Remote Accessibility to Diabetes Management and Therapy in Operational Healthcare Networks

REACTION (FP7 248590)

D7-1 Security, privacy and trust requirements

Date 2011-11-28

Version 1.4

Dissemination Level: Public

Table of Content

Document control page

Code	D7-1_2011-11-28_ Security-privacy-and-trust-requirements_V1.4.doc
Version	1.4
Date	2011-11-28
Dissemination level	PU
Category	R
Participant Partner(s)	ATOS, FHG-SIT
Author(s)	Carlos Cavero, Carlos Marcos (ATOS), Frederik Franke (FHG-SIT)
Verified and approved by	
Work Package	WP7
Fragment	No
Distribution List	WP7
Abstract	This deliverable contains the security requirements needed for the REACTION system taking into account different components of the architecture.
Comments and modifications	
Status	☐ Draft ☒ Task leader accepted ☒ WP leader accepted ☒ Technical supervisor accepted ☐ Medical Engineering supervisor accepted ☐ Medical supervisor accepted ☒ Quality manager checked ☒ Project Coordinator accepted
Action requested	☐ to be revised by partners involved in the preparation of the deliverable ☐ for approval of the task leader ☐ for approval of the WP leader ☐ for approval of the Technical Manager ☐ for approval of the Medical Engineering Manager ☐ for approval of the Medical Manager ☐ for approval of the Quality Manager ☐ for approval of the Project Coordinator **Deadline for action**:
Keywords	
References	
Previous Versions	

Version Notes

Version	Author(s)	Date	Changes made
0.1	Carlos Cavero	2010-10-18	Initial version, TOC
0.2	Carlos Cavero	2010-11-07	First readable version
0.3	Carlos Cavero	2010-11-17	Including first round of partners comments
1.0	Carlos Cavero	2010-11-28	Corrections and elaboration of reviewer's comments. Internal version available for the consortium.
1.1	Carlos Cavero	2011-09-15	Initial changes in the consolidation process
1.2	Carlos Cavero	2011-10-13	Consolidation finished
1.3	Carlos Cavero	2011-10-14	Minor changes, deliverable ready for revision
1.4	Carlos Cavero	2011-11-28	Final version including the reviewers' comments.

Internal review history

Reviewed by	Date	Comments made
Matthias Enzmann	2011-10-24	The document needs more

			discussion on the actual requirements than on the process how to obtain them.
	Manolis Spanakis	2011-10-17	Include more details about each individual requirement.

1. Executive Summary

The objective of the WP7 – “Security, Privacy and Confidentiality” is to develop a visible and controllable distributed security and privacy model, based on the concept of trust as a multilateral relation among stakeholders in a community of patients, informal and formal healthcare carers. This deliverable aims to elicit the security requirements for the REACTION system in such a way as to provide a private, secure and trusted healthcare platform for in-patient and out-patient environment. This version is the result of the discussions maintained with clinical and technological experts regarding Security Framework in order to reach a common understanding on *what security means* inside the REACTION project.

Security, privacy and trust requirements have been considered a part of the overall REACTION platform design and implementation. When designing application for security protections, especially when sensible data is managed, we should consider several requirements such as risk associated with using information technology, the security dimensions (Authenticity, Privacy, Usability, Confidentiality …) which affect the requirements. Therefore, security and safety of the proposed services have been studied as well the legal framework for patient safety and privacy, without leaving out ethical issues that have been also analyzed. Based on the recommendations gathered the necessary actions to minimize risks and preserve privacy and security have been carried out.

Actors’ specifications and their roles have been done in line with the proposed REACTION use cases which cover the functionalities and expectations of the framework. The Security dimensions are described (designed) taking into account the different components of the REACTION platform, distinguishing between in-hospital and primary care domain. A textual treatment/summary of the requirements is essential to easily understand the purpose of this document, thus the exported JIRA requirements are included in the annex (section 11). Implications of standardization activities have also been listed in order to integrate the REACTION system with the major European and national initiatives.

The requirements are the pillars of the implementation process, because they define the constraints the platform must take into account. In this way, the requisites act as the guideline of the overall development process. JIRA tool has been used to elaborate the list of them and 67 security requirements have been discussed. This document summarizes the constraints for the system regarding security issues and it should be used as a reference in the implementation phase.

2. Terms and Definitions

For the purposes of this deliverable, the following abbreviations and acronyms apply.

2.1 Abbreviations and Acronyms

AGC	Automatic Glucose Control
BAN	Body Area Network
CGM	Continuous blood Glucose Monitoring
DoW	Description of Work
DSS	Data Security Standard
EE	Enterprise Edition
EHR	Electronic Health Record
EPR	Electronic Patient Record
ESB	Enterprise Service Bus
EC	European Commission
EU	European Union
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
ICT	Information and Communication Technologies
ID-FF	Identity Federation Framework
ID-WSF	Identity Web Services Framework
ISO	International Organization for Standardisation
IT	Information Technology
ICU	Intensive Care Unit
NFC	Near Field Communication
OAD	Oral Anti-diabetic Drug
OASIS	Organization for the Advancement of Structured Information Standards
PAN	Personal Area Network
PCI	Payment Card Industry
PoC	Point of Care
POCT	Point Of Care Technology
QoS	Quality of Service
RFID	Radio Frequency IDentification
RM	Requirements Management
RPM	Remote Patient Monitoring
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SoA	Service oriented Architecture
SOAP	Simple Object Access Protocol (XML protocol)
SOPs	Standard Operating Procedures
SSO	Single Sign On

SOX	Sarbanes-OXley
SVN	Source Versioning Number
TGC	Tight Glycaemic Control
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
W3C	World Wide Web Consortium
WAN	Wireless Area Network
WAN-IF	Wireless Area Network InterFace
WP	Work Package
WS	Web Services
WSS	Web Service Security
WSSF	Web Service Software Factory

3. Introduction

This document is the result of the discussions regarding the Security Framework maintained with clinical and technological experts in order to reach a common understanding on what security means inside the REACTION project. The elicitation of the security requirements for the REACTION platform (T7.1 – "Security Requirements") has been done using the Volere template and JIRA issue tracker.

The work on this deliverable was carried out in several steps:

- Security requirements were included in the REACTION requirements JIRA project as a result of the WP2 (Initial requirements) and WP4 (Data management requisites) elicitation process.
- Based on the REACTION scenarios the assets and the actors involved were identified and the requirements have been broken down taking into account the different parts of the system.
- Finally, all the requirements already stored in the REACTION JIRA project were consolidated, avoiding duplication and overlapping. The security requirements were stratified in order to have a clear picture of the necessities of the REACTION platform.

In the next sections we will explain a brief summary of the steps done to reach the elicitation of the requirements, starting on the REACTION scenarios and ending on the discussion of the security, privacy and trust requisites in order to better describe the platform constraints.

3.1 Overview of the REACTION Project

The REACTION project aims to research and develop an intelligent service platform that can provide professional, remote monitoring and therapy management to diabetes patients in different healthcare regimes across Europe.

The REACTION platform will feature an interoperable peer-to-peer communication platform based on a service oriented architecture (SOA) – all functionalities, including devices, are represented as services and applications consist of a series of services orchestrated to perform a desired workflow.

A range of REACTION applications will be developed mainly targeting insulin-dependent type 1 patients. The applications aim to improve continuous blood glucose monitoring (CGM) and tight glycaemic control for improved insulin therapy management and bolus dose adjustments.

The developed applications will assist healthcare professional, patients and informal carers, to better manage diabetes insulin therapy in a variety of settings, help patients understand their disease, support self-management and provide a safe environment by monitoring adverse and potentially life-threatening situations with appropriate crisis management.

The project will focus on and validate the REACTION platform in two operational healthcare domains 1) professional decision support in hospital environments for diabetic patients admitted to the general wards, and 2) control and management of outpatients in clinically diabetes schemes, including therapy compliance and support for self management. All applications will include closed-loop feedback mechanisms in a variety of forms [14].

3.2 Purpose, Context and Scope of this Deliverable

This section discusses the main intention of the deliverable. It shows on which work this deliverable is dependent, respectively, which work will be based on it. Moreover, it outlines the target audience and the scope of this deliverable.

3.2.1 Background and Context

Practically all partners participated in both of the two workshops held in the outpatient and the in-hospital domain in order to specify the healthcare scenarios with partners and invited experts and stimulate the discussions regarding common security criteria to provide a private, secure and trusted healthcare environment. The first internal version of D7.1 – "Security, privacy and trust requirements" was the result of these activities and was delivered on M9 in order to have a first overview of the security requirements. This final version of the document includes the consolidation process of all the aforementioned requisites.

The security requirements are closely related with WP2- "User Centric Requirements Engineering and Validation" and WP4 – "Data Management and Service Orchestration", therefore the initial security

requirements were available in the D2.5 – “Initial requirements report” and D4.3 – “Technical requirements for an implementation of a medical data management model” deliverables. The task T7.1 will study in depth the security requirements elicited in the previous documents in order to start the design of the security architecture (T7.2 – “Security Architecture”).

3.2.2 Target Audience

The target audience of the deliverable are primarily technical partners, but also ethical, legal and sociological aspects have to be incorporated into the security model for REACTION. Especially, questions concerning data privacy, data security or data availability must be addressed.

3.2.3 Purpose

D7.1 elicits the technical security requirements for the REACTION architecture, based on the functional requirements derived in WP2 and WP4. Thus, it is an important foundation for a secure and robust architecture.

3.2.4 Scope

The scope of D7.1 is not restricted to the gathering of technical requirements, but also covers the correlation with the legal issues, because privacy and trust requirements are also important for the users.

According to D2.5 and D4.3 also D7.1 follows the iterative approach for the yearly refinement of the requirements in the context of a user centred design approach whose results will be reported in future deliverables and fully managed using appropriate requirement management tools.

3.3 Focus group risk analysis

The main objective of the definition of the focus groups is to understand the relevant personal, social and cultural factors related to potential REACTION services. We aim to understand what diabetic patients, nurses, doctors as well as healthcare professionals and administrators expect from technology and what values, beliefs, hopes, concerns and hype are related to the use of REACTION services. We aim also to learn how the use of information technology is changing the experience of living with diabetes. Understanding societal factors is a core preliminary requisite for addressing ethical and social issues at the design stage of technology development. In order to collect, analyse and formulate the focus groups definition, in terms of requirements, a series of meetings have been taken place in different European countries between November 2010 and July 2011.

Regarding security issues the main themes that were explored during the focus group concern: Protection of personal data: Electronic Healthcare Networks require, in order to work, the processing of personal data. Data protection is a right protected by Article 8 of the EU Charter of Fundamental Rights. One of the objectives of data protection is to avoid the use of data concerning health for purposes different than disease management and, in particular, by someone who may abuse such information. At the same time, redirecting health data can be a successful part of the treatment of disease using remote monitoring systems. The difficulty for patients is to be able to discern whether they are giving away their information to trustworthy persons and not to someone who may abuse their data. The patient may have an interest in knowing which categories of information are transmitted and/or retained, or not? The patient may want to control any use of his or her personal data and be asked for consent. In addition to issues of Data protection, the question of a patient’s trust in the use of an internet platform in conveying personal medical information will be explored. In particular it will be important to gauge the potential user’s perceptions of the level of security that can be provided by such platforms.

Patient-care provider relationship: REACTION may bring about profound changes that affect patients’ participation the healthcare service. It may imply that a patient, sitting at home, will have measurements (glucose level, weight, blood pressure) taken and sent electronically to the doctor or the nurse. Whilst this would mean action by both patient and healthcare provider, the level of face to face interaction is reduced. This might affect the patient’s perception of the level of attention and guidance he or she is receiving from the care provider. The lack of personalisation in the medical relationship may nourish fears in the consistency of the REACTION platform in providing safe user feedback. The possibility of disruption in the infrastructure of the REACTION platform due to outside events e.g. telecoms failure may also serve to create fears in the minds of potential patients with regard to the platform’s safety.

4. Security Requirement Engineering

4.1 Introduction

The user-centred approach of REACTION requires management tools that allow requirements storage and monitoring during the various iterations of the evolutionary design and during the entire lifecycle of the project [16].

In principle, every software or application development project must be clearly defined before development begins. It must address a problem that the organization currently has. A requirement is a condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. The primary activities within requirements management include (see fig. 1) [16]:

- Planning the requirements phase
- Establishing the requirements process
- Monitoring and controlling requirements changes
- Tracking progress
- Resolving issues

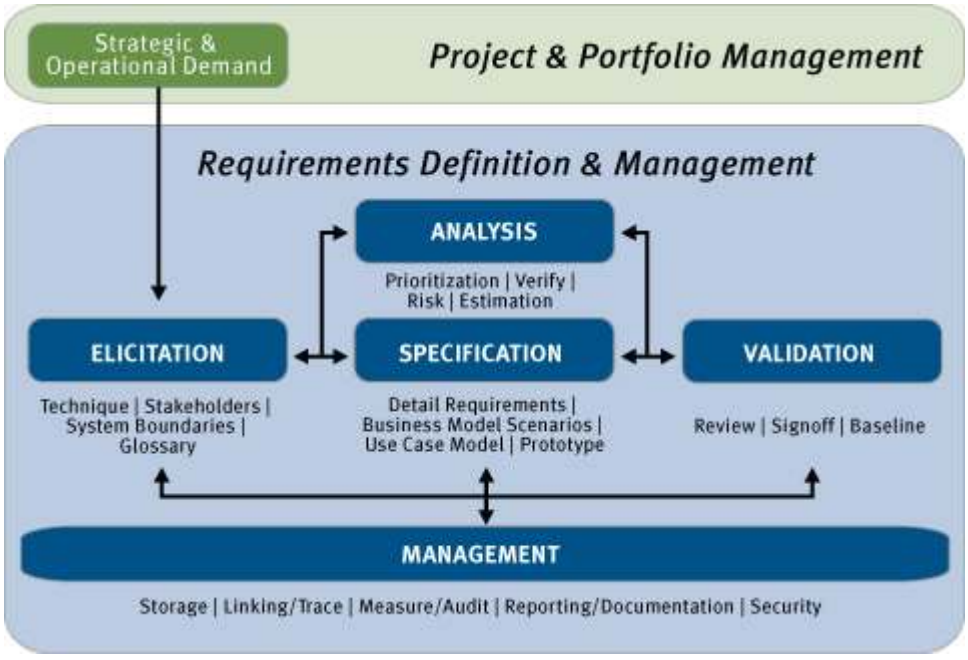


Figure 1: Requirements management process

4.2 JIRA Issue Tracker

JIRA is a proprietary issue tracking product, developed by Atlassian [1] and allow quite easily prioritizing, assigning, tracking, reporting and auditing project “issues” (i.e. requirements).

For the REACTION project the estimated needs were to have not more than 25 users and to manage not more than hundreds of requirements. This project size was considered very suitable to be managed with JIRA allowing a very low license cost, a reasonable cost for the JIRA server and the possibility of performing effectively the overall administration and configuration with a single person saving money and resources. Comparing the functionalities of JIRA to expensive RM tools it is possible to state that JIRA was much more attractive and suitable for the estimated needs of the REACTION project.

For the above reasons it was decided that JIRA is an ideal solution for the requirements gathering, analysis and management of the REACTION project [16].

4.3 JIRA Configuration

JIRA was installed on a server hosted at IN-JET premises and then configured for managing requirements in the REACTION project. The implemented configuration follows the ***Volere Requirements Specification Template***, as shown in fig. 2 [16].

