Project # FP7-ICT-StrokeBack-288692

Title of the deliverable:

PHR Design and Architecture

Deliverable No.		**D5.1**	
WP No.	**5**	WP Title:	**Universal Patient Health Record (PHR) Platform & Rehabilitation Related Applications and Services**
Task No.	**1**	Task Title:	**Design and Architecture of the PHR System**
Lead authors (partner)		**Intracom Telecom (No: 4)**	
Co-authors (partner)		**<Names of co-developing organisation(s)>**	
Planned delivery:		**Month 6**	
Dissemination level: **PU** Public **PP** Restricted to other program participants **RE** Restricted to groups defined by consortium **CO** Confidential, for consortium members only		**PP**	
Status: (F: final; D: draft; RD: revised draft)		**F**	
File Name:		**PHR Design and Architecture v1.0.doc**	

Document version:	**1.0**
Project start date and duration	**1st October 2011 - 36 months**

Table of contents

List of Figures

DOCUMENT HISTORY

Version	Date	Comment
0.1	1/11/2011	TOC (ICOM)
0.2	21/12/2011	First Draft (ICOM)
0.3	20/03/2012	Second Draft (ICOM)
0.4	28/03/2012	Third Draft (ICOM)
0.5	29/03/2012	Fourth Draft (ICOM)
0.6	30/03/2012	Release Draft (ICOM)
1.0	06/06/2012	Final

Executive Summary

This deliverable provides an extended set of requirements, the full technical specifications of the proposed universal PHR System, the architecture decomposition into functional modules with definition of interfaces used among them and with external entities including protocol definition and applicable communication and programming standards used. The architecture presented here stands as reference architecture for the design of a universal PHR-S. On parallel the end user requirements collection and documentation runs within the context of Work Package 2. The outcome of this process will be used in the forthcoming future as a basis for fine tuning our architectural approach and making some tailored interventions, if necessary. Having said that, this document, although formally due for the end of M6 of the project should be considered as a live document for the first year of the project, which is actually dedicated to system design and specification.

The introductory section of this document is dedicated to the presentation of some relative definitions and mainly the scope of a Personal Health Record. Section 2 is dedicated to generic functional requirements related to a universal PHR-S. Finally, in Section 3 we present the StrokeBack PHR-S reference architecture.

List of abbreviations

Abbreviation	Explanation
ID	Identifier
PHR-S	Personal Health Record System
PHR	Personal Health Record
EHR	Electronic Health Record
EMR	Electronic Medical Record
ESP	External Service Provider
HL7	Health Level Seven
RMI	Remote Method Invocation
SQL	Script Query Language
WSDL	Web Service Definition Language

1 Introduction

1.1 Definitions

According to the NAHIT report [1] on defining key health information technology terms, the following definitions apply:

Electronic Medical Record (EMR): An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.

Electronic Health Record (EHR): An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.

Personal Health Record (PHR): An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

The most salient feature of the PHR, and the one that distinguishes it from the EMR and EHR, is that the information it contains is under the control of the individual. The concise definition above, names the individual as the source of control, but that leaves room for others acting in the individual's interest—their agent or agents—to have control over access to the PHR. An agent may be expressly designated by the individual but not in all cases; examples of an agent acting for an individual include parents acting for children, or, in the later stages of life, children acting for parents.

The individual is distinctively the guardian of information stored or accessible within a PHR. She decides what volumes of information to include, how they are maintained and ordered, and who can read them or "check them out." Standards and policy will need to determine if and how individuals can delete or modify information in a PHR that originated from an EHR and how these modifications are communicated to other providers with whom the data in the PHR are shared. Having control also means that an individual's PHR can exist independently of the entity that sponsors it—the PHR is portable. This requirement for portability excludes models in which sponsors such as health insurers or health care providers give individuals access to health-related information that is dependent on the individual remaining with that sponsor.

1.2 PHR scope

According to the NAHIT the long-term goal of a PHR is to be a lifelong resource of pertinent health information for an individual. Thus it should have both the depth and breadth of information to enable individuals to become more engaged in their own healthcare as they move from being passive recipients to active participants in their personal health management. The health information in a PHR can be drawn from a broad range of possible sources. Significant sources may include, but are not limited to:

- **Individuals**—Self-generated information for personal management or information for care providers, including information about allergies, prescribed medications, eating habits, exercise objectives, the progression of an illness or recovery from it, and preferences regarding care in various circumstances.

