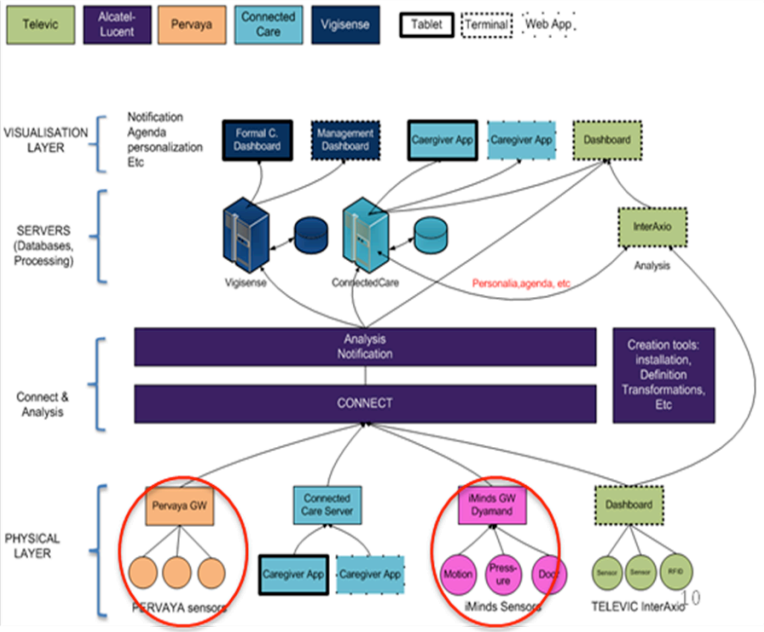
- EN ISO 9999: Assistive products for persons with disability - Classification and terminology

Privacy and Security



Data protection specifications

- Directive 95/46/EC: Protection of individuals with regard to the processing of personal data and on the free movement of such data
- HL7 IG for CDAR2: Consent Directives, Release 1", CDAR2 : HL7 Implementation Guide for CDA®, Release 2: Consent Directives, Release 1
- ISO/IEC 27000: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002: Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC 29100: Information technology -- Security techniques -- Privacy framework
- ISO/IEC CD 29101: Information technology -- Security techniques -- Privacy architecture framework
- ISO/IEC WD 24760: Information Technology -- Security Techniques -- A Framework for Identity Management
- PbD: Privacy by Design
- SbD: Security by Design



Alarm systems

- CLC/TR 50456: Alarm systems - Guidelines to achieving compliance with EC directives for equipment of alarm systems
- CLC/TR 50515: List of interpretations on published standards on "Alarm Systems"
- CLC/TR 50531: Alarm systems - Terms and definitions
- CLC/TS 50398: Alarm systems - Combined and integrated alarm systems
- EN 50130: Alarm systems
- EN 50518: Monitoring and alarm receiving centre
- SCAIP: Digital social alarm - Social care alarm internet protocol (SCAIP) - Specification

1. Privacy and ethical considerations

1.1 General description

Care4Balance is not a healthcare platform, but a caregiver platform / telecare platform.

1.2 Belgium

The Commission for the Protection of Privacy (CPP), better known as the Privacy Commission, is an independent body ensuring the protection of privacy when personal data are processed.

The Privacy Commission was established by the Belgian Federal House of Representatives with the Act of 8 December 1992 (the so-called "Privacy Act").

The Privacy Commission's mission is to ensure that privacy is respected when personal data are processed. It is a federal body, although there has been a Flemish Supervisory Commission for Electronic Administrative Data Flows since December 2009. The Flemish Commission has similar powers, but only at Flemish level.

1.3 Netherlands

The Dutch DPA stands for the fundamental right to the protection of personal data.

The Dutch Data Protection Authority (the Dutch DPA) supervises processing of personal data in order to ensure compliance with the provisions of the law on personal data protection and advises on new regulations.

The fundamental right to personal data protection is essential for the functioning of the rule of law. The Dutch DPA protects this fundamental right by:

- Addressing infringements of the law;
- Advising on new laws and regulations;
- Being aware of societal dilemmas related to privacy;
- Raising awareness with governmental organisations, businesses and civil society on their respective responsibilities regarding data protection;
- Providing information to enable people to exercise their rights;
- Making the results of its supervisory and enforcement actions public;
- Seeking national and international cooperation in order to better protect personal data.