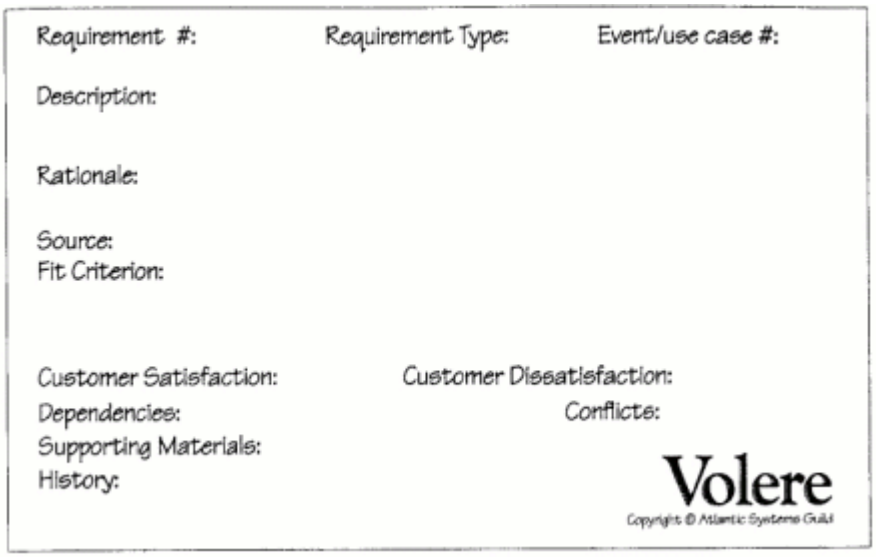


Figure 2: The Volere scheme/template

4.4 Towards a REACTION Security Architecture

REACTION platform should consider the evaluation criteria below when:

- **Types of security threats:** What set of security threats must the application protect against? What are the consequences of a security breach?
- **Laws and regulations:** What laws, regulations, or industry standards govern your industry or company? Do these laws, regulations, or standards raise the stakes in the event of a security breach? Do they mandate certain types of audit trails, minimum authentication and authorization constraints, digital signatures, and other security provisions?
- **Security policies:** What security policies has your organization established? What security requirements do they identify for different types of users or applications?
- **Types of users:** What types of users will access the application? Are they internal (employee, contractor, temp), external (employee, partner, supplier), or all of the above?
- **Types of client platforms:** What types of platforms will users or digital clients use to access the application? What are the native security features used by those platforms?
- **Type of server platform:** What application platform will the application run in? Is the strength of the platform's native application security framework sufficient to support the surety requirements of the application?
- **Type of protocols:** What protocols will clients use to access the application? What security facilities are supplied as a native function of the protocols? Are those security facilities sufficient to support the surety requirements of the application?

5. REACTION Use Cases

5.1 REACTION Use Cases

5.1.1 In-hospital Care

In-hospital hyperglycaemia has been found to be an important marker of poor clinical outcome and mortality among diabetic patients. The in-hospital care application domain of the REACTION platform will feature a suite of services aiming at Tight Glycaemic Control (TGC) of diabetics in the general hospital wards using continuous glycaemic monitoring and closed-loop feedback to the healthcare professionals at the point of care (PoC). Applications for Intensive Care Unit (ICU) patients are not envisioned, as all vitals of these patients typically are closely monitored, including measuring blood glucose directly on blood samples [18].

To enhance the mutual understanding of diabetes management in a hospital setting a workflow workshop was held at the University Hospital of Graz (clinical partner MUG), providing overviews of daily in-hospital routine and glycaemic management in a general ward, with existing workflows and workflow elements outlined [18].

5.1.2 Outpatient Care

The number of people with diabetes, both Type I and Type II, is increasing. Combined with an ageing population and the increase in other chronic diseases, closely related to unhealthy lifestyles, this constitutes a major challenge for healthcare services across Europe.

An essential part of diabetes case management for outpatients is glycaemic management, which is not a linear process. Co-morbidities and other clinical factors are involved; there is no clear finish and it remains iterative until death. Between check-ups blood glucose levels are the patients' own responsibility in terms of modifying their diet, taking their medications, measuring blood glucose and adjusting the dosage and timing of insulin, if prescribed. Measuring blood glucose is cumbersome and requires various paraphernalia at hand, and many patients do not carry out the measurements as often as they should. Therefore glycaemic management is generally poor, resulting in increased risk of long-term complications and hyperglycaemic and hypoglycaemic episodes. Real-life examples have been obtained through the results of an interview workshop involving five diabetes patients from Chorleywood Health Centre (CHC), one of the clinical partners. These patients portray five very different, but typical case histories, the common denominator being co-morbidities, usually also chronic [15].

5.2 REACTION Prototypes: Use-Cases for Applications

This section presents business use-cases for the inpatient and the primary care prototypes identified in the REACTION Scenarios [15]. These use-cases enable technical partners to obtain a better understanding of the main components of the REACTION prototypes, including how these components interact with users. Moreover, this chapter relates technical requirements for the REACTION data management model to (1) the inpatient glucose control and (2) the primary care disease management application. Therefore, for each of the prototypes, typical use-cases have been designed and use-case diagrams have been created for visualization. Requirements related to each prototype have been assigned to the use-cases and finally the implications for the REACTION platform technology have been described.

5.2.1 Inpatient Glucose Control (In-hospital Care)

In-hospital hyperglycaemia has been found to be an important marker of poor clinical outcome and mortality among diabetic patients. The in-hospital care application domain of the REACTION platform will feature a range of services aiming at Safe Glycaemic Control of diabetic patients using an individual target level depending on the history and actual state of the patient. In order to understand the clinical needs in the inpatient ward, a workshop at the inpatient site in Graz was held [15].

In the general ward, a REACTION application must monitor a range of parameters including blood glucose, nutritional intake as well as measures of insulin sensitivity. The data will be contextualised in the Data Management component and mathematical algorithms will be used to calculate the required insulin

doses. Results will be delivered to dedicated diabetes experts specialised in glycaemic control (usually located in a specialist diabetes centre) for verification and evaluation. Their on-line appraisal will be fed back to the physicians and nurses at the point of care in the patients ward. For the implementation of the new REACTION application, hospital systems will need to be adapted and hospital protocols across wards for monitoring of blood glucose levels and administrating insulin infusions will be required [18].

Figure 4 extracted from previous deliverables [18] summarise the results of the meetings as an Use Case Diagram.

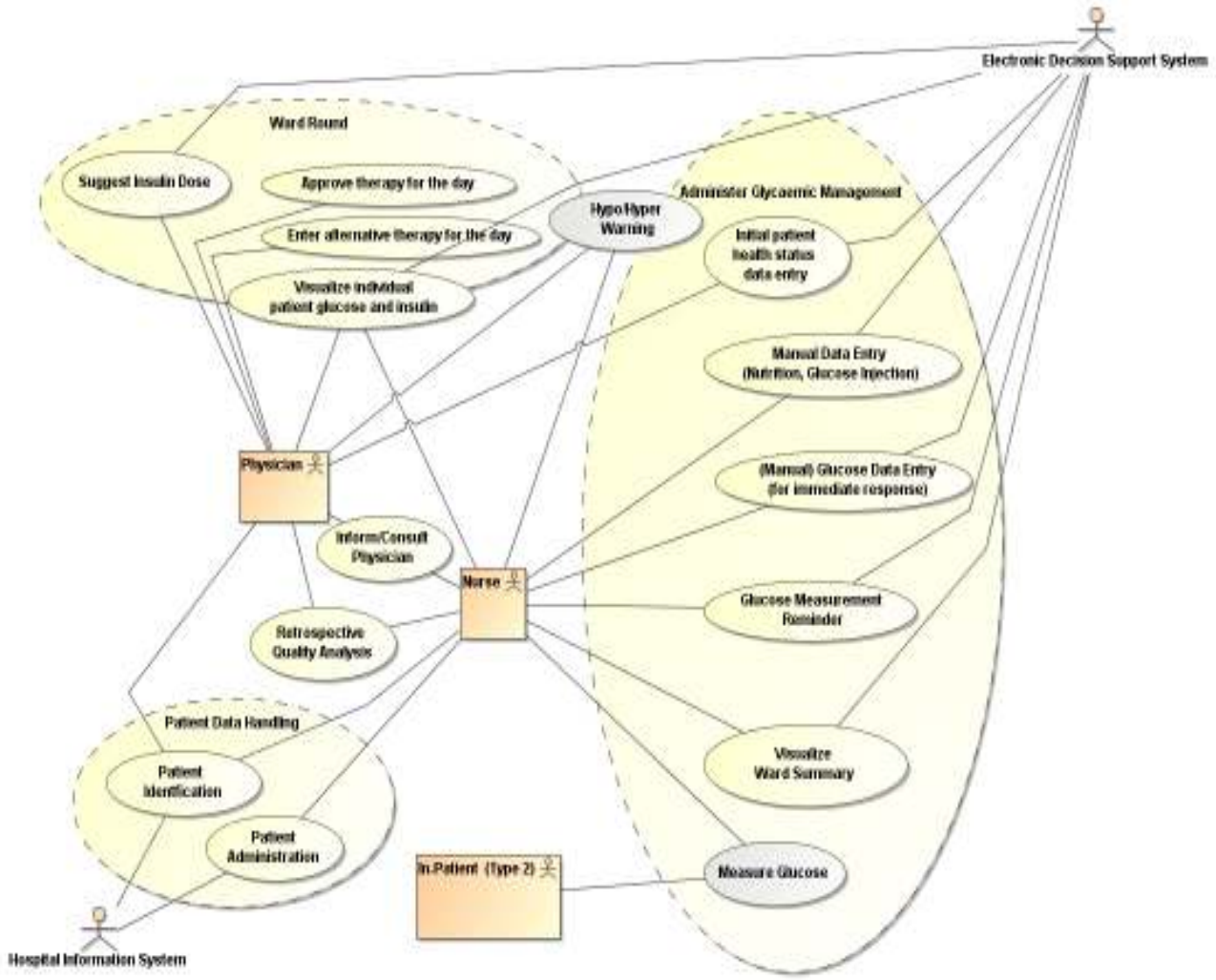


Figure 3: Use-Case Diagram for Inpatient Glucose Control

5.2.2 Primary Care Diabetes Management (Outpatient Care)

Diabetes mellitus is a chronic disease which starts slowly and progresses continuously. For this reason diabetes is diagnosed and treated mainly by primary care. In several healthcare systems in Europe, specialised units for diabetes care exist although their form and integration in health care varies (either hospital clinics mainly caring for complications as is the case in the U.K. or specialist practices outside the hospital that also take part in routine diabetes care as in Germany) [18].

REACTION aims at building a platform to support routine care for diabetes patients.

Several aspects have been identified, which the REACTION platform aims to support [18]:

- Continuous professional care: this comprises measures and actions to support disease management and patient care in the physician surgery.
- Self-management: this comprises measures and actions to support the patient in taking an active role in the management of the disease, supported by devices and an infrastructure to communicate measured values and receive support.

- Practice Organisation: Steps to improve quality of care to be taken at the level of the organisation (e.g. clinic, surgery).
- Administration: Required administrative steps

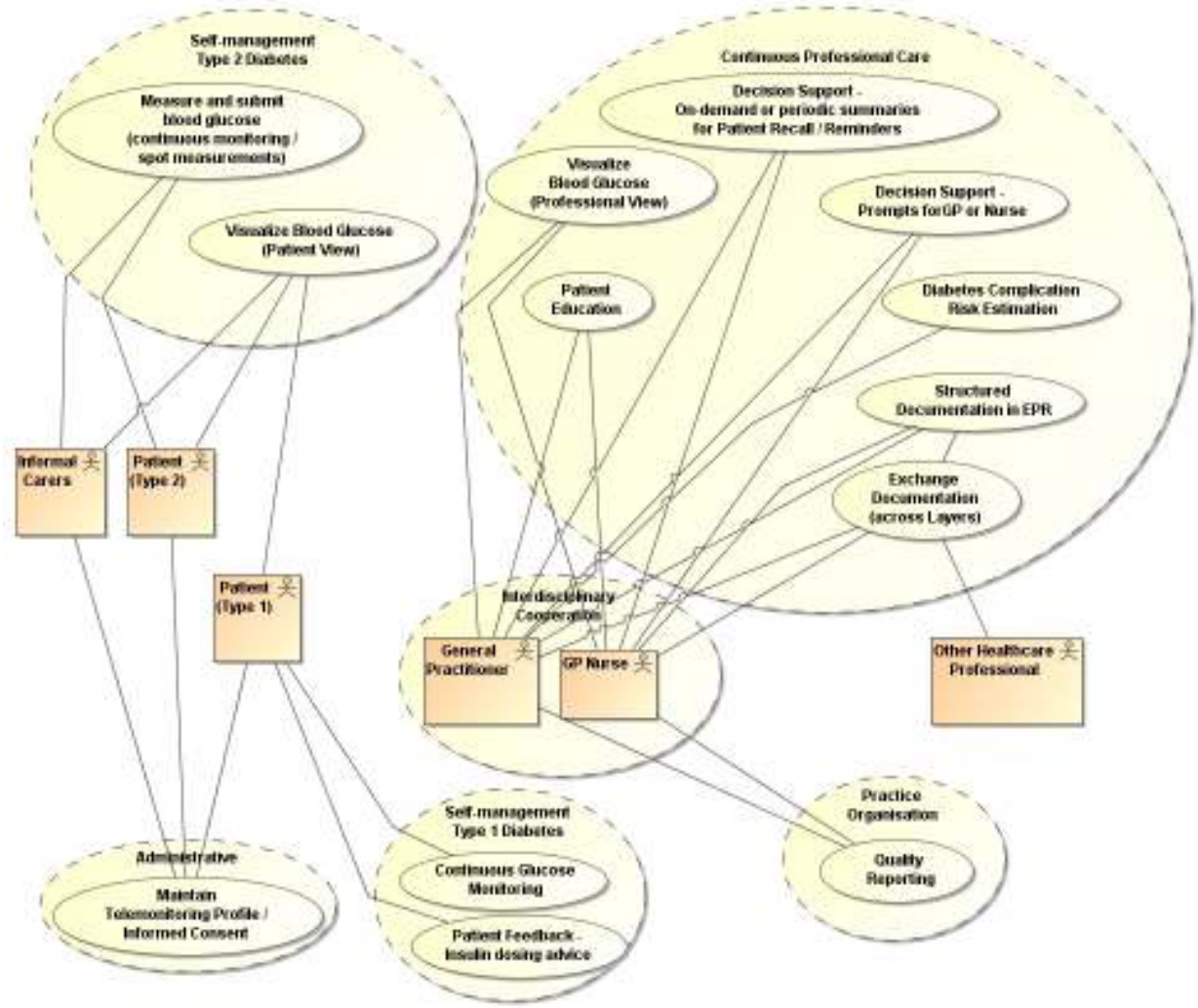


Figure 4: Use-Case Diagram for Primary Care Diabetes Management

5.3 Identification of involved actors

An actor "may represent roles played by human users, external hardware, or other subjects. Note that an actor does not necessarily represent a specific physical entity but merely a particular facet (i.e., "role") of some entity that is relevant to the specification of its associated use cases. Thus, a single physical instance may play the role of several different actors and, conversely, a given actor may be played by multiple different instances" [13].

The system will assist patients for whom it was decided to perform glucose management treatment by their physicians. Users of the system will be the medical staff (physicians and nurses) and technicians for system maintenance (all users can be considered as *professional users*).

The following subsections will break down the different actors and roles involved in REACTION and they were extracted from [17].

5.3.1 Patient / Relatives

A patient is any person who receives medical attention, care, or treatment. In the case of the REACTION platform the individual suffers from diabetes, both Type I and Type II and need the treatment by a physician or other health care professional, although one who is visiting a physician for a routine check-

up may also be viewed as a patient. The patient is also the person who will have the monitoring equipment in their home, use devices to take physiological measurements, input data into monitoring system and receive feedback via the monitoring system. The relatives are the individuals in charge of caring the patient such as: family members, friends, partners, wives, husbands, children or employers. The carer (family) is the person nominated by the patient who may also view patient data / assist patient in taking measurements.

5.3.2 Nurse

A diabetic nurse is a specialised health practitioner who focuses on managing the health conditions of her diabetic patients. Nurse practitioners have generally taken advanced courses in pharmacology (the effect of drugs on the body), pathophysiology (disease states) as well as health assessment. Diabetic nurses are required to have at least two years nursing experience as a registered nurse. Certain employers may require that diabetic nurses have a Master of Science nursing degree and be certified in diabetic education.

Nurses are the first line clinicians responsible for the patient – they will liaise with General Practitioners. They will:

- Identify patients to be put on the system
- Register patients onto the system
- Train patients in using the equipment in their home
- Receiving Alerts
- Review patient data on the system
- Follow intervention protocols
- Document actions on the system
- Contact patients
- De-register patients from the system

5.3.3 Physician / General Practitioner

A physician — also known as medical practitioner, doctor of medicine, medical doctor, or simply doctor — practices the ancient profession of medicine, which is concerned with maintaining or restoring human health through the study, diagnosis, and treatment of disease or injury (diabetics in this case). The physician has to define and to document (paper-based or paperless) the treatment (oral antidiabetic drugs (OADs) and/or insulin) and the number of measurement of the patient with hyperglycaemia or diabetes mellitus based on many important criteria (medical history, general health status, actual status, nutrition and associated conditions, planned examinations/treatments, interaction with other medication).