- **Health care providers**—Including hospitals, skilled nursing homes, long term care, and other facilities; pharmacies, lab, and diagnostic facilities reporting test results.
- **Health care clinicians**—Including physicians, nurses, behavioural health professionals, registered dieticians, chiropractors, and other licensed or certified care providers.
- **Medical devices**—Instruments, machines and implanted devices monitoring clinical indices, for immediate use as well as for historical purposes.
- **Wellness promoters**—Entities supplying services or information to generate and maintain good health, such as proactive medicine centres, fitness centres, rehabilitation experts, and complementary/ alternative medicine practitioners.
- **Health insurers**—Information arising from claims for insurance payments, disease management programs recommending certain actions and collecting results, updated information on drugs in a formulary, and other coverage policies specific to an individual.
- **Public health**—Government health departments, disease surveillance and immunization programs, school-based care providers and social workers, and nongovernmental organizations engaged in health and wellness.
- **Research institutions**—Information about opportunities to engage in clinical trials and studies, and recently published results of interest to the individual.

The sum of these and other inputs is a well-rounded picture comprising clinical information, administrative information, and wellness information for individuals to employ and impart to others at their discretion. In the PHR-S reference architecture presented below (paragraph 2.1) we use the term External Service Providers (ESPs) to generalize the above-mentioned entities.

1.3 The need for a novel PHR System

Within this paragraph we address the issue of why it is necessary to develop a new personal health record system and which is the target added value, compared to the existing ones. In order to answer to this question we first appose the view of the HL7 standards development organization, and more specifically of the HL7 PHR-S Working group [2].

First there is a distinction between a Patient Health Record and a Patient Health Record System: *the PHR is the underlying record that the software functionality of a PHR-System maintains*.

Then, with regards to the PHR-S it is mentioned that: *The overarching theme of a PHR-S involves a patient centric tool that is controlled for the most part, by the individual. It should be immediately available electronically,* ***and able to link to other systems, either in a "pull-push" or "push-pull" method****. The PHR-S is intended to provide functionality to help an individual maintain a longitudinal view of his or her health history, and may be comprised of information from a plethora of sources—i.e., from providers and health plans, as well as from the individual. Data collected by the system is administrative and/or clinical, and the tool may provide access to a wealth of forms (advance directives) and advice (diet, exercise, disease management).* ***A PHR-S would help the individual collect*** *behavioural health, public health, patient entered and patient accessed data (including medical monitoring devices), medication information,* ***care management plans and the like, and could be connected to providers, laboratories, pharmacies, nursing homes, hospitals and other institutions and clinical resources****. At its core, the PHR-S should provide the ability for the individual to capture and*

maintain demographic, insurance coverage, and provider information. It should also provide the ability to capture health history in the form of a health summary, problems, conditions, symptoms, allergies, medications, laboratory and other test results, immunizations and encounters. ***Additionally, personal care planning features such as advance directives and care plans should be available****.* ***The system must*** *be secure and have appropriate identity and access management capabilities, and* ***use standard nomenclature, coding and data exchange standards for consistency and interoperability****. A host of optional features have been addressed over the course of this initiative, including secure messaging, graphing for test results, patient education, guideline-based reminders, appointment scheduling and reminders, drug-drug interactions, formulary management, health care cost comparisons, document storage and clinical trial eligibility. The effective use of a PHR-S is a key point for improving healthcare in terms of self-management, patient-provider communication and quality outcomes*.

In the above quote we have highlighted those parts we consider as not being adequately covered by existing PHR-S solutions and therefore leave space for further R&D activities, to be pursued within the StrokeBack project. In principal, there are two dimensions highlighted there:

- **Integrated care management plans or integration with related third party systems**: Current PHR systems do not adequately support this need. Take for example Google Health[1] or Microsoft Health Vault: notwithstanding the fact that these products offer very attractive web interfaces for the patients to edit and store their personal record of health related information they lack of any functionality related to the lay out and maintenance of a rehabilitation plan. Typically, this need is covered by special purpose software solutions that are entirely clinicians-oriented and do not actively put the patients in the loop (i.e. not Personal Health Systems). In contrast, our approach is patient-centric: the intention of the project is to build a PHR-S that facilitates personal care planning. This does not mean that the clinicians are made subordinates in the rehabilitation process: the proposed PHR-S facilitates their tele-supervision, if granted such a right by the patients.
- **Standard nomenclature, coding and data exchange standards for consistency and interoperability**: The significance of these parameters is that they ensure human readability and machine processability of health related data. In HL7, the former is guaranteed by a Clinical Document Architecture (CDA) HL7 standard, while the latter is guaranteed by v2.x or v3 HL7 Messaging standard. HL7 CDA is an XML-based markup standard intended to specify the encoding, structure and semantics of clinical documents for exchange. The CDA specifies that the content of the document consist of a mandatory textual part (which ensures human interpretation of the document contents) and optional structured parts (for software processing). The structured part relies on coding systems (such as from SNOMED and LOINC) to represent concepts. The consortium is not aware of any PHR-S that claims full adoption of the HL7 CDA. For example, Google Health supports a subset of CCR [3], a competing standard to CDA, while Microsoft Health Vault claims to support a subset of CCR and CDA [4], but actually only for importing information from other systems, and not for exporting [5]. As for the underlying messaging scheme, to our knowledge, none of these PHR-S claim support of a widely used standard messaging scheme, such as those of HL7.

[1] Google has suspended this product

[2] The only limitation is the requirement for support of SQL commands

On top of the above one should add the need for a controllable, integrated, yet fully open ICT solution that ensures the smooth execution of the project trials. The accumulated experience indicates that while a significant amount of yet unmet ICT-related end-user related requirements arise whenever a new medical issue is examined within an R&D project, in most of the cases neither the legacy ICT systems in the trials sites are open and accessible nor the IT personnel easily accepts intervention and links to such systems. From this perspective, by embedding within the project ICT environment a novel, open PHR-S allows StrokeBack to deliver a self-contained ICT solution able to be deployed in both rich and virgin e-Health environments.

1.4 Deliverable scope

The bunch of PHR-S functional requirements that are presented within this paragraph comprise a synthesis of requirements that have been recorded in the international state of the art in Personal Health Record Systems and are relevant to the general objectives of StrokeBack, as described in the project's Technical Annex. It should be emphasized that these requirements are not the outcome of a formal requirements elicitation process that included the relevant project stakeholders, i.e. technical participants and PHR-S end users. Actually, this is a work to be carried out in the context of Work Package 2 (more specifically within the tasks *2.1: User Requirements and Design Specification* and *2.2: StrokeBack Architecture*). This work runs on parallel with Work Package 5 and its findings will be documented in *D2.1 User Needs and System Specification* (M6) and *D2.3 Design Guidelines and StrokeBack Architecture* (M12). While the intention of this document is to track the generic functional requirements related to a PHR-S the original requirements that spring from the StrokeBack Consortium will be documented within Work Package 2, where a correlation with the generic requirements documented in this deliverable will also be executed.

2 PHR-S Functional Requirements

The functions that are supported by a Personal Health Record-System (PHR-S) are those that enable an individual to manage information about his or her healthcare. These functions provide direction as to the individual's ability to interact with a Personal Health Record in such a way to individualize the record and maintain a current and accurate record of his or her healthcare activities. The functions include activities such as managing wellness, prevention and encounters. These functions are designed to encourage and allow an individual to participate actively in his/her healthcare and better access the resources that allow for self-education and monitoring [5]. The principal users of these functions are expected to be individuals referenced as account holders; the patient or subject of care and healthcare providers will have access to certain functions to view, update or make corrections to their Personal Health Record. The Account Holder will receive appropriate decision support, as well as support from the PHR-S to enable effective electronic communication between providers, and between the provider and the account holder or account holder's designated representative.

In the subsequent paragraphs we present functional requirements grouped in 7 different categories:

1. Management of historical clinical data
2. Management of personal observations & measurements
3. Management of care plans
4. Security aspects
5. Management of administrative issues
6. ESP related issues
7. Management of other resources

2.1 Historical clinical data management

The functions in the historical data management concern data gathered by clinicians or by the patient himself. In Table 1 a minimum set of data is presented in order to form a complete patient's medical history. The historical data should be constantly updated with new records by both parties. The clinicians accessing the historical data can have a thorough idea on a patient's medical status.