The Dutch DPA acts with complete **independence** in exercising the functions entrusted to it. This means that the Dutch DPA determines its own priorities within the framework set out by the law. It chooses these priorities based, amongst others, on criteria such as the seriousness and magnitude of infringements of the law and the amount of individuals affected. Internally, the Dutch DPA stimulates the use of the independence and knowledge of its employees.

1.4 Switzerland

In Switzerland, the Federal Data Protection and Information Commissioner has in particular the following tasks:

- He supervises federal bodies
- He supervises private bodies
- He advises private bodies
- He assists federal and cantonal authorities in the field of data protection
- He gives his opinion on draft Confederation legislation
- He cooperates with data protection authorities in Switzerland and abroad
- He informs the public about his findings and recommendations
- He maintains and publishes the Register for Data Files

The principle of transparency in the federal administration is enshrined in a federal law. Accordingly, the Federal Data Protection and Information Commissioner (FDPIC) has been assigned a number of functions:

- He informs and advises private citizens on how to gain access to official documents
- He advises the various administrative authorities and federal departments on the implementation of the Transparency Act
- He acts as mediator in the event of a disagreement
- He sends written recommendations to the persons concerned
- He gives an opinion on draft legal texts prepared by the federal authorities that have an impact on the principle of transparency

The principle of transparency establishes an enforceable right of access to the official documents of the federal administration and the parliamentary services. The law applies to all official documents that have been produced since 1 July 2006. Any individual may ask to see the documents in question without having to provide any reason for doing so. Right of access may be limited if the document may compromise an overriding public or private interest. If access is refused, the authority must justify its decision.
Furthermore, the FDPIC verifies the implementation, effectiveness and cost of the Transparency Act, and submits a report to the Federal Council on a regular basis.

1.5 France

The CNIL has been entrusted with the general duty to inform people of the rights that the data protection legislation allows them. It tries to reach out to the general public, either through the press, through its Internet site, appearing on social network sites or by providing teaching tools.

Directly accessed by many organizations, companies or institutions to help them carry out training programs and programs to raise awareness of the data protection legislation, the CNIL is involved also in seminars, fairs and conferences to provide information and at the same time to obtain information. The public information and guidance section deals with requests from private individuals and professionals and records all the preliminary formality cases.

As a means of asserting its expert opinion, the CNIL suggests to the government legislative and regulatory measures that may adapt protection of freedoms and privacy to fit in with technological developments. The government consults the CNIL before passing on to Parliament draft legislation relating to data protection. The CNIL advises personal data controllers on their obligations, and it trains the data protection officers and offers them a special service, via a dedicated extranet.

Everyone can contact the CNIL when they find it difficult to exercise their rights. The CNIL will ensure that citizens can access in an effective way data contained in any data processing operations that may affect them.

The CNIL drafts and publishes, after receiving if applicable the proposals put forward by the representatives of the representative organizations, standards aimed at simplifying the disclosure requirement.

In the case of data processing or the most current and least dangerous personal data files, the CNIL will draft text frames to which personal data controllers must refer in order to complete the simplified reporting formalities or be exempt from them.

"Risky" or sensitive data processing is subject to approval from the CNIL or to CNIL's view. The file managers who do not comply with these formalities are subject to administrative or criminal penalties.

1.6 Example of recommendations (CNIL)

Below is a list of good practices intended to treat risks that the processing of personal data may pose to the civil liberties and privacy of data subjects from the document CNIL-ManagingPrivacyRisksMeasures_v1.0. It supplements the risk management method of the Commission Nationale de l'Informatique et des Libertés (CNIL, the French data protection authority) with regard to risks to civil liberties and privacy and helps to determine the measures proportionate to the risks identified using this method.