The General Practitioner is the second line clinician responsible for patient. While they may perform some of the same actions as the Clinician – Nurse, their main interaction with the system will be to:

- Receiving Alerts
- Review patient data on the system
- Follow intervention protocols
- Document actions on the system

5.3.4 Specialist

If complications are detected the patient will be referred to a specialist service which takes place outside of the General Practice. The sort of complications detected could come from:

- Cardiovascular Team
- Renal Team
- Ophthalmology
- Vascular Surgeon
- Neurologist
- Obs Gynae – pregnant patients only

5.3.5 Tele-health support team

Patients will be provided with a monitoring device. Clinicians and / or the Telehealth Support Team will view this data each day to review each patient's progress against individualised targets for the patients:

Medication Titration:

- Provide feedback to clinicians and patients on effectiveness of lifestyle and or medication therapies
- Safely optimise dosage
- Reassure patients concerned about their blood sugars

On-going Management:

- Support patients who are having difficulty managing their diabetes
- Provide feedback to clinicians and patients on effectiveness of lifestyle and or medication therapies
- Provide reinforcement to patients of required lifestyle changes
- Form part of the patient education on diabetes
- Used as part of a screening programme to identify better diabetes management for patients

5.3.6 Installer

The installer will be responsible for the installation, de-installation of equipment and patient training - could be a Clinician – Nurse

- Register patients onto the system
- Installing equipment
- Train patients in using the equipment in their home
- De-installing equipment
- Trouble shooting equipment

5.3.7 Administrator

The role of the "administrator", which is short for "system administrator", refers to either a responsible person or the job functions of managing and maintaining the system. The administrator carries out activities related to support the users of the platform: configuration, registration, maintenance producers (backups & restore), reviewing data and running reports.

5.3.8 Workflow Analysis

Inpatient Glucose Control (In-hospital Care)

The workflow of the in-hospital glycaemic management is impeded in the daily routine of the patients, the nursing and the medical staff. The routine of the latter two groups is very structured and standardised whereas the patients' workflows differs from day to day depending on the patients' health status as well as the planned examinations and their potential delays. These circumstances have to be taken into account for safe glycaemic control.

The current in-hospital workflow related to glycaemic management at the Endocrinology and Cardiology wards of the Medical University of Graz is described below and in Figure 5: Workflow description of Glycaemic Management of a General Ward. For further details see [17]

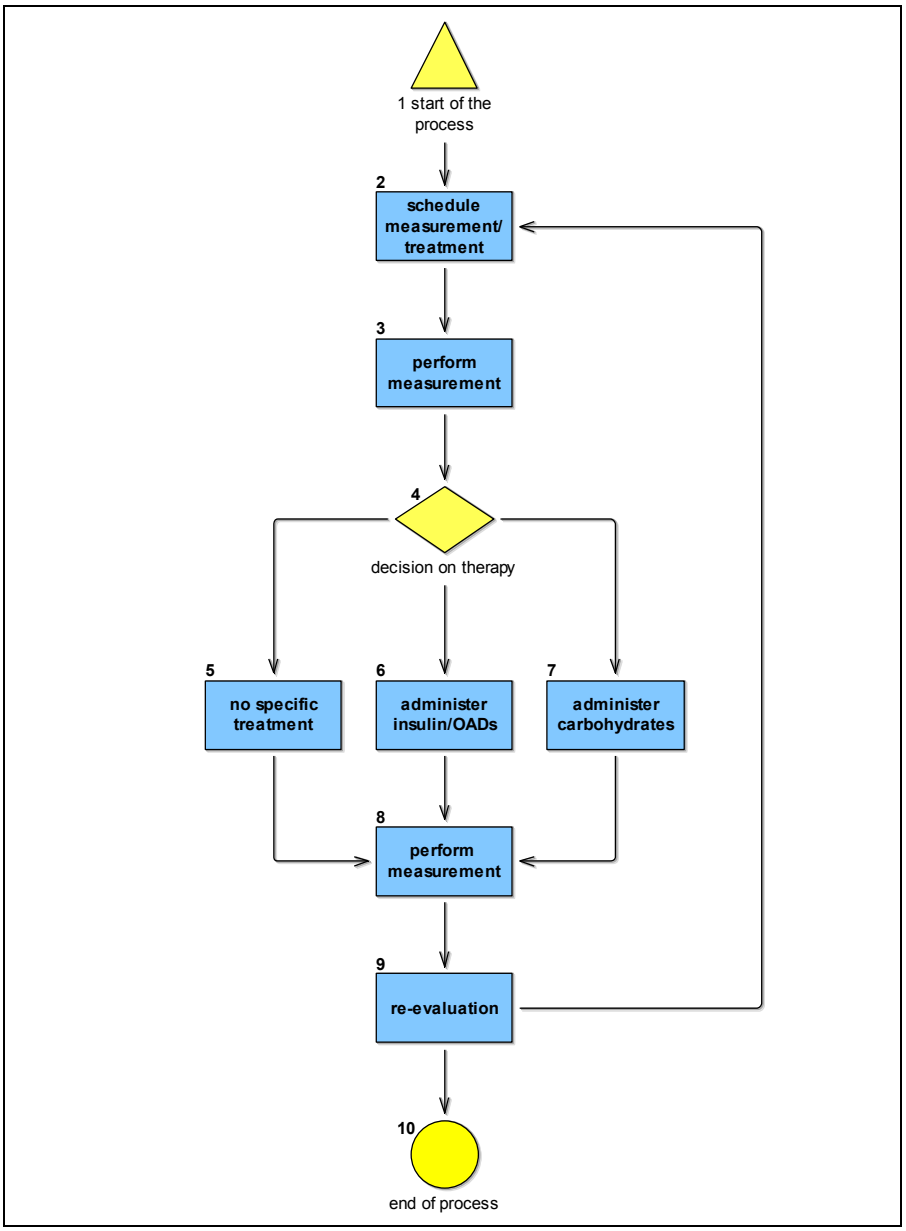


Figure 5: Workflow description of Glycaemic Management of a General Ward

Primary Care Diabetes Management (Outpatient Care)

The REACTION platform will be used to support various stages within Diabetes Management in Primary Care:

Medication Titration:

1. Provide feedback to clinicians and patients on effectiveness of lifestyle and or medication therapies
2. Safely optimise dosage
3. Reassure patients concerned about their blood sugars

On-going Management:

1. Support patients who are having difficulty managing their diabetes
2. Provide feedback to clinicians and patients on effectiveness of lifestyle and or medication therapies
3. Provide reinforcement to patients of required lifestyle changes
4. Form part of the patient education on diabetes

5. Used as part of a screening programme to identify better diabetes management for patients

Patients will be provided with a monitoring device. Clinicians and / or the Telehealth Support Team will view this data each day to review each patients progress against individualised targets for the patients. All actions, clinical notes and test results are documented in an Electronic Patient Record. Figure 7 provides an overview of this process. See further details in [17].

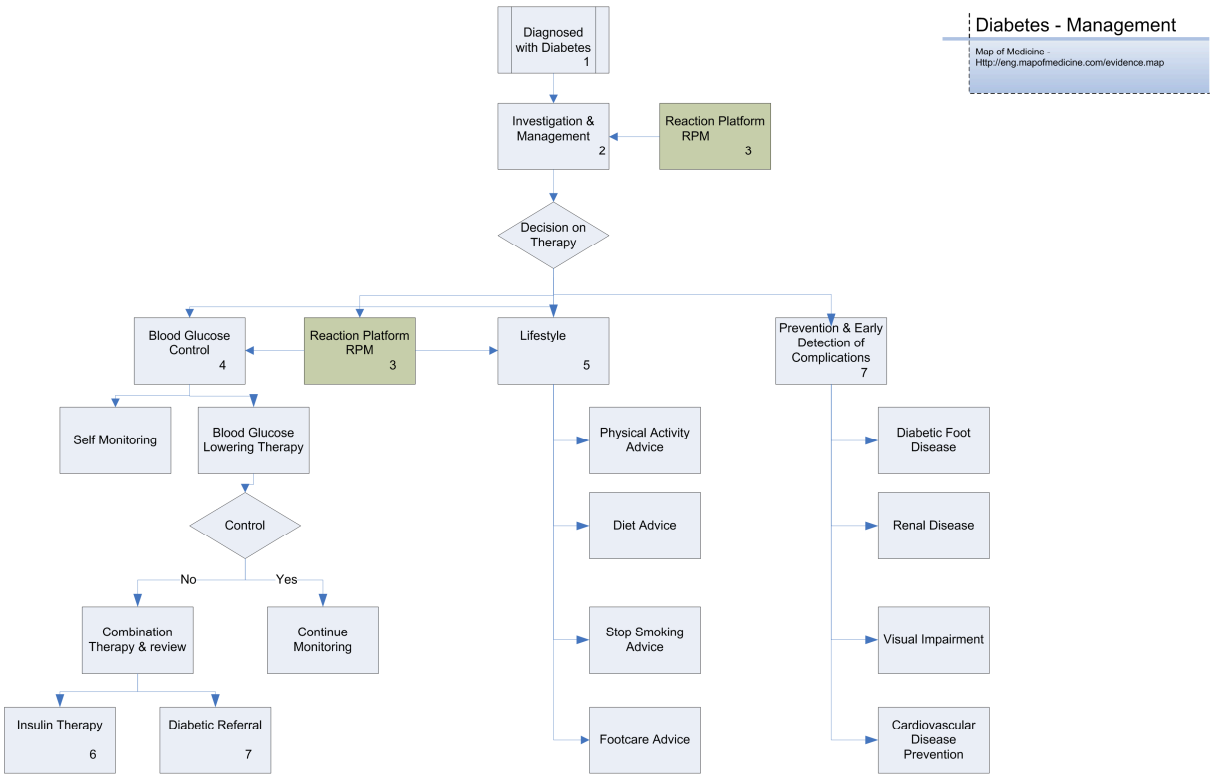


Figure 6: Workflow description of Primary Care Diabetes Management

5.4 Security dimensions

We can characterize security in terms of key security concepts **[ISO/IEC 27002]**: confidentiality, integrity, authentication, authorization, non-repudiation, and availability. These security goals are never absolute: it is not possible to guarantee 100% confidentiality, non-repudiation, etc. However, a well designed and implemented security response model can ensure acceptable levels of security risk. For example, depending on the information to be protected, using a well-designed cipher to encrypt messages may make the cost of breaking communications so great and so lengthy that the information obtained is valueless.

While confidentiality and integrity can be viewed as primarily the concerns of the direct participants in an interaction; authentication, authorization, and non-repudiation imply the participants are acting within a broader social structure.

5.4.1 AAA (Authentication, Authorization and Accounting)

Authentication refers to the process by which one participant can be assured of the identity of other participants.

Authorization concerns the legitimacy of the interaction. Authorization refers to the means by which an owner of a resource may give permissions to the information or part of it to certain users.

Accounting is the capability associated with resources that allows for the use of those resources to be measured and accounted for. This implies that not only can the *use* of resources be properly measured, but also that those *using* those resources also be properly identified.

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

5.4.2 Availability

Availability concerns the ability of systems to use and offer the services for which they were designed. One of the threats against availability is the so-called denial of service attack in which attackers attempt to prevent legitimate access to the system.

We differentiate here between general availability – which includes aspects such as systems reliability – and availability as a security concept where we need to respond to active threats to the system.

5.4.3 Confidentiality

Confidentiality concerns the protection of information of participants in their interactions. Confidentiality refers to the assurance that unauthorized entities are not able to read messages or parts of messages that are transmitted.

Note that confidentiality has degrees: in a completely confidential exchange, third parties would not even be aware that a confidential exchange has occurred. In a partially confidential exchange, the identities of the participants may be known but the content of the exchange obscured.

5.4.4 Integrity

Integrity concerns the protection of information that is exchanged – either from unauthorized modification or inadvertent corruption. Integrity refers to the assurance that information that has been exchanged has not been altered.

Integrity is different from confidentiality in that messages that are sent from one participant to another may be obscured to a third party, but the third party may still be able to introduce his own content into the exchange without the knowledge of the participants and possibly without them being able to detect the injected content.

5.4.5 Non-repudiation

Non-repudiation concerns the accountability of participants. To foster trust in the performance of a system used to conduct shared activities it is important that the participants are not able to later deny their actions: to repudiate them. Non-repudiation refers to the means by which a participant may not, at a later time, successfully deny having participated in the interaction or having performed the actions as reported by other participants.

5.4.6 Privacy

The term “privacy” is used frequently in ordinary language as well as in philosophical, political, legal and of course in Information Technology discussions, yet there is no single definition or analysis or meaning of the term. The concept of privacy has broad historical roots in sociological and anthropological discussions about how extensively it is valued and preserved in various cultures. Moreover, the concept has historical origins in well known philosophical discussions, most notably Aristotle's distinction between the public sphere of political activity and the private sphere associated with family and domestic life. Yet historical use of the term is not uniform, and there remains confusion over the meaning, value and scope of the concept of privacy.

Privacy is not about data—it's about people. Privacy is not secrecy, and it is not about hiding information. Privacy is concerned with the proper handling of personal information and with respecting the dignity of the individual to whom the information refers. The fundamentally contextual nature of the use of personal information prevents us from formulating a single strict definition of “privacy.” However, privacy principles accommodate this context and guide the development of enterprise privacy practices that can reduce risk and cost [4].

6. Security Requirements: REACTION Platform

The term “requirement” in engineering, is a singular documented need of what a particular product or service should be or perform. It is most commonly used in a formal sense in systems, software, or enterprise engineering. It is a statement that identifies a necessary attribute, capability, characteristic, or quality of a system in order to give value and utility to a user.

In the classical engineering approach, sets of requirements are used as inputs into the design stages of product development. Requirements are also an important input into the verification process, since tests should trace back to specific requirements. Requirements show what elements and functions are necessary for the particular project. [13]

Requirements Classification: from Wikipedia “Requirements are typically placed into these categories [13]:

- Functional requirements (F) describe the functionality that the system is able to execute; for example, formatting some text or modulating a signal. They are sometimes known as capabilities.
- Non-functional requirements (NF) describe characteristics of the system that the user cannot affect or (immediately) perceive. Non functional requirements are sometimes known as quality requirements.
- Constraint requirements (C) impose limits upon the design alternatives or project/process operations. No matter how the problem is solved: the constraint requirements must be adhered to.

The elicitation of the security requirements for the REACTION platform (T7.1 – “Security Requirements”) has been done using the Volere template and JIRA issue tracker. With regard to REACTION security requirements the requisites have been divided into several categories taking into account protection, privacy and security issues of the REACTION platform: General, Medical Devices, Communication, Data/Message, Access Control, Digital Entities and Privacy.

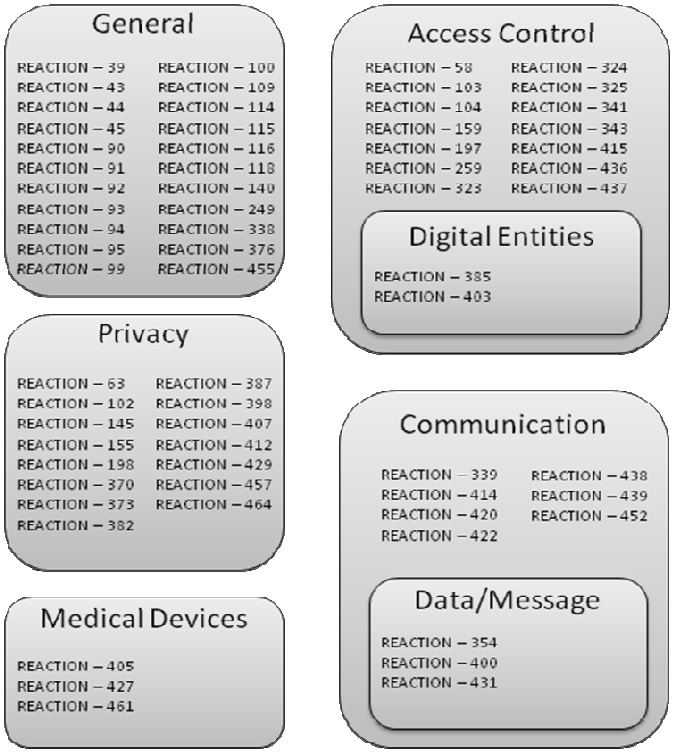


Figure 7: Security requirements - General overview

The security requirements have been divided in categories in order to facilitate the top/bottom discussion. The first group (General) contains the general constraints of the system: Integrity, Confidentiality,

Availability, Authentication, Authorization, etc, which are the overall restrictions of the platform in terms of robustness and stability. The rest of the requisites are related to those general aspects and they should be compatible with them. The categories are focused on particular components of the system. Starting from the Medical Devices which will provide the measurements to the rest of the systems involved. The Communications should be protected in order to avoid the risk of eavesdropping or tampering and the Data/Messages inside the transport layer should be ensured by means of encryption, signature and authentication. We have taken into consideration the Access Control to the system in order to check "who can access what type of information". Nurses and clinicians will have different roles and thus different permissions to the data. The restrictions to the information could be given automatically by means of Digital Entities generated by trusted (third) parties, e.g., certification authorities. Finally, Privacy issues have been also taken into account.