1. Minimize the amount of personal data
2. Manage personal data retention periods
3. Inform the data subjects
4. Obtain the consent of data subjects
5. Permit the exercise of the right to object
6. Permit the exercise of the direct access right
7. Allow the exercise of the right to correct
8. Partition personal data
9. Encrypt personal data
10. Anonymize personal data
11. Backup the personal data
12. Protect personal data archives

13. Monitor the integrity of personal data

14. Trace the activity on the IT system

15. Manage personal data violations

16. Avoid sources of risk

17. Mark documents that contain personal data

18. Manage persons within the organization who have legitimate access

19. Monitor logical access controls

20. Manage third parties with legitimate access to personal data

21. Combat malicious codes

22. Control physical access

23. Protect against sources of non-human risks

24. Reducing software vulnerabilities

25. Reducing hardware vulnerabilities

1.7 Security Guide for Personal Date

The European directive on the protection of personal data unambiguously requires all companies to implement adequate security measures if they are established in a member state or otherwise make use of data processing means situated in Europe.

Securing an IT system requires taking into account all aspects of its management. This security resorts to the respect of good practices and the maintenance of the data-processing tool in a state-of-the-art condition with regard to the attacks to which it can be subjected.

However, this security will only be effective if rigor is applied to the delivery (and the withdrawal) of security clearances as well as the processing of some unavoidable incidents.

In order to guarantee that all IT system users only have access to the data they need to know, two elements are necessary:

- Providing a unique identifier to each user, in association with authentication means: an authentication method;

- Applying prior access controls to data for each category of users: an authorization management.

In addition, the protection of data concerning persons requires that such data is:

- "Collected and processed in an fair and lawful manner" (Article 6 al. DPA Act)

- "Collected for determined, explicit and legitimate purposes and is not later on processed in a way that is incompatible with these purposes" (Article 6 al.2 DPA Act).

Observing how the IT system is used can only assess these requirements. Consequently, it is necessary to implement a logging facility, i.e. recording each user's actions on the system during a defined period of time.

Moreover, the Data Processing and Freedoms Act lays out that data must be "accurate, complete and updated when necessary" (Article 6 al.4 DPA Act). These obligations require information systems to include mechanisms that guarantee data integrity.

The law also lays out that this data "is preserved in a form allowing the identification of the persons concerned for a period of time which shall not exceed the duration required by the purposes for which it is collected and processed " (Article 6 al.5 DPA Act). Therefore, the systems must include a mechanism for any suppression, archiving, or anonymisation of this data when its retention period expires.

Finally, risk management represents an effective way to protect "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" (article 1 of Directive 95/46/EC).

Below is an impact analysis. There are multiple phases: the R&D phase (C4B) and the phase with a growing number of users. Within C4B we have gone as far as we are planning to go. **When the number of users starts to grow then it is useful for us to go further and start to implement the "will be implemented"**.

The main requirements are:	
1 - Managing risks	
- Make an inventory of files, personal data and the their processing	Will be implemented
- Identify the threats and their impacts on privacy	Will be implemented
- Implement security measures that are scaled to the threats	Will be implemented
2 - Authenticating users	
- Define a unique identifier (login) for each user	Already implemented
- Adopt a strict policy for user passwords	Will be implemented
- Make the user change his/her password after it has been reset	Will be implemented
3 - Authorisation management and awareness-raising	
- Define authorisation profiles	Will be implemented
- Remove obsolete access authorisations	Will be implemented
- Document operational procedures	Will be implemented
- Write an IT charter and link it to staff regulations	Will be implemented
4 - Backup and business continuity management	
- Perform regular backups	Already implemented
- Store the backup media in a secure location	Already implemented
- Implement security measures to protect the transportation of backups	Will be implemented
- Define a business continuity plan and test it regularly	Will be implemented
5 – Supervising maintenance	
- Record maintenance interventions in a register	not concerned
- Erase data from any equipment before it is discarded	Not concerned