6.1 General

The system should comply with those main concepts broken down in this section. Overall terms like Integrity, Privacy and Authentication are the corner stone of the security measures for the platform. They are above of the more fine-grained requirements but all of them together should cover all those general restrictions.

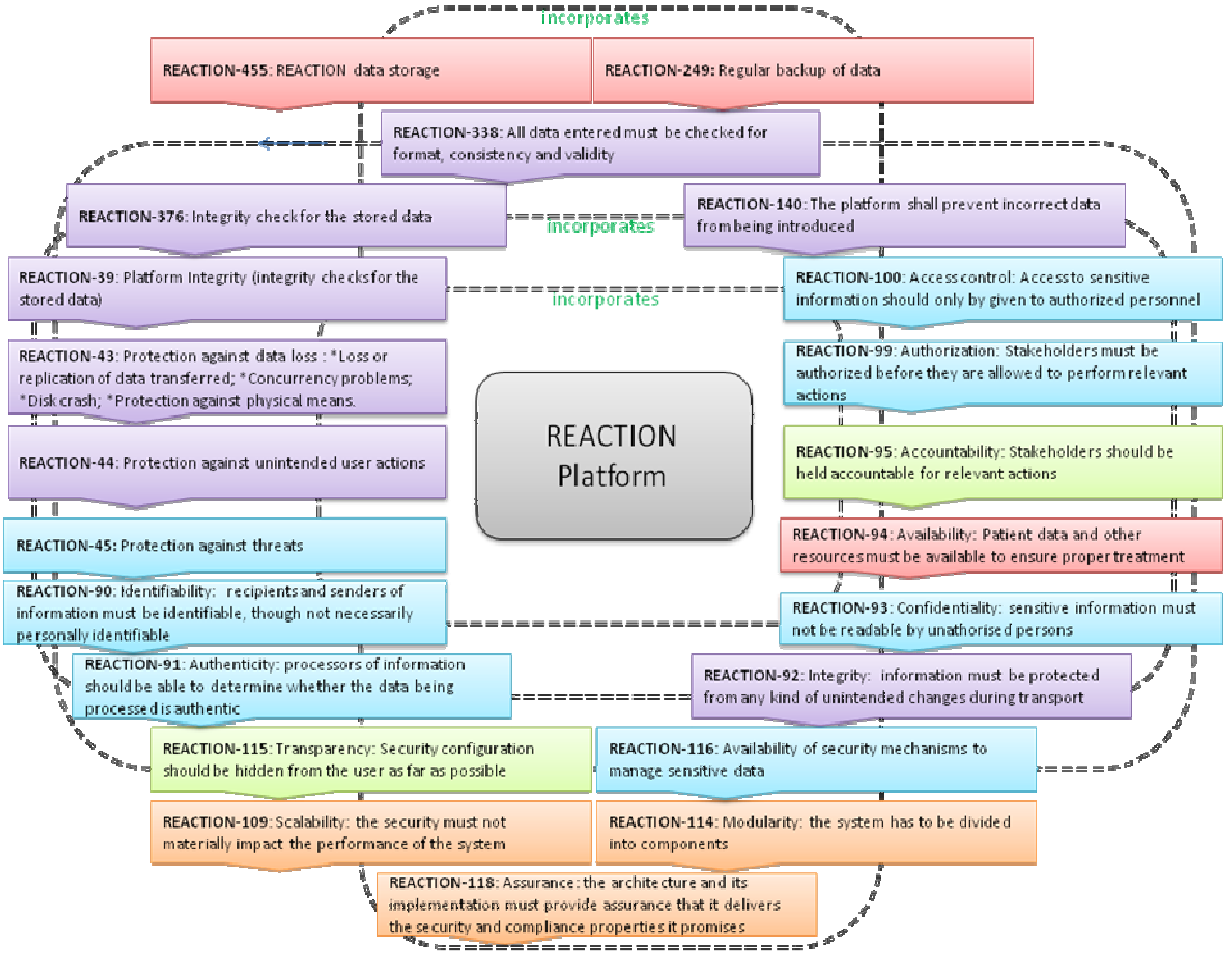


Figure 8: General / Architecture requirements

Each colour represents the interrelations between the requirements (red: availability, blue: management of sensitive information, orange: implementation aspects, violet: Integrity issues). There is not a unique correlation because some mechanisms incorporate several aspects as for instance: **REACTION-259, Regular backup of data** incorporates integrity and availability to the system.

The overall purpose of the security framework is to protect the system from the attacks outside the platform, but also to avoid the misuse of the available critical and personal information. The first important requisite is the **Platform Integrity for the stored data (REACTION-39)** in order to guarantee the integrity of the stored data in the case of an unwanted happening. Of course, in REACTION, we are dealing with sensitive data, thus security must be **available** on developed prototypes of the REACTION platform

(**REACTION-116). Scalability (REACTION-109), Modularity (REACTION-114) and Transparency (REACTION-115)** will facilitate the implementation of the protection mechanisms, because at the end, security must not materially impact the performance of the system.

As it is mentioned before, security deals with **protection against threats (REACTION-45) and against unintended user actions (REACTION-44)** and with **protection against loss or replication of data transferred between two systems (REACTION-43).** Because of the sort of data (medical) stored in the system, the unauthorized access to the information should be avoided. Therefore unauthorized persons cannot be allowed to neither obtain administer rights nor have access to personal data. **All data entered must be checked for format, consistency and validity (REACTION-338)**. In case of doubt, the user must be warned and asked what to do and must be able to correct mistakes easily. The functional test should include specific tests in order to verify such circumstances.

REACTION architecture and its implementation must provide **assurance (REACTION-118)** that delivers the security and compliance properties it promises. The obligations to comply with the security regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which require the system, its health care components and users in order to protect the **integrity (REACTION-92)**, **confidentiality (REACTION-93)** and **availability (REACTION-94)** of individually **identifiable** (**REACTION-90)** (not necessarily personal) health information created, received, transmitted or maintained include the implementation of security measures and particular safeguards to ensure the abovementioned issues, the protection against any reasonable anticipated threats and uses or disclosures of personal data.

In such a way the triple A, **Authentication (REACTION-91)**, **Authorization (REACTION-99)** and **Accounting (REACTION-95)** should assess:

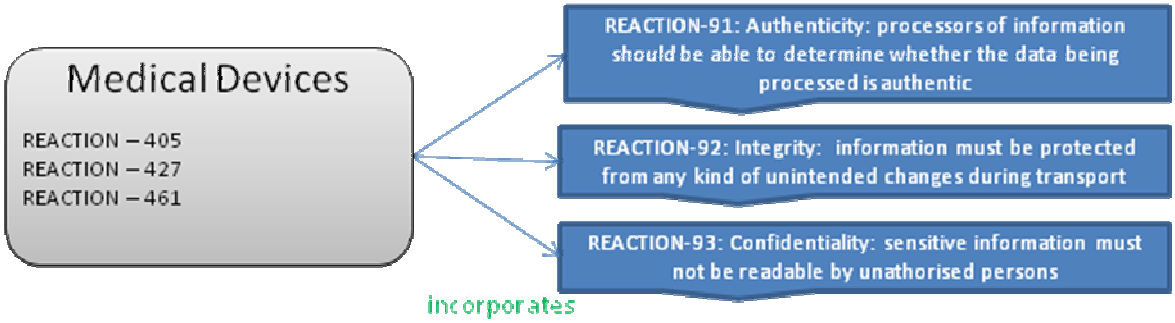
- The data's quality, incorporating mechanisms to verify that for instance the blood glucose measurements or personal data is originated from a known/trusted source.
- The relevant actions should be made by the correct person, thus it should be clear who made the decision, what kind of decision was made and when it was made.

Access Control (REACTION – 100), should provide the permissions to specify who can see the information. Sharing patient data is necessary in health care to treat patients but access to sensitive data should only be given to persons involved in the treatment which means authorized personnel. This requisite should provide the roles of each actor accessing the data and allow or deny the treatment of the private information.

The platform shall prevent incorrect data from being introduced (REACTION-140) mainly because incorrect information might hamper a correct clinical decision. This way the integrity of the stored data is guaranteed in the case of an unwanted happening. Besides, the platform should realize the **integrity checks for the stored data (REACTION-376)** using adequate methods like e.g. hash keys or redundancy codes for the information stored.

Finally **regular backup of data (REACTION-249)** should be done. Information shall be available even in case of a power failure, system breakdown or network unavailability through regular backup of data. This requisite is closely related to the **REACTION data storage (REACTION-455)** which provides a persistence layer for data storage with emphasis on data security and data access. The REACTION data storage should also use security mechanisms to include/exclude patient data access.

6.2 Medical Devices



Medical Devices

REACTION – 405. Authentication and integrity of transmitted measurements MUST be ensured.

REACTION – 427. Confidentiality of transmitted measurements SHOULD be ensured.

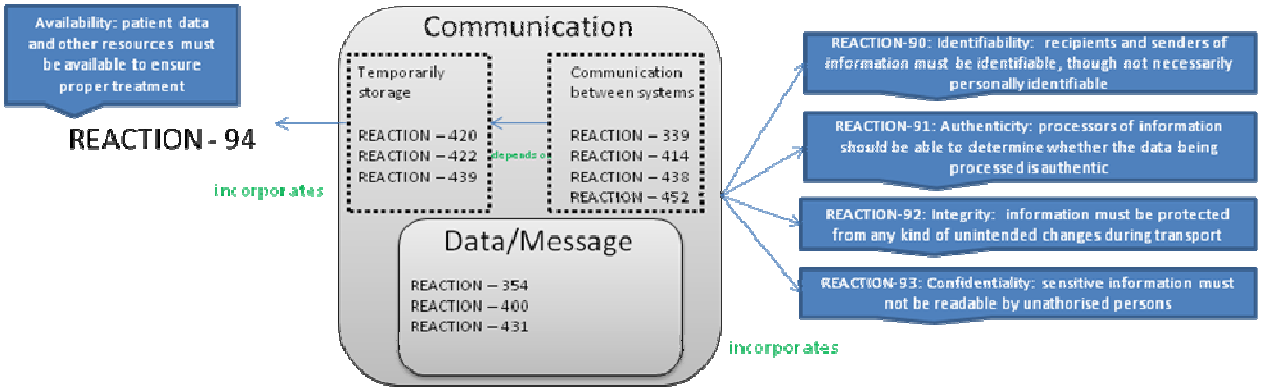
REACTION – 461. Sensor devices (PAN/LAN devices) and receiving devices (AHDs) MUST be paired to ensure entity authentication.

Figure 9: Medical devices requirements

The cornerstone of the REACTION system is the capability of recording information from sensors (blood glucose meters, etc). The security infrastructure should pay attention to the communication between the devices and the platform. Without any authentication, sensors may send data to unintended receivers, which might become a privacy problem, or AHDs may receive measurements from devices which are not the patient's, which might become a security problem and eventually a health problem if the patient receives the wrong treatment due to 'false' measurements. For this reasons, **sensor devices (PAN/LAN devices) and receiving devices (AHDs) must be paired to ensure entity authentication (REACTION-461).** The medical device must fulfil the Medical Device Directive (MDD) 93/42/EEC and subsequent amending directives like the directive 2007/47/EC

As it is mentioned in the general requirements the sensor layer must also ensure the transmission of information using **authentication and integrity of measurements (REACTION-405)** and of course preserve the **confidentiality (REACTION-427)** of the transmitted data, because without any data authentication, any measurement might be sent to the AHD without the AHD being able to distinguish between measurements from associated sensors and others. Also, if the measurements could be undetectably changed during transport, intentionally or unintentionally, this may have ill-effects on the patient's health because he might receive the wrong treatment due to 'false' measurements.

6.3 Communication security



Temporarily Storage

REACTION – 420 Data should be automatically saved in temporary file when PDA battery is running out.

REACTION – 422 User tranparency in case of communication failure

REACTION – 439 Information should be cashed in local storage to prevent loss in case of a node or communication failure.

Data/Messages

REACTION – 354 Data/messages exchanged between the Reaction Host Client and the Reaction Device Hosting Server MUST be authentic (message authentication) with integrity and confidential.

REACTION – 400 Data/messages exchanged between the Reaction Device Hosting Server and the EPR/EHR System SHOULD be authentic (message authentication) with integrity and confidential.

REACTION – 431 Data/messages exchanged between the Reaction Device Hosting Server and the GP EPR SHOULD be authentic (message authentication) with integrity and confidential.

Communication Between Systems

REACTION – 339 Communication between the Reaction Device Hosting Server and the patient's/GP's web browser MUST be authentic (entity authentication) with integrity and confidential

REACTION – 414 Communication between the Reaction Hosting Client and the Reaction Device Hosting Server MUST be authentic (entity authentication) with integrity and confidential

REACTION – 438 Communication between the Reaction Device Hosting Server and the GP EPR MUST be authentic (entity authentication), with integrity and confidential

REACTION – 452 Communication between the Reaction Device Hosting Server and the EPR/EHR System MUST be authentic (entity authentication) with integrity and confidential

Figure 10: Communications and Data / Messages and their relation to the general requirements

Figure 10 shows how the communication requirements incorporate the general requisites in order to protect the platform. Communication deals with the transport layer (the channel) but not necessarily with the data inside the connection. Thus the system should also take into account the message authentication, encryption and signature.

The communication security is the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. In the REACTION system it will be necessary to ensure the communications between the REACTION Hosting Client and the REACTION Device Hosting Server (REACTION-414) by means of entity authentication. It must be assumed that data transmission from the different entities and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it must be ensured that the communication channel is authentic, with integrity, and confidential. Likewise the communication between the REACTION Device Hosting Server and the EPR/EHR System (REACTION-452), the GP EPR (REACTION-438) and the patient's/GP's web browser (REACTION-339) must be authentic. Those requirements cover the communication channel (the transport layer) but the data transmitted over this channel should be protected.

This group also covers the temporarily storage of the information in case of communication failure. Data should be automatically saved in temporary file when PDA's battery is running out (REACTION-420). Information should be cashed in local storage to prevent loss in case of a node or communication failure (REACTION-438). In case of low battery the client application should be able to store temporary data. This will a) allow user to continue the process later and b) prevent corrupted / incomplete data to be uploaded to the main server. It is important to remark that user transparency should be provided in case of communication failure (REACTION-422). In case of network error the client application should be able to store temporary data. The system should detect problems on the network and start the local storage.

From the client's viewpoint, failures should be perfectly masked, and service should be completely fault-tolerant.

6.3.1 Data/message

The security framework aims at ensuring the information in the system. The data/message transmitted between sensors, REACTION platform and clients must be protected. In the REACTION system it will be necessary to ensure the data/messages exchanged between the REACTION Hosting Client and the REACTION Device Hosting Server (REACTION-354) by means of message authentication, encryption and signature. The security of messages transferred between the REACTION Host Client and the REACTION Device Hosting Server must be ensured even after the message was received - this is true even if the message was received over a secure communication channel. To guarantee this, the messages themselves MUST be self-contained with respect to authenticity, integrity, and confidentiality. Likewise the data/message exchanged between the REACTION Device Hosting Server and the EPR/EHR System (REACTION-400) and the GP EPR (REACTION-431) should be authenticated.