- Obtain the user's agreement prior to any intervention on his/her workstation	Will be implemented
6 - Tracing accesses and managing incidents	
- Implement a system to collect log files	Will be implemented
- Inform the users about the installation of the log files collecting system	Will be implemented
- Protect the log fuiles collecting system and the logs	Will be implemented
- Notify concerned people of any fraudulent accesses to their data	Will be implemented
7 - Securing servers and applications	
- Adopt a strict policy for administrator passwords	Already implemented
- Install critical updates without delay	Already implemented
- Ensure data availability	Already implemented
8 - Managing subcontractors	
- Envisage a specific clause in the subcontractors contracts	Will be implemented
- Ensure the effectiveness of the planned guarantees (safety audits,visits…)	Will be implemented
- Define the conditions for data restitution and destruction	Will be implemented
9 - Archiving	
- Implement specific access methods to the archived data	Will be implemented
- Destroy obsolete files in a secure way	Will be implemented
10 – Securing exchanges with other organisations	
- Encrypt data prior to sending it	Will be implemented
- Ensure it is to the proper recipient	Will be implemented
- Transmit secret through a distinct message and through a different channel	Will be implemented

1.8 Listing guidelines concerning the provisioning of telecare services

User centered design and testing

1 - User Centered Development (UCD) methods should be an integral part of any development process of telecare services.

2 - UCD methods should be applied throughout all phases telecare service development.

3 - The telecare service design and development process should be a systematic procedure, based on prototyping and where relevant, iterative.

4 - Evaluations and testing of telecare services should be conducted with domain experts and representative user samples during all stages (including customization), with the evaluation results fed back into the product and service development process.

5 - Industry standard formats and tools should be used to support the definition and management of user requirements and system functional specifications along different stages of the telecare lifecycle.

Privacy and confidentiality guidelines

1 - Stakeholders should respect a client's right to give, withhold or withdraw consent for others to access or disclose sensitive information about themselves. Telecare systems should be designed and operated such that the appropriate stakeholders are able to protect these rights.

2 - Stakeholders should understand the duty of confidentiality they have towards clients. Telecare systems should be designed and operated such that the appropriate stakeholders are able to meet this duty of confidentiality.

3 - Stakeholders should consider whether other factors relating to data security, e.g. integrity, authentication, non-repudiation and availability, need to be addressed in order to allow them to meet their duty of confidentiality towards their clients.

4 - Whether conducting trials or providing real services stakeholders should provide a clear explanation to the client of the procedures they will implement to protect the clients' privacy. Clients should be asked if the procedures are acceptable.

5 - Stakeholders should develop and implement an information retention policy, which describes how long, and under what conditions, client information may be kept.

6 - Stakeholders should ensure that a telecare system or service does not compromise existing security measures protecting the privacy of clients.

Ethics guidelines

1 - Telecare systems should support the health, well-being and independent living of the client.

2 - Telecare systems should respect the client's decisions, dignity, integrity and preferences.

3 - Telecare systems should not adversely affect the delivery and user experience of existing services provided to clients.

4 - Appropriately qualified individuals should assess whether the proposed client is capable of consenting to take part in telecare research, or to have a telecare system installed as part of a running service.

5 - If the objective of researching, developing or deploying a telecare system is to reduce the amount of human input into a client's health/care regime then this should be clearly stated.

6 - National or regional rules for safeguarding the rights of participants should be followed when researching, developing or deploying a telecare system.

7 - End users that participate in the research, design or development of a telecare system should be appropriately acknowledged and/or remunerated.

8 - Consider the disruption and distress that the installation of a telecare system may cause to the client and minimize this by keeping the installation time to a minimum.

9 - Clients should be provided with the means to raise any issues they may have with a telecare service or trial.

Guidelines for legal aspects

1 - Legal experts should be consulted to identify the relevant legal requirements for the country in which the telecare system will be deployed.

2 - Understand and accept the liabilities with respect to developing a technology that is subsequently used as part of a telecare service, or for providing a telecare service.

3 - Insurance cover should be in place when installing or maintaining telecare equipment within the end-user premises.

4 - Contracts should be setup between the various stakeholders involved in the development, manufacture and provision of telecare products and services. The contracts should clearly state the contractual undertakings, including responsibilities and liabilities, of the various stakeholders involved.

5 - Telecare equipment should meet the required electromagnetic compatibility standards for the country in which the equipment will operate.

6 - Telecare equipment should meet the required electrical safety standards for the country in which the equipment will operate.

7 - Telecare equipment should meet the required radio spectrum standards for the country in which the equipment will operate.