6.4 Access Control

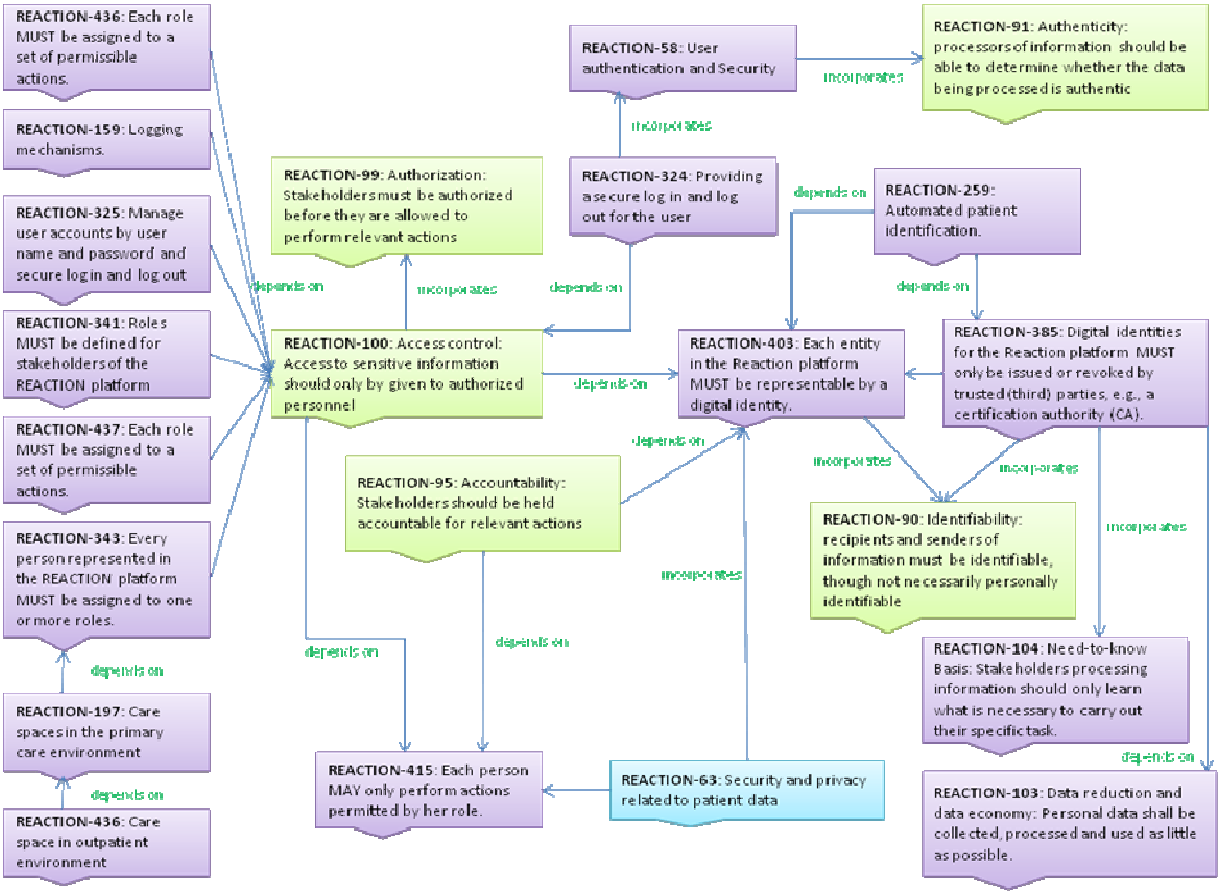


Figure 11: Access Control and Digital Entities requirements

Figure 11 shows how the Access Control is applied to the system and how the requirements are interconnected with each other and with the other groups (green, general and blue, privacy). The access control security mainly deals with the roles inside the system, what profiles should access the information and what should not. This way, it also deals with the log in and log out in the system by means of user authentication and security and of course the logging mechanisms to control the system and permit the traceability. Digital Entities can permit to process the information as little as possible.

Access control is a system which enables an authority to control access to areas and resources in a given physical facility or computer-based information system. In REACTION system **the patient identification should be automatic (REACTION-259)** in order to avoid identification mistakes. Risks of wrong patient

identification have to be negligible. The REACTION identification system must be flexible enough to integrate existing identification methods employed on site, e.g., wards in a hospital.

Sharing patient data is necessary in health care to treat patients but access should only be given to persons involved in the treatment, for this reason **access to sensitive information should only be given to authorized personnel (REACTION-100)** preventing the misuse of data. Each person in the REACTION platform will have the right to perform a certain set of actions. In order to simplify the administration of these rights, each person will be assigned to a role and roles are assigned to permissible actions. The access should be given **providing a secure log in and log out for the user (REACTION-324)** incorporating the **user authentication and security (REACTION-58).** The system shall be protected with a secure login for each user on the system; users shall be required to log out upon the end of the task. The system shall have a clear hierarchy for different type of users (Patient, Clinic, etc) and each user logging into the system shall be logged into the correct user type. Each user of the whole system should have access only to the components that are related to his work. Also there should be different level of access to the functionality within the components based on his role. The platform should also provide **logging mechanisms (REACTION-159)** from all components within Health Status Profile to easily control the system. The advantage of this approach is that it is easier to manage the rights of a role than managing individual rights for each person **(REACTION-341, REACTION-343, REACTION-437 and REACTION-415)**. In order to interact with the REACTION platform, persons need certain rights which depend on the **care spaces in the primary care environment (REACTION-197) or care space in the outpatient environment (REACTION-436)**. Patients and informal carers have to be included in the process of care. Care spaces (for each patient) have to be developed where the roles and tasks are distributed among the multidisciplinary health care team members. The patients have to be provided with their own self management tasks in an ongoing relationship with the other members of the team. Only people registered in the patient care space can access the patient data (clinical and demographic).

The system will provide **the possibility to manage user accounts by user name and password and secure log in and log out (REACTION-325).** The administrator of the system shall have full ability to reset user name and password of users and should assign the roles to the corresponding people in order to allow the users accessing to the right set of information and actions to be done with the data.

6.4.1 Digital Entities

In the REACTION platform, entities must be uniquely **identifiable and recognisable** by **digital entities (REACTION-403)** in order to allow repeated communication, referrals, accountability of actions, exclusion of ill-behaving entities, etc. **Digital identities for the REACTION platform MUST only be issued or revoked by trusted (third) parties, e.g., a certification authority (CA) (REACTION-385).** Without a trusted party (TP), anyone could produce its own digital identity and someone relying on such an identity would have to trust that the claimed identity is genuine. By incorporating a TP, relying parties trust that the TP ensures the validity of their issued digital identities. This eases relying parties' tasks as they only have to establish a single trust relationship (with the TP) as opposed to having a multitude of trust relationships with others. The same goes for parties that had been excluded from the REACTION platform, as each relying party would have to determine by itself if another party is still part of the REACTION platform or not. In case of a trusted party, the relying part could simply query the TP if some identity is still valid or had been revoked, e.g., because its owner left the platform.

The use of digital entities facilitates the **Need-to-know Basis** approach**: Stakeholders processing information should only learn what is necessary to carry out their specific task (REACTION-104).** In an information processing chain, several stakeholders might be involved but it might not be necessary for every stakeholder to know which exact data another stakeholder has processed and of course the **data reduction and data economy: personal data shall be collected, processed and used as little as possible (REACTION-103).** Handling personal data has to conform to privacy laws. In particular, personal data shall be rendered anonymous or pseudonymous as allowed by the purpose for which they are collected and/or further processed or used.

6.5 Privacy

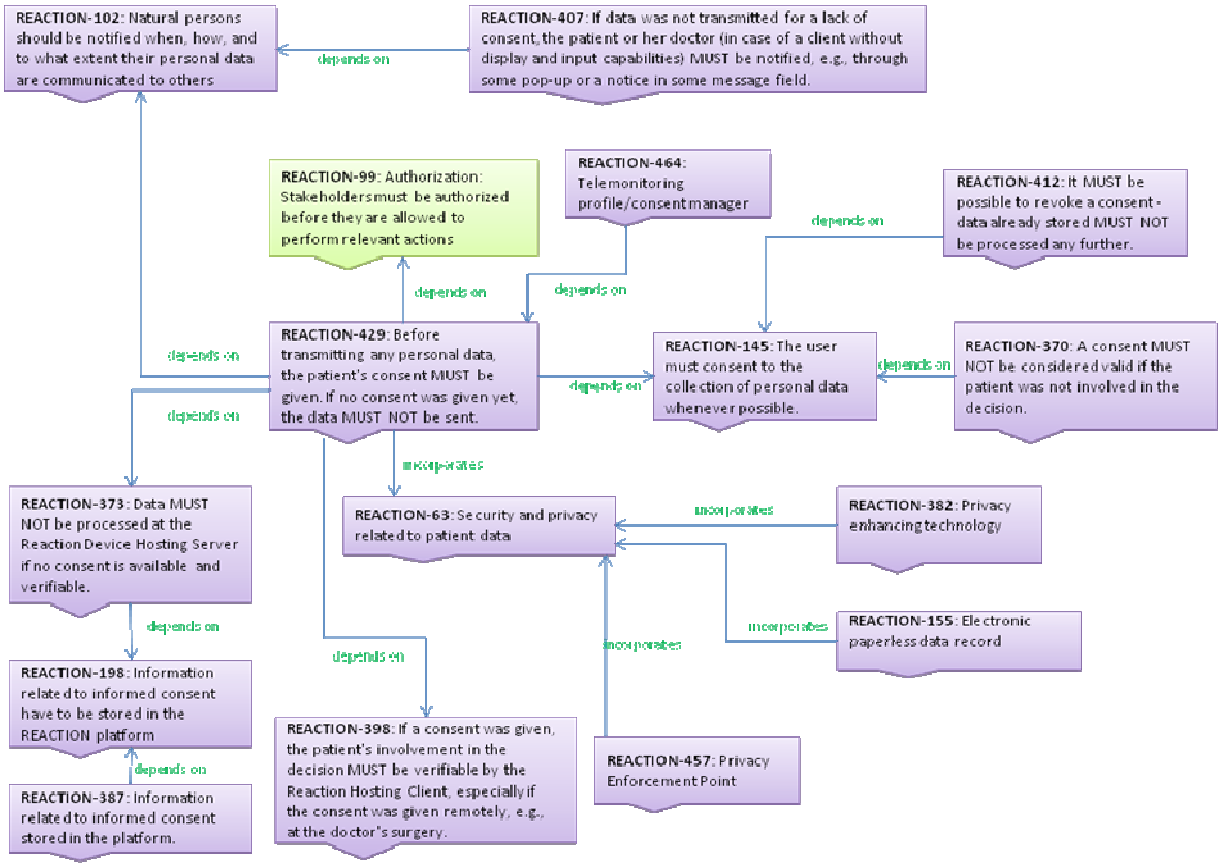


Figure 12: Privacy requirements

Figure 12 shows the interrelation between the Privacy requirements and how to deal with the management of private information of the patient. The main concept here is consent, which is the acceptance by the patients to the access to their personal data. Revoking the consent means the immediate denial of accessing the data stored.

Security and privacy related to patient data (REACTION-63) are of utmost importance. The patient data should be transferred and maintained in a secure way while any access to them should be monitored and logged (getting advantage of a login mechanism available in the applications). Privacy ensures that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for. In such a way handling of personal data has to conform to privacy laws. In REACTION system in order to protect the privacy of the users personally identifiable information (PII) and further more personal data the focus will be in enhancing the privacy of the individual inside the platform **(REACTION-382).** Each measurement in each transmission channel shall be separated from the patient data and association between measurements and patient shall not be possible for whoever may intercept the measurements. In particular, personal data shall be rendered anonymous or pseudonymous as allowed by the purpose for which they are collected and/or further processed or used. This (might be/) is in conflict with unnecessary collection of personal data, which are not required to fulfil a specific task **(REACTION-102)**. Privacy laws require that data subjects have to consent to the transmission and processing of their data. If a new data item is to be transferred which was not foreseen in the initial consent, the subject has to give a 'new' consent before the new data item can be transferred and subsequently processed. If the subject's AHD has a display and input capabilities, the AHD may directly ask the subject for a new consent -- of course, the subject may also decline the request (**REACTION-407)**. If the AHD is an appliance without display, the transmission must include some kind of notice to inform the requesting party, usually the patient's doctor, that some data item was not transmitted and that the subject should be asked for an extended consent.

Telemonitoring profile/consent manager (REACTION-464) module should provide security mechanism for data stored in the REACTION platform. Patients have to acknowledge that personal data gathered from them can be stored and transmitted within the technical infrastructure of REACTION. Therefore the

patient has to sign a consent form and the information about this should be stored within the system. **The user must consent to the collection of data whenever possible (REACTION-145)**. The user is taken to be an autonomous individual who, in principle, decides what personal data to disclose and to whom. Of course this is not an absolute right, because legal obligations such as the law, contractual obligations, but also consequences of the performance of a contract, may overrule the right for the individual to withhold consent. Consent contributes to the realisation of a number of fundamental human values founding modern (western) societies, such as individuality, autonomy, dignity and civility.

Currently all actions are recorded on a paper chart/record. Because of data privacy protection and safety issues this record must not stay at the patient's bed but will be stored centrally. The medical staff (nurse/physician) has to look for the patient record every time before he/she goes to the patient. This means that the information is only available for one person at the same time (REACTION-155). Furthermore, in an information processing chain, several stakeholders might be involved but it might not be necessary for every stakeholder to know which exact data another stakeholder has processed (REACTION-104).

The patients have to give their consent to REACTION system in order to use their personal information. For this reason, **information related to informed consent has to be stored (REACTION-198, REACTION-429).** An ethical approved informed consent has to be signed (either digitally or in paper form) by patients before they can be enrolled in the REACTION platform. The enrolment procedure shall allow the storage of the digitally signed informed consent or of a scanned copy of the paper form signed informed consent and this procedure shall be completed before any other operation can be performed. The consent must be verifiable by the REACTION Hosting Client and the REACTION Device Hosting Server **(REACTION-398)** and **REACTION-373).** This consent must not be considered valid if the patient was not involved in the decision **(REACTION-370)** and it must be possible to revoke the consent **(REACTION-412).** A patient must have the option to decide whether personal data is processed or not at any time. If the patient once gave his/her consent it must still be possible for the patient to revoke his/her consent, which means that any further processing of the affected data is forbidden. Also, if a patient revoked his/her consent the existing data may not necessarily be deleted, however, it MUST be excluded from any further processing.

7. Standardization Activities

A custom application security framework can implement an enterprise's unique security requirements that are not supported by platform or third-party frameworks. A custom framework can hide the differences between the security features of different programming languages and development platforms. And a custom framework can define security features in isolation from the underlying systems that actually implement the many aspects of security functionality.

Government regulations such as Sarbanes-Oxley (SOX), the Revised International Capital Framework (Basel II), the Health Insurance Portability and Accountability Act (HIPAA), and the EU Directive 95/46/EC on Data Protection, as well as industry standards such as the Payment Card Industry (PCI) Data Security Standard (DSS) mandate specific levels of auditability, confidentiality, and other forms of information security. Enterprises subject to such regulations have much to lose if they cannot comply with them. For these organizations, developing a custom security framework that can be easily used by all applications regardless of platform or programming language is well worth the effort and expense.

Most large organizations have highly heterogeneous information technology (IT) environments. Enterprises typically rely on multiple application platforms, such as .NET, Java EE, mainframe systems, ESBs, and so forth. Native security frameworks are by definition specific to an application platform; their APIs and programming libraries are not portable to or usable from other platforms. Third-party frameworks are often tied to vendors' infrastructure products, and unless their APIs are completely based on open standards such as SAML, WSSecurity, or XACML, their interoperability with other infrastructure is limited. Open source frameworks are either language-specific or limited in functionality.

SAML 1.1 has become the de jure and de facto standard for most federated identity activity. Additional federated identity standards are still being developed by the Shibboleth project, the Liberty Alliance, and the Web Services Federation (WS-Federation) Technical Committee at OASIS.

The Shibboleth Project, a project of Internet2, a higher education consortium, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. The Shibboleth Protocols and Profiles specification, which builds on SAML 1.x, was submitted to OASIS.

The Liberty Alliance initially focused on addressing federation requirements for web applications. The Liberty Identity Federation Framework (ID-FF) extends SAML 1.x to enable web-application account linking, and this specification has been submitted to OASIS. SAML 2.0, which was ratified March 2005, brings together SAML 1.x, Liberty ID-FF, and Shibboleth functionality, and supports: authentication, authorization, and attribute assertions; single logout; account linking; attribute exchange; metadata exchange; pseudonymity; and other functions into a single set of specifications.

The Liberty Alliance has also developed the Identity Web Services Framework (ID-WSF), which provides a framework for creating and interacting with identity-based services, which are web services that can retrieve information about an identity, update information related to an identity, or perform some action for the benefit of some identity. ID-WSF includes a security framework for identity-based web services that extends WS-Security. ID-WSF also includes authentication, authorization, and SSO frameworks based on SASL that can support simple identity federation across web services using a credential mapping model. These capabilities compete, to a degree, with WS-Trust.

The WS-Federation specification builds on and extends the WSSF to support federation for web services. Similar to SAML 2.0, WS-Federation supports single logout, account linking, attribute exchange, metadata exchange, and pseudonymity, but unlike SAML 2.0, it provides these services for both web applications and web services. WSFederation also supports claims-based authorization and protection of a principal's privacy with respect to claims asserted in security tokens.

Technologies come and go, but software applications can have a long lifetime. By providing a high-level interface that is decoupled from platform- or product-specific features and APIs, a custom security framework can also free the enterprise to retire aging technologies and incorporate newer or more secure technologies without forcing developers to learn new methods and tools, and without rewriting existing applications.

8. Conclusions

The requirements of the system are the pillars of the platform. A complete list of constraints the system must comply with is essential in order to build a robust and scalable architecture. The security measurements to apply to the system have to be shortened, because security covers almost everything and developers must focus on the actual problem. Thus the security requirements help in the aim of protecting the REACTION system, breaking down all the components and considering the convenient mechanisms to protect them. Privacy (the right to limit who see the personal data) and trust (reliance on another person or role) and confidentiality (the obligation of others to respect the privacy of disclosed data) are key concepts in any health environment, because the access to sensitive information should be controlled by the system.

The deliverable started with a brief explanation of the security requirement engineering (already explained in [16]) and the use of JIRA and the Volere templates to manipulate the requisites. Secondly we reviewed the In-patient and out-patient use cases in order to give to the reader the context to understand the different components inside the REACTION platform. A detailed description of the actors and roles involved was provided in order to relate them to the Access Control requirements elicited. Also a brief outline of the new REACTION workflows for in-hospital and primary care prototypes was described. Finally a review of standardization activities was provided.

The security requirements (67) have been divided into seven groups in order to facilitate the top/bottom discussion:

- General: contained the general constraints of the system: Integrity, Confidentiality, Availability, Authentication, Authorization, etc, which are the overall restrictions of the platform in terms of robustness and stability.

- **Communication:** covered the requisites regarding the communication channels to be protected in order to avoid the risk of eavesdropping or tampering
    - **Data/Message**: breaks down the security measures which should be applied to the content of the transport layer: encryption, signature and authentication

- **Medical Device**: enumerated the restrictions applied to the measurements (data/messages) and the communications with the rest of the platform.

- **Access Control:** deals with the roles in the system and the access to certain sort of data. Medical professionals will have different profiles in the system and thus different permissions to the information.
    - **Digital Entities:** the restrictions to the information could be given automatically by means of Digital Entities generated by trusted (third) parties, e.g., certification authorities.

- **Privacy:** as we already mentioned covered the requirements which limit who can consult the personal data.

9. List of Figures

10. References

[1] http://www.atlassian.com/software/jira/overview
[2] Application Security frameworks, Joe Niski, Burton Group, 2008
[3] Enterprise Service Bus: A definition, Anne Thomas Manes, Burton Group, 2007
[4] Identity and Privacy strategies - Privacy, Ian Glazer and Bob Blakley, Burton Group, 2009
[5] Security and risk management strategies, Information Confidentiality, Trent Henry, Burton Group 2009
[6] Working Document on the processing of personal data relating health in Electronic Health Records (EHR), Article 29 – "Data Protection Working Party" of Directive 95/46/EC, 2007
[7] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification, 2006
[8] WS-Trust 1.3, OASIS Standard Specification, 2007
[9] Reference Architecture for Service Oriented Architecture Version 1.0, OASIS Standard Specification, 2008
[10]Performance issues in a secure health monitoring wireless sensor network, D.D. Kouvatsos, G. Min and B. Qureshi
[11] A context-related authorization and access control method based on RBAC: a case study from the health care domain, Marc Wilikens, Simone Feriti and Marcelo Masera.
[12] Security and Privacy issues with Health Care Information technology, Marci Meingast, Tanya Roosta and Shankar Sastry
[13] Wikipedia, http://en.wikipedia.org/wiki/
[14] REACTION "Description of Work" (DoW)
[15] D2.1 – "Scenarios for usage of the REACTION platform"
[16] D2.5 – "Initial Requirements Report"
[17] ID2.6 – "Prototype Application Specification"
[18] D4.3 – "Technical requirements for Medical Data Management"

11. Appendix A - Complete Set of Security, Privacy and Trust Requirements

11.1.1 [REACTION-464] Telemonitoring profile/consent manager Created: 29/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Stephan Spat	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - REACTION platform
Work package:	WP7
Rationale:	This module should provide security mechanism for data stored in the REACTION platform. Patients have to acknowledge that personal data gathered from them can be stored and transmitted within the technical infrastructure of REACTION. Therefore the patient has to sign a consent form and the information about this should be stored within the system. It should be possible to exclude several personal information from storage/transmission. This manager could be queried, e.g. by the data fusion component (or any other component that processes personal patient data) before anything is processed in order to determine if the processing was permitted by the patient. Such a permission would be expressed by way of a consent.
Source/Originator:	E-mail discussion between Stephan S. and Tamás T. with contribution from Matthias E. (2010-07-20 and 2010-07-21)
Fit Criterion:	Telemonitoring profile/consent manager will be technically implemented into the REACTION platform.
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.2 [REACTION-461] Sensor devices (PAN/LAN devices) and receiving devices (AHDs) MUST be paired to ensure entity authentication. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	PAN/BAN, Portable Devices, Security, Sensors

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP3, WP7
Rationale:	Without any authentication, sensors may send data to unintended receivers, which might become a privacy problem, or AHDs may receive measurements from devices which are not the patient's, which might become a security problem and eventually a health problem if the patient receives the wrong treatment due to 'false' measurements.
Source/Originator:	FHG SIT
Fit Criterion:	Some kind of 'pairing mechanism' or entity authentication MUST be used before any sensor data is transmitted or received.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.3 [REACTION-457] Privacy Enforcement Point Created: 29/Jul/10 Updated: 16/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Architecture, Backend Middleware, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Stephan Spat	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - REACTION platform
Work package:	WP4
Rationale:	A component that could be added to the client side would be some kind of 'Privacy Enforcement Point'. Such a component could be examining outgoing data for information that the client did not authorize to be sent, yet. That is, the component would match the client's consents (with respect to the processing of her data) with the the kind of information from the outgoing message and, possibly, delay the transmission of certain information which the client has not decided on. The component could stay hidden in other components for the time being, such as the Network Manager on the client side. The Privacy Enforcement Point should perform as a counterpart of the Consent Manager at the Reaction Device Hosting Server.
Source/Originator:	E-mail discussion between Matthias E. and Peter R. (2010-07-20 and 2010-07-22)
Fit Criterion:	Privacy Enforcement Point is available for the REACTION client side.
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.4 [REACTION-455] REACTION data storage Created: 29/Jul/10 Updated: 16/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Backend Middleware, Data Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Stephan Spat	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - REACTION platform
Work package:	WP4
Rationale:	The REACTION platform should provide a storage module (database). Data gathered within REACTION should be stored here, as well as relevant data from external sources. The REACTION data storage should also use security mechanisms to include/exclude patient data access.
Source/Originator:	Technical Meeting in Crete, architecture prototype.
Fit Criterion:	The REACTION platform provides a persistence layer for data storage with emphasis on data security and data access.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.5 [REACTION-452] Communication between the Reaction Device Hosting Server and the EPR/EHR System MUST be authentic (entity authentication), with integrity, and confidential.

Created: 20/Jul/10 Updated: 25/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Backend Middleware, Communication, Interfaces with HIS/EPR, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann

Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-168	Remote Patient Monitoring (RPM)	In Progress
	Incorporate			
	incorporates	REACTION-90	Identifiability: Recipients and sende...	In Progress
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
	incorporates	REACTION-91	Authenticity: Processors of informati...	In Progress
	incorporates	REACTION-92	Integrity: Information, in particular...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7, WP10			
Rationale:	It must be assumed that data transmission from the Reaction Device Hosting Server to the EPR/EHR System and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it MUST be ensured that the communication channel is authentic, with integrity, and confidential.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide communication channels with authenticity, integrity, and confidentiality.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.6 [REACTION-439] Information should be cashed in local storage to prevent loss in case of a node or communication failure. Created: 23/Jul/10 Updated: 17/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Backend Middleware, Communication, Networking, PAN/BAN, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Antonis Miliarakis	**Assignee:**	Antonis Miliarakis
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**			
	incorporates	REACTION-422	User tranparency in case of communica...	Open
	is incorporated by	REACTION-417	Dynamic data structure for inpatient ...	Open
Requirement Type:	Functional - REACTION platform			
Work package:	WP4			
Rationale:	In case of network error the client application should be able to store temporary data. This will a) allow user to continue the process later and b) prevent corrupted / incomplete data to be uploaded to the main server.			
Source/Originator:	DoW			
Fit Criterion:	The functional test should include specific tests in order to ensure that there is no data loss in case of network failure.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.7 [REACTION-438] Communication between the Reaction Device Hosting Server and the GP EPR MUST be authentic (entity authentication), with integrity, and confidential. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Backend Middleware, Communication, Interfaces with HIS/EPR, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann

Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-168	Remote Patient Monitoring (RPM)	In Progress
	Incorporate			
	incorporates	REACTION-90	Identifiability: Recipients and sende...	In Progress
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	It must be assumed that data transmission from the Reaction Device Hosting Server to the GP EPR and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it MUST be ensured that the communication channel is authentic, with integrity, and confidential.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide communication channels with authenticity, integrity, and confidentiality.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.8 [REACTION-437] Each role MUST be assigned to a set of permissible actions. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Context Management, Interfaces with HIS/EPR, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-100	Access control: Access to sensitive i...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Since some actions are reserved for specific roles it has to be decided which actions are permissible for which role.			
Source/Originator:	FHG SIT			
Fit Criterion:	According to the roles' needs, each role is assigned to a set of appropriate permissions.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.9 [REACTION-436] Care space in outpatient environment Created: 23/Jul/10 Updated: 16/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Data Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-197	Care spaces in the primary care envir...	Open
Requirement Type:	Functional - Primary care pilot application			

Work package:	WP4
Rationale:	Patients and informal carers have to be included in the process of care. Care spaces (for each patient) have to be developed where the roles and tasks are distributed among the multidisciplinary health care team members.
Source/Originator:	D2.1 and workshops
Fit Criterion:	The data management shall allow the storage of the care space for each patient with specific roles for each member of the care space.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness

11.1.10 [REACTION-431] Data/messages exchanged between the Reaction Device Hosting Server and the GP EPR SHOULD be authentic (message authentication), with integrity, and confidential.

Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Interfaces with HIS/EPR, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**			
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
	is incorporated by	REACTION-91	Authenticity: Processors of informati...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	The security of messages transferred between the Reaction Device Hosting Server and the GP EPR must be ensured even after the message was received - this is true even if the message was received over a secure communication channel. To guarantee this, the messages themselves MUST be self-contained with respect to authenticity, integrity, and confidentiality.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide data authenticity, integrity, and confidentiality			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.11 [REACTION-429] Before transmitting any personal data, the patient's consent MUST be given. If no consent was given yet, the data MUST NOT be sent. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major	
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann	
Resolution:	Unresolved	**Votes:**	0	
Issue Links:	**Depend**			
	depends	REACTION-102	Notice: Natural persons should be not...	Open
	depends	REACTION-145	The user must consent to the collecti...	Open
	depends	REACTION-99	Authorisation: Stakeholders must be a...	In Progress
Requirement Type:	Non-functional - Legal			
Work package:	WP7, WP9			
Rationale:	Privacy laws require that data subjects have to consent to the transmission and processing of their data. Without a consent, processing of personal data is not permitted by law.			
Source/Originator:	FHG SIT			

Fit Criterion:	A 'watchdog' component must be in place that supervises the transmission of personal data and takes action if data to be transmitted is not covered by the subject's consent.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.12 [REACTION-427] Confidentiality of transmitted measurements SHOULD be ensured. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Communication, PAN/BAN, Security, Sensors

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP3, WP7
Rationale:	Without any mechanism providing confidentiality, measurements sent from sensors might be overheard by third parties. This circumstance is alleviated a bit by the fact that sensors usually have a limited transmission range but active eavesdroppers may still use, say, antennas powerful enough to catch the signal.
Source/Originator:	FHG SIT
Fit Criterion:	A mechanism to ensure data confidentiality SHOULD be used whenever measurements are sent from the sensor to the AHD.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.13 [REACTION-422] User tranparency in case of communication failure Created: 30/Jul/10 Updated: 17/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Communication, Interfaces with HIS/EPR, Networking, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Manuel Marcelino Perez	**Assignee:**	Manuel Marcelino Perez
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**		
	is incorporated by	REACTION-439	Information should be cashed in local... Open
Requirement Type:	Functional - REACTION platform		
Work package:	WP4		
Rationale:	In case of network error the client application should be able to store temporary data (RDMM 76). The system should detect problems on the network and start the local storage. From the client's viewpoint, failures should be perfectly masked, and service should be completely fault-tolerant.		
Source/Originator:	DoW		
Fit Criterion:	User transparency refers to a combination of user friendliness' and 'high efficiency'.		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		

11.1.14 [REACTION-420] Data should be automatically saved in temporary file when PDA's battery is running out. Created: 23/Jul/10 Updated: 04/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	PAN/BAN, Portable Devices, Security, Sensors

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Antonis Miliarakis	**Assignee:**	Antonis Miliarakis
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP4
Rationale:	In case of low battery the client application should be able to store temporary data. This will a) allow user to continue the process later and b) prevent corrupted / incomplete data to be uploaded to the main server.
Source/Originator:	Forthnet
Fit Criterion:	The functional test should include specific tests in order to ensure that data are always stored correctly in case of a battery-forced shut down.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.15 [REACTION-415] Each person MAY only perform actions permitted by her role. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Interfaces with HIS/EPR, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-99	Authorisation: Stakeholders must be a...	In Progress
	depends	REACTION-100	Access control: Access to sensitive i...	In Progress
	is depended by	REACTION-168	Remote Patient Monitoring (RPM)	In Progress
	is depended by	REACTION-95	Accountability: Stakeholders should b...	In Progress
	is depended by	REACTION-63	Security and privacy related to patie...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Before a requested action is performed, a control mechanism has to check whether the requested action is part of the requester's set of permissible actions according to its role.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of a control mechanism which decides whether a requested action may be granted or denied according to the requester's role.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.16 [REACTION-414] Communication between the Reaction Hosting Client and the Reaction Device Hosting Server MUST be authentic (entity authentication), with integrity, and confidential.

Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Communication, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-168	Remote Patient Monitoring (RPM)	In Progress
	Incorporate			
	incorporates	REACTION-90	Identifiability: Recipients and sende...	In Progress
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	It must be assumed that data transmission from the Reaction Hosting Client to the Reaction Device Hosting Server and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it MUST be ensured that the communication channel is authentic, with integrity, and confidential.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide communication channels with authenticity, integrity, and confidentiality.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.17 [REACTION-412] It MUST be possible to revoke a consent - data already stored MUST NOT be processed any further. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-145	The user must consent to the collecti...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7, WP9			
Rationale:	A patient must have the option to decide whether personal data is processed or not at any time. If the patient once gave her consent it must still be possible for the patient to revoke her consent, which means that any further processing of the affected data is forbidden. Also, if a patient revoked her consent the existing data may not necessarily be deleted, however, it MUST be excluded from any further processing.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms and procedures to enable consent revocation.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.18 [REACTION-407] If data was not transmitted for a lack of consent, the patient or her doctor (in case of a client without display and input capabilities) MUST be notified, e.g., through some pop-up or a notice in some message field. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Interfaces with HIS/EPR, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**		
	depends	REACTION-102	Notice: Natural persons should be not... Open
Requirement Type:	Non-functional - Legal		
Work package:	WP7, WP9		
Rationale:	Privacy laws require that data subjects have to consent to the transmission and processing of their data. If a new data item is to be transferred which was not foreseen in the initial consent, the subject has to give a 'new' consent before the new data item can be transferred and subsequently processed. If the subject's AHD has a display and input capabilities, the AHD may directly ask the subject for a new consent -- of course, the subject may also decline the request. If the AHD is an appliance without display, the transmission must include some kind of notice to inform the requesting party, usually the patient's doctor, that some data item was not transmitted and that the subject should be asked for an extended consent.		
Source/Originator:	FHG SIT		
Fit Criterion:	A notification mechanism for insufficient consents must be established for AHDs with and without display.		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		

11.1.19 [REACTION-405] Authentication and integrity of transmitted measurements MUST be ensured. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	PAN/BAN, Portable Devices, Security, Sensors

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP3, WP7
Rationale:	Without any data authentication, any measurement might be sent to the AHD without the AHD being able to distinguish between measurements from associated sensors and others. Also, if the measurements could be undetectably changed during transport, intentionally or unintentionally, this may have ill-effects on the patient's health because she may receive the wrong treatment due to 'false' measurements.
Source/Originator:	FHG SIT
Fit Criterion:	Mechanisms to ensure data integrity and entity authentication MUST be used for communication between sensors and AHDs.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.20 [REACTION-403] Each entity in the Reaction platform MUST be representable by a digital identity. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-259	Automated patient identification	Open
	is depended by	REACTION-63	Security and privacy related to patie...	In Progress
	is depended by	REACTION-95	Accountability: Stakeholders should b...	In Progress
	is depended by	REACTION-100	Access control: Access to sensitive i...	In Progress
	Incorporate			
	incorporates	REACTION-90	Identifiability: Recipients and sende...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	In the Reaction platform, entities must be uniquely identifiable and recognisable in order to allow repeated communication, referrals, accountability of actions, exclusion of ill-behaving entities, etc.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of a digital identity mechanism.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.21 [REACTION-400] Data/messages exchanged between the Reaction Device Hosting Server and the EPR/EHR System SHOULD be authentic (message authentication), with integrity, and confidential. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Interfaces with HIS/EPR, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**			
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
	is incorporated by	REACTION-91	Authenticity: Processors of informati...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	The security of messages transferred between the Reaction Device Hosting Server and the EPR/EHR System must be ensured even after the message was received - this is true even if the message was received over a secure communication channel. To guarantee this, the messages themselves MUST be self-contained with respect to authenticity, integrity, and confidentiality.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide data authenticity, integrity, and confidentiality			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.22 [REACTION-398] If a consent was given, the patient's involvement in the decision MUST be verifiable by the Reaction Hosting Client, especially if the consent was given remotely, e.g., at the doctor's surgery. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP7, WP9
Rationale:	Consents must be expressed by the data subject such that a third party, e.g., an AHD, can verify that the consent was actually given by the data subject herself -- this is especially relevant when the consent was given at the doctor's surgery and afterwards pushed back to the patient's AHD. Otherwise, anyone could produce a 'suitable' consent in the data subject's name.
Source/Originator:	FHG SIT
Fit Criterion:	Genuineness of a consent can be verified.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.23 [REACTION-387] Information related to informed consent stored in the platform Created: 23/Jul/10 Updated: 24/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Data Management, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-198	Information related to informed conse...	Open
Requirement Type:	Functional - REACTION platform			
Work package:	WP4			
Rationale:	An ethical approved declaration of informed consent has to be signed (either digitally or in paper form) by patients before they can be enrolled in the REACTION platform.			
Source/Originator:	D2.1 and workshops			
Fit Criterion:	The enrolment procedure shall allow the storage of the digitally signed informed consent or of a scanned copy of the signed paper This procedure shall be completed before any other operation can be performed.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.24 [REACTION-385] Digital identities for the Reaction platform MUST only be issued or revoked by trusted (third) parties, e.g., a certification authority (CA). Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-103	Data reduction and data economy: Pers...	Open
	is depended by	REACTION-259	Automated patient identification	Open
	is depended by	REACTION-90	Identifiability: Recipients and sende...	In Progress
	is depended by	REACTION-95	Accountability: Stakeholders should b...	In Progress
	is depended by	REACTION-152	Patient recruitment (or enrolment)	In Progress
	Incorporate			
	incorporates	REACTION-196	End of process for the diabetic patie...	Open
	incorporates	REACTION-104	Need-to-know Basis: Stakeholders proc...	Part of specification
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Without a trusted party (TP), anyone could produce its own digital identity and someone relying on such an identity would have to trust that the claimed identity is genuine. By incorporating a TP, relying parties trust that the TP ensures that its issued digital identities are genuine. This makes life easier for relying parties as they only have to establish a single trust relationship (with the TP) as opposed to having a multitude of trust relationships with others. The same goes for parties that had been excluded from the Reaction platform, as each relying party would have to determine by itself if another party is still part of the Reaction platform or not. In case of a trusted party, the relying part could simply query the TP if some identity is still valid or had been revoked, e.g., because its owner left the platform.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of a party which is trusted to orderly issue and revoke digital identities.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.25 [REACTION-382] Privacy enhancing technology Created: 23/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Backend Middleware, Communication, Networking, PAN/BAN, Security

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP4, WP7
Rationale:	Protect the privacy of users personally identifiable information (PII) and further more personal data.
Source/Originator:	FORTH-ICS & FORTHNET internal focus group
Fit Criterion:	Each measurement in each transmission channel shall be separated from the patient data and association between measurements and patient shall not be possible for whoever can intercept the measurements.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	Neutral Unhappiness

11.1.26 [REACTION-376] Integrity check for the stored data Created: 22/Jul/10 Updated: 19/Oct/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matts Ahlsen

Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-39	Platform Integrity (integrity checks ...	Open
	depends	REACTION-43	Protection against data loss System m...	Open
Requirement Type:	Non-functional - Security			
Work package:	WP4			
Rationale:	To guarantee the integrity of the stored data in the case of an unwanted happening.			
Source/Originator:	DoW			
Fit Criterion:	Use of adequate methods like e.g. Hash keys or redundancy codes for the data stored.			
Customer Satisfaction:	Very Pleased			
Customer Dissatisfaction:	Neutral Unhappiness			

Comments

Comment by Stephan Spat [13/Aug/10 9:41 AM]

main requirement subtype: Data storage

11.1.27 [REACTION-373] Data MUST NOT be processed at the Reaction Device Hosting Server if no consent is available and verifiable. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-198	Information related to informed conse...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7, WP9			
Rationale:	If patient data is to be processed at the REACTION Device Hosting Server, the server's provider must take the necessary steps to ensure that such a processing is permitted by the patient.			
Source/Originator:	FHG SIT			
Fit Criterion:	A 'watchdog' component must be in place that supervises the processing of patient data and takes action if data to be processed is not covered by the patient's consent.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.28 [REACTION-370] A consent MUST NOT be considered valid if the patient was not involved in the decision. Created: 20/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-145	The user must consent to the collecti...	Open
Requirement Type:	Non-functional - Legal			

Work package:	WP7, WP9
Rationale:	If it cannot be verified that a consent was produced by or with the help of the affected data subject the 'expressed will' of the data subject is doubtful. Hence, no processing should be done as it is unclear that the data subject allowed it.
Source/Originator:	FHG SIT
Fit Criterion:	A mechanism is available that allows to verify (or infer) that a given consent was the data subject's own decision.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.29 [REACTION-354] Data/messages exchanged between the Reaction Host Client and the Reaction Device Hosting Server MUST be authentic (message authentication), with integrity, and confidential. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**			
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
	is incorporated by	REACTION-91	Authenticity: Processors of informati...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	The security of messages transferred between the Reaction Host Client and the Reaction Device Hosting Server must be ensured even _after_ the message was received - this is true even if the message was received over a secure communication channel. To guarantee this, the messages themselves MUST be self-contained with respect to authenticity, integrity, and confidentiality.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide data authenticity, integrity, and confidentiality			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.30 [REACTION-343] Every person represented in the Reaction platform MUST be assigned to one or more roles. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Context Management, Interfaces with HIS/EPR, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-100	Access control: Access to sensitive i...	In Progress
	is depended by	REACTION-197	Care spaces in the primary care envir...	Open
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	In order to interact with the Reaction platform, persons need certain rights. As rights are associated with roles, persons MUST have at least one role to interact with the Reaction platform.			
Source/Originator:	FHG SIT			
Fit Criterion:	Each person is assigned to at least one role.			

Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.31 [REACTION-341] Roles MUST be defined for stakeholders of the Reaction platform, e.g., doctor, nurse, patient, informal carer, administrative personnel etc. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Interfaces with HIS/EPR, Portable User Interface, Security, Sensors, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-100	Access control: Access to sensitive i...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Each person in the Reaction platform has the right to perform a certain set of actions. In order to simplify the administration of these rights, each person is assigned to a role and roles are assigned to permissible actions. The advantage of this approach is that it is easier to manage the rights of a role than managing individual rights for each person.			
Source/Originator:	FHG SIT			
Fit Criterion:	Roles are defined for every actor from the Reaction use cases.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.32 [REACTION-339] Communication between the Reaction Device Hosting Server and the patient's/GP's web browser MUST be authentic (entity authentication), with integrity, and confidential. Created: 21/Jul/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-168	Remote Patient Monitoring (RPM)	In Progress
	Incorporate			
	incorporates	REACTION-90	Identifiability: Recipients and sende...	In Progress
	incorporates	REACTION-93	Confidentiality: Sensitive informatio...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	It must be assumed that data transmission from the Reaction Device Hosting Server to the patient's/GP's web browser and vice versa takes place over an insecure channel, i.e., data might be overheard or tampered with. Since personal data is to be transmitted it MUST be ensured that the communication channel is authentic, with integrity, and confidential.			
Source/Originator:	FHG SIT			
Fit Criterion:	Availability of mechanisms to provide communication channels with authenticity, integrity, and confidentiality.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.33 [REACTION-338] All data entered must be checked for format, consistency and validity

Created: 22/Jul/10 Updated: 24/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Architecture, Backend Middleware, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Franco Chiarugi
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-44	Protection against unintended user ac...	In Progress
Requirement Type:	Non-functional - Security			
Work package:	WP4			
Rationale:	Unintended user actions should not harm data integrity and the overall functioning of the platform. In case of doubt, the user must be warned and asked how to proceed. The user must be able to correct mistakes easily.			
Source/Originator:	DoW			
Fit Criterion:	The functional test should include specific tests in order to verify such circumstances.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.34 [REACTION-325] The possibility to manage user accounts by user name and password and secure log in and log out Created: 15/Aug/11 Updated: 16/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Data Management, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matts Ahlsen	**Assignee:**	Chorleywood Health Centre
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP2
Rationale:	Administrator of the system shall have full ability to reset user name and password of users, Add , Delete and Edit user accounts. The users shall be added to the system by their name and their role (user type) and also the ability to suspend and reactivate the user's account.
Source/Originator:	CHC workshop
Fit Criterion:	The system shall differ between active and suspended user accounts. Active users shall be displayed both with colour indicator and as a list function.
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Neutral Unhappiness

11.1.35 [REACTION-324] Providing a secure log in and log out for the user Created: 15/Aug/11 Updated: 16/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matts Ahlsen	**Assignee:**	Chorleywood Health Centre
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP2
Rationale:	The system shall be protected with a secure login for each user on the web portal, users shall be required to log out upon the end of the task. The system shall have a clear hierarchy for different type of users (Patient, Clinic, etc) and each user logging into the system shall be logged into the correct user type.
Source/Originator:	Chorleywood , Primary Care , D2-6.
Fit Criterion:	The system shall automatically log out the user when being dormant longer then a predefined time. The system shall be validated according to the predefined test plan.
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Neutral Unhappiness

11.1.36 [REACTION-323] Providing a complete audit trail for each user's data and action taken on the system Created: 15/Aug/11 Updated: 27/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Data Management, Portable User Interface, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matts Ahlsen	**Assignee:**	Chorleywood Health Centre

Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - Primary care pilot application
Work package:	WP2
Rationale:	There must be a complete audit trail of all actions taken in the system by any user. No user shall have the permission to permanently delete data from the system. This refers to the system logging and all actions taken by different users. The system shall also provide traceability of each action to the user taken those actions.
Source/Originator:	Chorleywood Health Centre workshop.
Fit Criterion:	The system shall foresee the possibility of traceability for each action which has been taken in the system by the user.
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Neutral Unhappiness

11.1.37 [REACTION-259] Automated patient identification Created: 21/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-403	Each entity in the Reaction platform ...	Open
	depends	REACTION-385	Digital identities for the Reaction p...	Open
	Incorporate			
	is incorporated by	GMSIP-12	Automated on-side patient identificat...	Open

Requirement Type:	Functional - In-hospital pilot application
Work package:	WP7
Rationale:	Automated patient identification to avoid identification mistakes. Risks of wrong patient identification have to be negligible. The REACTION identification system must be flexible enough to integrate existing identification methods employed on site, e.g., wards in a hospital.
Source/Originator:	D2.1 and workshops
Fit Criterion:	An effective, proper and easy-to-use way for automated patient identification, when mobile device is close to the patient (RFID, NFC?) has to be present. For example, each patient might wear wristband with a barcode which identifies the patient. This is standard in many hospitals and in some wards of the inpatient clinical site these wristbands are in use. This way shall reduce errors in patient identification and speed-up the patient management.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness
Dependencies:	

11.1.38 [REACTION-249] Regular backup of data Created: 21/Jun/10 Updated: 03/Nov/11 Resolved: 19/Jul/11

Status:	Resolved
Project:	REACTION requirements
Component/s:	Architecture, Data Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Franco Chiarugi
Resolution:	Duplicate	**Votes:**	0

Issue Links:	**Incorporate**			
	is incorporated by	GMSIP-72	Regular backup of system data.	Open

Requirement Type:	Functional - In-hospital pilot application
Work package:	WP4, WP8, WP10
Rationale:	Information shall be available even in case of a power failure, system breakdown or network unavailability through regular backup of data
Source/Originator:	D2.1 and workshops
Fit Criterion:	The field trials in the Inpatient environment shall foresee regular backup of data and restore procedures in order to face properly situations of sudden system breakdown or malfunctions.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness
Dependencies:	REACTION-156

11.1.39 [REACTION-198] Information related to informed consent have to be stored in the REACTION platform Created: 17/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Data Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-387	Information related to informed conse...	Open
	is depended by	REACTION-373	Data MUST NOT be processed at the Rea...	Open
Requirement Type:	Functional - REACTION platform			
Work package:	WP7, WP4, WP9			
Rationale:	An ethical approved informed consent has to be signed (either digitally or in paper form) by patients before they can be enrolled in the REACTION platform.			
Source/Originator:	D2.1 and workshops			
Fit Criterion:	The enrolment procedure shall allow the storage of the digitally signed informed consent or of a scanned copy of the paper form signed informed consent and this procedure shall be completed before any other operation can be performed.			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.40 [REACTION-197] Care spaces in the primary care environment Created: 17/Jun/10 Updated: 24/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Communication, Data Management, Interfaces with HIS/EPR, Ontology/Terminology, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-343	Every person represented in the React...	Open
	is depended by	REACTION-436	Care space in outpatient environment	Part of specification
Requirement Type:	Functional - Primary care pilot application			
Work package:	WP4, WP5, WP7, WP8, WP10			
Rationale:	Patients and informal carers have to be included in the process of care. Care spaces (for each patient) have to be developed where the roles and tasks are distributed among the multidisciplinary health care team members. The patients have to be provided with their own self management tasks in an ongoing			

	relationship with the other members of the team. Only people registered in the patient care space can access the patient data (clinical and demographic).
Source/Originator:	D2.1 and workshops
Fit Criterion:	Each member of the care space will have specific roles and tasks in the patient's care.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.41 [REACTION-176] Automated identification of patients while recording data for inpatient glucose control Created: 16/Jun/10 Updated: 27/Nov/11 Resolved: 20/Jul/11

Status:	Resolved
Project:	REACTION requirements
Component/s:	Architecture, Backend Middleware, Communication, Context Management, Interfaces with HIS/EPR, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Peter Beck	**Assignee:**	Matthias Enzmann
Resolution:	Duplicate	**Votes:**	0

Issue Links:	**Incorporate**			
	is incorporated by	GMSIP-12	Automated on-side patient identificat...	Open
Requirement Type:	Functional - In-hospital pilot application			
Work package:	WP4			
Rationale:	Automated identification of patients while recording data for inpatient glucose control (e.g. RFID)			
Source/Originator:	D 2.61 (p.62/63)/MSG			
Fit Criterion:	Automated patient identification			
Customer Satisfaction:	Very Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			
Dependencies:	REACTION-259			

11.1.42 [REACTION-159] Logging mechanisms Created: 16/Jun/10 Updated: 27/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Architecture, Backend Middleware, Communication, Context Management, Data Management, Risk Assessment, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Peter Beck	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - REACTION platform
Work package:	WP4
Rationale:	Using logging from all components within Health Status Profile it's easier to integrate and control the system.
Source/Originator:	FORTH
Fit Criterion:	A logging mechanism is implemented in the REACTION platform
Customer Satisfaction:	Pleased
Customer Dissatisfaction:	Neutral Unhappiness