8 - Telecare equipment should display the relevant certification marks for the country in which it will operate.

Availability and reliability guidelines

1 - Telecare systems should be designed and operated such that the availability and reliability of the service meets the needs of the end user.

2 - Telecare equipment or services should be designed to have the required availability and reliability when used by the intended user group also in adverse environments and under adverse environmental conditions.

3 - Telecare equipment or services should provide some means of remote service access.

Integrity guidelines

1 - Telecare systems should be designed and operated such that data and information within the system cannot be tampered with, nor accidentally changed during transfer, storage and retrieval.

Safety guidelines

1 - Telecare systems should be designed for error avoidance, to minimize the probability of the user making errors with adverse effects.

2 - Telecare systems should be designed and operated with error tolerance, so as to minimize the adverse effects of any user error.

3 - Telecare system failures should not harm the user.

Usability and accessibility guidelines

1 - A telecare system's output should be perceivable by users. Important information, such as alarms or loss of critical functions, should be effectively notified to users.

2 - Telecare equipment should require a minimum of effort and time to achieve the desired goal. Furthermore, it should be easy for users to raise alarms in an emergency situation.

3 - The operation of telecare equipment should be understandable to all users.

4 - Assistive technologies should be usable in conjunction with telecare equipment. Telecare equipment should allow both direct use, and use by means of assistive technologies.

5 - Telecare equipment and services should support adaptation to clients' abilities and preferences, as well as to the context of use (e.g. when roaming).

6 - Consistency and standardized elements among user interfaces should be promoted in related telecare equipment and services, also when roaming (if supported).

7 - All users should have equivalent security, privacy and safety when using the telecare service, regardless of their functional abilities.

User education guidelines

1 - Telecare services should offer user education through the entire service provision cycle.

2 - User education material should be developed covering all necessary details, including:

1. User education material should be offered in a localized way, taking into

consideration the capabilities and limitations of the addressed user group(s).

2. User education should be offered in all necessary languages and through multiple

modalities in an accessible way, to all users.

3. User education should be offered using the most proper media selected.

4. Legal and safety considerations should be addressed.

Localization, customization and personalization guidelines

1 - Consider the target languages when producing the source texts and illustrations. Be aware of dialect variants, the adaptation of visual content to local cultures, formal and informal addressing, and the use of English-language terms.

2 - Use technical communicators who write in their own native language, and translators who translate into their own native language.

3 - Translators need to understand how the product is to be used, ideally by being provided with a prototype of the terminal or preferably, a service pilot. An explanation of how a new product or service differs from its predecessor may be sufficient.

4 - Differences among languages regarding the total number of characters required for a particular text should be taken into account.

5 - Provide localized versions in sign language (as it may be a primary language for people with hearing disabilities).

6 - Visual content (illustrations, icons, pictures, images) should be adapted for local cultures, when necessary.

7 - Translations and localized versions should be validated with end users and validators, who should have good knowledge of the product terminology in the local market.

8 - The validator should not be involved in any product development team (as the goal is to provide user-friendly, not too technical language).

Guidelines for organizational aspects

1 - Stakeholders should be aware of how the introduction of a telecare system may affect and change the work practices of those individuals who provide care to clients, and take steps to minimize any negative affects of such changes.

2 - Stakeholders should be aware of how the introduction of a telecare system may affect and change the organizational structure of those organizations involved in the care delivery process, and take steps to minimize any negative affects of such changes.

3 - Telecare trials should include research into how the telecare system might affect the current working practices and organizational structure of those individuals and organizations that might deploy the system.

Servicing and maintenance guidelines

1 - To be able to access telecare services, users should ideally not have to be exposed to any installation, setup, configuration and maintenance procedures.

2 - Installation, setup, configuration and maintenance should be addressed by service providers through manual, automatic, remote or presence procedures, which should remain as transparent as possible for clients, demanding minimal interaction from them.

3 - Avoid unnecessarily frequent upgrades of telecare equipment (hardware and software). Upgrades that only marginally enhance the service should be avoided. For the benefit of the end-user continuation and maintenance of hardware equipment is advised.