11.1.43 [REACTION-155] Electronic paperless data record Created: 16/Jun/10 Updated: 21/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Architecture, Context Management, Data Management, Interfaces with HIS/EPR, Networking, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Peter Beck	**Assignee:**	Peter Beck
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Functional - In-hospital pilot application
Work package:	WP4
Rationale:	Currently all actions are recorded on a paper chart/record. Because of data privacy protection and safety issues this record must not stay at the patient's bed but will be stored centrally. The staff (nurse/physician) has to look for the patient record every time before he/she goes to the patient. This means that the information is only available for one person at the same time (i.e. if the nurse is at the patient with the record the physician- who may be in a different room- has no access to the data in order to discuss it with colleagues)
Source/Originator:	D2.1 (p.62)/MSG
Fit Criterion:	The inpatient pilot application stores data records/charts
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	High Unhappiness

11.1.44 [REACTION-145] The user must consent to the collection of personal data whenever possible Created: 15/Jun/10 Updated: 20/Oct/11

Status:	Open
Project:	REACTION requirements
Component/s:	Data Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Eugenio Mantovani	**Assignee:**	Eugenio Mantovani
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-429	Before transmitting any personal data...	Open
	is depended by	REACTION-370	A consent MUST NOT be considered vali...	Open
	is depended by	REACTION-412	It MUST be possible to revoke a conse...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7, WP9			
Rationale:	The user is taken to be an autonomous individual who, in principle, decides what personal data to disclose and to whom. Of course this is not an absolute right, because legal obligations such as the law, contractual obligations, but also consequences of the performance of a contract, may overrule the right for the individual to withhold consent. Consent contributes to the realisation of a number of fundamental human values founding modern (western) societies, such as individuality, autonomy, dignity and civility.			
Source/Originator:	DOW			
Fit Criterion:	The fact that consent is instrumental to a number of fundamental values, means that it has to be revocable when it turns out that the effects of the previously given consent are different than the user may have expected given the available information at the time. Consent requires the user to be able to: • give informed agreement to the collection and processing of personal data • give explicit permission to the entity collecting the personal data to perform the servcies contracted for • give specific, unambiguous agreement to the collection and processing of sensitive data • give special consent when data will not be editable • agree to the automatic collection and processing of (personal) data (the main reasons for which this requirement has been inserted) Questions to be asked: Does the application offer the user ways to provide explicit consent to (personal) data disclosure? Does the application offer the user ways to provide explicit permission to use certain data for performing			

	the service contracted for? Does the application offer ways to treat sensitive personal data different from the way it treats other personal data? Does the application provide special warnings when data is not editable after disclosure? Does the application offer ways for the user to explicitly agree to the automatic collection and processing of (personal) data Does the application offer ways to revoke previously given consent?
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.45 [REACTION-140] The platform shall prevent incorrect data from being introduced Created: 15/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Data Management, Interfaces with HIS/EPR, Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Franco Chiarugi
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP7, WP10
Rationale:	Incorrect data might hamper a correct clinical decision
Source/Originator:	DoW and workshops
Fit Criterion:	Check that the user interface and specific procedures protect the end-user from the introduction of incorrect data as much as possible
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness

11.1.46 [REACTION-118] Assurance: the architecture and its implementation must provide assurance that it delivers the security and compliance properties it promises Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Legal
Work package:	WP7
Rationale:	If allegedly secure functions do not live up to their expected functionality, the whole platform could be compromised.
Source/Originator:	DoW/ATOS
Fit Criterion:	Successful review of expected security functionality.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.47 [REACTION-116] Availability of security mechanisms to manage sensitive data Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Maintainability and portability
Work package:	WP7
Rationale:	In REACTION, we are dealing with sensitive data, thus security must be available on all platforms.
Source/Originator:	DoW/SIT
Fit Criterion:	Security mechanisms are available for all target platforms of REACTION.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness

11.1.48 [REACTION-115] Transparency: Security configuration should be hidden from the user as far as possible Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Usability
Work package:	WP7
Rationale:	Users usually do not have the expertise to choose the 'right' security options.
Source/Originator:	DoW/SIT
Fit Criterion:	No, or as few as possible, additional user interactions for security.
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	High Unhappiness

11.1.49 [REACTION-114] Modularity: the system has to be divided into components Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Maintainability and portability
Work package:	WP7
Rationale:	It is easier to implement, exchange, and integrate the modules.
Source/Originator:	DoW/ATOS

Fit Criterion:	REACTION platform should be modular
Customer Satisfaction:	Uninterested
Customer Dissatisfaction:	Neutral Unhappiness

11.1.50 [REACTION-109] Scalability: the security must not materially impact the performance of the system Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Performance
Work package:	WP7
Rationale:	the security resources have to scale well with the overall architecture
Source/Originator:	DoW/ATOS
Fit Criterion:	Security does not significantly impact overall latency of the system
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.51 [REACTION-104] Need-to-know Basis: Stakeholders processing information should only learn what is necessary to carry out their specific task Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Part of specification
Project:	REACTION requirements
Component/s:	Architecture, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**			
	is incorporated by	REACTION-385	Digital identities for the Reaction p...	Open
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	In an information processing chain, several stakeholders might be involved but it might not be necessary for every stakeholder to know which exact data another stakeholder has processed			
Source/Originator:	DoW/SIT			
Fit Criterion:	Process design takes into account the need-to-know principle			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.52 [REACTION-103] Data reduction and data economy: Personal data shall be collected, processed and used as little as possible. Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major

Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-385	Digital identities for the Reaction p...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7			
Rationale:	Handling personal data has to conform to privacy laws. In particular, personal data shall be rendered anonymous or pseudonymous as allowed by the purpose for which they are collected and/or further processed or used. This (might be/) is in conflict with unnecessary collection of personal data, which are not required to fulfil a specific task.			
Source/Originator:	DoW/SIT			
Fit Criterion:	Processes are designed such that personal data are only collected when necessary and anonymisation/pseudonymisation techniques are employed whenever possible			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.53 [REACTION-102] Notice: Natural persons should be notified when, how, and to what extent their personal data are communicated to others Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Context Management, Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-429	Before transmitting any personal data...	Open
	is depended by	REACTION-407	If data was not transmitted for a lac...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7			
Rationale:	Handling of personal data has to conform to privacy laws			
Source/Originator:	DoW/SIT			
Fit Criterion:	Process design takes into account the fair-processing principle			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.54 [REACTION-100] Access control: Access to sensitive information should only by given to authorised personnel Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-403	Each entity in the Reaction platform ...	Open
	is depended by	REACTION-341	Roles MUST be defined for stakeholder...	Open
	is depended by	REACTION-343	Every person represented in the React...	Open
	is depended by	REACTION-437	Each role MUST be assigned to a set o...	Open

	is depended by	REACTION-415	Each person MAY only perform actions ...	Open
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Sharing patient data is necessary in health care to treat patients but access should only be given to persons involved in the treatment			
Source/Originator:	DoW/SIT			
Fit Criterion:	Availability of a mechanism allowing to control access to sensitive data			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			
Dependencies:				

11.1.55 [REACTION-99] Authorisation: Stakeholders must be authorised before they are allowed to perform relevant actions Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-429	Before transmitting any personal data...	Open
	is depended by	REACTION-415	Each person MAY only perform actions ...	Open
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Certain actions are not permitted for everybody but may only be carried out by authorised personnel			
Source/Originator:	DoW/SIT			
Fit Criterion:	Availability of a procedure or mechanism allowing to authorise relevant actions			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.56 [REACTION-95] Accountability: Stakeholders should be held accountable for relevant actions Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-415	Each person MAY only perform actions ...	Open
	depends	REACTION-403	Each entity in the Reaction platform ...	Open
	depends	REACTION-385	Digital identities for the Reaction p...	Open
Requirement Type:	Non-functional - Legal			
Work package:	WP7			
Rationale:	Certain actions or decisions will have an impact on the person making the decision or on the person affected by it, thus it should be clear, e.g., who made the decision, what kind of decision was made, and when was it made			

Source/Originator:	DoW/SIT
Fit Criterion:	Availability of a procedure or mechanism allowing to review relevant actions of stakeholders
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.57 [REACTION-94] Availability: Patient data and other resources must be available to ensure proper treatment Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Antonis Miliarakis
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP7, WP5
Rationale:	Non-availability of patient data will hamper further treatment and might even impair the patient's health
Source/Originator:	DoW/SIT
Fit Criterion:	REACTION platform should remain operational in case of failures
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.58 [REACTION-93] Confidentiality: Sensitive information must not be readable by unauthorised persons Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**		
	is incorporated by	REACTION-414 Communication between the Reaction Ho...	Open
	is incorporated by	REACTION-354 Data/messages exchanged between the R...	Open
	is incorporated by	REACTION-400 Data/messages exchanged between the R...	Open
	is incorporated by	REACTION-431 Data/messages exchanged between the R...	Open
	is incorporated by	REACTION-438 Communication between the Reaction De...	Open
	is incorporated by	REACTION-339 Communication between the Reaction De...	Open
	is incorporated by	REACTION-452 Communication between the Reaction De...	Part of specification
Requirement Type:	Non-functional - Security		
Work package:	WP4, WP7		
Rationale:	Various stakeholders exchange information over the REACTION platform which, without any safeguards, would allow third parties to learn sensitive information of patients		
Source/Originator:	DoW/SIT		
Fit Criterion:	Availability of a mechanism for ensuring data confidentiality		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		
Dependencies:			

11.1.59 [REACTION-92] Integrity: Information, in particular health data, must be protected from any kind of unintended changes during transport Created: 14/Jun/10 Updated: 25/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security, Sensors

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**		
	is incorporated by	REACTION-452 Communication between the Reaction De...	Part of specification
Requirement Type:	Non-functional - Security		
Work package:	WP7		
Rationale:	Any kind of undetectable changes in patient's data may give rise to wrong treatment and harm patients		
Source/Originator:	DoW/SIT		
Fit Criterion:	Availability of a mechanism for ensuring data integrity		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		

11.1.60 [REACTION-91] Authenticity: Processors of information should be able to determine whether the data being processed is authentic Created: 14/Jun/10 Updated: 25/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Incorporate**		
	incorporates	REACTION-354 Data/messages exchanged between the R...	Open
	incorporates	REACTION-400 Data/messages exchanged between the R...	Open
	incorporates	REACTION-431 Data/messages exchanged between the R...	Open
	is incorporated by	REACTION-452 Communication between the Reaction De...	Part of specification
Requirement Type:	Non-functional - Security		
Work package:	WP7		
Rationale:	Medical personnel should know if information relating to their patient originates from a known/trusted source, e.g., the patient's blood glucose sensor or medical personnel, in order to assess the data's quality		
Source/Originator:	DoW/SIT		
Fit Criterion:	Availability of a mechanism that allows to verify the authenticity of some information		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		

11.1.61 [REACTION-90] Identifiability: Recipients and senders of information must be identifiable, though not necessarily personally identifiable Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Matthias Enzmann	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	depends	REACTION-385	Digital identities for the Reaction p...	Open
	Incorporate			
	is incorporated by	REACTION-414	Communication between the Reaction Ho...	Open
	is incorporated by	REACTION-438	Communication between the Reaction De...	Open
	is incorporated by	REACTION-339	Communication between the Reaction De...	Open
	is incorporated by	REACTION-403	Each entity in the Reaction platform ...	Open
	is incorporated by	REACTION-452	Communication between the Reaction De...	Part of specification
Requirement Type:	Non-functional - Security			
Work package:	WP7			
Rationale:	Reports/measurements must be assignable to the 'right' patient file/device			
Source/Originator:	DoW/SIT			
Fit Criterion:	Recipients and senders must have unique identifiers			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.62 [REACTION-63] Security and privacy related to patient data Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major	
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann	
Resolution:	Unresolved	**Votes:**	0	

Issue Links:	**Depend**			
	depends	REACTION-415	Each person MAY only perform actions ...	Open
	depends	REACTION-403	Each entity in the Reaction platform ...	Open
Requirement Type:	Functional - REACTION platform			
Work package:	WP7, WP10			
Rationale:	Privacy concerns are of utmost importance. The patient data should be transfer and maintained in a secure way while any access to them should be monitored and logged (getting advantage of a login mechanism available in the applications).			
Source/Originator:	DoW & Technical meeting in London			
Fit Criterion:	Verify that any access to patient data is logged and is performed in a secure way			
Customer Satisfaction:	Very Pleased			
Customer Dissatisfaction:	High Unhappiness			
Conflicts:	REACTION-103			

11.1.63 [REACTION-58] User authentication and Security Created: 14/Jun/10 Updated: 19/Jul/11 Resolved: 19/Jul/11

Status:	Resolved
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Major
Reporter:	Franco Chiarugi	**Assignee:**	Franco Chiarugi
Resolution:	Duplicate	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP10
Rationale:	Each user of the whole system should have access only to the components that are related to his work. Also thre should be different level of access to the functionality within the components based on his role
Source/Originator:	DoW
Fit Criterion:	No user can view or edit data that are not required for his work.
Customer Satisfaction:	Very Pleased
Customer Dissatisfaction:	High Unhappiness
Dependencies:	REACTION-93, REACTION-99, REACTION-100

11.1.64 [REACTION-45] Protection against threats Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matthias Enzmann
Resolution:	Unresolved	**Votes:**	0

Requirement Type:	Non-functional - Security
Work package:	WP7, WP10
Rationale:	Medical data are sensible data and protection against threats and and unauthorized access should be provided. The system must protect against: *Unauthorized persons obtaining manager rights through the internet (hacking). *Unauthorized persons getting access to personal data. *The system must conform to Law on Handling of Personal Data.
Source/Originator:	DoW
Fit Criterion:	The functional test should include specific tests in order to verify such circumstances
Customer Satisfaction:	Extremely Pleased
Customer Dissatisfaction:	Extreme Unhappiness

11.1.65 [REACTION-44] Protection against unintended user actions Created: 14/Jun/10 Updated: 21/Nov/11

Status:	In Progress
Project:	REACTION requirements
Component/s:	Portable User Interface, Security, Web User Interface

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Franco Chiarugi
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**		
	is depended by	REACTION-338	All data entered must be checked for ... In Progress
Requirement Type:	Non-functional - Security		
Work package:	WP4, WP7, WP10		
Rationale:	Unintended user actions should not harm data integrity and the overall functioning of the platform. Unintended user actions may not cause the system to close down, neither on the client nor on the server. All data entered must be checked for format, consistency and validity. In case of doubt, the user must be warned and asked what to do. The user must be able to correct mistakes easily. The user must be able to interrupt long functions (e.g. waiting for a remote data transfer).		
Source/Originator:	DoW		
Fit Criterion:	The functional test should include specific tests in order to verify such circumstances		
Customer Satisfaction:	Extremely Pleased		
Customer Dissatisfaction:	Extreme Unhappiness		

11.1.66 [REACTION-43] Protection against data loss System must protect against: *Loss or replication of data transferred between two systems; *Concurrency problems; *Disk crash; *Protection against physical means. Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Security

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-376	Integrity check for the stored data	Part of specification
Requirement Type:	Non-functional - Security			
Work package:	WP4, WP7			
Rationale:	Data integrity has to be guaranteed. *Loss or replication of data transferred between two systems (e.g. system shutdown); *Concurrency problems (e.g. 2 doctors interact with the system simutaneously and prescribe different medicines, which one will the system pick?); *Disk crash (e.g. solution could be periodic backup or RAID); *Protection against physical means (e.g. solution could be remote backup)			
Source/Originator:	DoW			
Fit Criterion:	The functional test should include specific tests in order to verify such circumstances			
Customer Satisfaction:	Extremely Pleased			
Customer Dissatisfaction:	Extreme Unhappiness			

11.1.67 [REACTION-39] Platform Integrity (integrity checks for the stored data) Created: 14/Jun/10 Updated: 21/Nov/11

Status:	Open
Project:	REACTION requirements
Component/s:	Data Management, Security

Type:	Volere Requirement	**Priority:**	Critical
Reporter:	Franco Chiarugi	**Assignee:**	Matts Ahlsen
Resolution:	Unresolved	**Votes:**	0

Issue Links:	**Depend**			
	is depended by	REACTION-376	Integrity check for the stored data	Part of specification
Requirement Type:	Non-functional - Security			
Work package:	WP4, WP7, WP10			
Rationale:	To guarantee the integrity of the stored data in the case of an unwanted happening.			
Source/Originator:	DoW			
Fit Criterion:	Use of adequate methods like e.g. Hash keys or redundancy codes for the data stored.			
Customer Satisfaction:	Very Pleased			
Customer Dissatisfaction:	Neutral Unhappiness			