Functional requirement	Description
Identify and maintain a PHR	Unambiguously identify the account holder; correctly link the information with the account holder and vice-versa.
Manage historical clinical data and current health status data	Historical health information as well as current health status should be captured and maintained in the health record.
Manage patient originated data	Manage information sourced or input directly by the account holder.
Manage data & documentation from ESPs	Enable the PHR account holder to import and manage historical clinical information from external sources
Produce and present ad hoc views of the PHR	Support standard and customizable views of the PHR
Manage historical and current health status data	Capture and maintain the summary lists depicting the account holder's current medical status and history.
Manage problem lists	Manage the account holder's health problem list and provide

	the ability to manage the problem list over time.
Manage medication list	Manage the account holder's medication list.
Manage allergy, intolerance and adverse reaction list	Manage the PHR account holder's list of known allergens and adverse reactions with all pertinent information.
Manage immunization list	Manage the account holder's immunization data and associated capabilities including reminders, alerts, compliance, and administration.
Manage diagnoses history	Manage the account holder's history of diagnoses
Manage surgical history	Manage the account holder's history of surgical procedures.
Maintain family history	Manage the account holder's family health history.
Manage personal genetic information	Manage the account holder's genetic information.
Manage social history	Manage the account holder's social history including, health related habits and risk factors.
Capture genomic / proteomic data and documentation from ESPs	Incorporate genomic/proteomic data and documentation from external data sources.

Table 1: Management of historical clinical data within a PHR-S

2.2 Personal observations & measurements management

A patient should be able to feed the PHR-S with her own observations and gathered observations of daily living (ODLs). Patient's info should be available to clinicians as well (upon proper authorization by the patient). Personal observations and measurements will help the clinicians to have a detailed view of the patient's progress. Information gathered by this set of functions (Table 2) include measurements such as weight, systolic/diastolic pressure, questionnaires answered by the patient with questions about his daily activities, physical fitness, social support and quality of life.

Functional requirements	Description
Manage personal clinical measurements & observations of daily living	Provide the ability for the PHR Account Holder to enter personally sourced data and to make it available electronically to authorized Health Care Provider(s) or other Authorized Users or applications.
Manage Test Results	Manage results of diagnostic tests including inpatient, ambulatory and home monitoring tests.

Table 2: Management of personal observations & measurements within a PHR-S

2.3 Care plan management

A Care Plan is a set of actions provided by the clinician for the patients' benefit. The Care Plan supports the patient's therapy and is a part of the PHR-S. The Care Plan facilitates the patient to follow the clinician's guidelines, execute exercises, check for upcoming events such as visits or tests and manage their medications. A more detailed view of the Care Plan management is listed in Table 3.

Name	Statement/Description
Manage account holder implemented care plans	Assist the account holder to develop, manage, and follow his or her own care plans.
Manage provider implemented care plans	Enable the account holder to capture, record, and display account holder specific care plans received from authorized health care providers.
Manage medications	Assist the account holder to manage their individual

	medications.
Manage health calendar	Provide a calendar to record and display health care events.

Table 3: Management of care plans within a PHR-S

2.4 Security & authorization management

A PHR-S should protect the patient's data from unauthorized users. Therefore security and authorization functions (Table 4) play an essential role in the PHR-S. The data in a PHR should be kept confidential, using the proper technology to encrypt and encode the medical data. Another set of security functions ensure that the right data should be accessed by the right users; the users should be given discrete roles (e.g. patients, clinicians). Each role credits a set of permissions to different actions. The PHR-S users should be granted access to the system after passing through an authentication process using their credentials.

Functional requirement	Description
Security	Secure the access to the PHR-S and PHR information. Manage the sets of access control permissions granted within a PHR-S. Prevent unauthorized use of data, data loss, tampering and destruction
Entity authentication	Authenticate PHR-S account holder and/or entities before allowing access to a PHR-S.
Entity authorization	Manage the sets of access control permissions granted to entities that use a PHR-S. Enable PHR-S account holders to extend partial or full access to PHR information to other individuals who can act on behalf of the account holder (proxy users), clinicians, systems, and others.
Entity access control	Verify and enforce access control to all PHR-S components, PHR information and functions for end-users, applications, sites, etc., to prevent unauthorized use of a resource.
Non-repudiation	Limit a PHR-S user's ability to deny (repudiate) the origination, receipt, or authorization of a data exchange by that user.
Secure data exchange	PHR data needs to be exchanged securely. This requires measures to insure the confidentiality and integrity of the data.
Secure data routing	Route electronically exchanged PHR data only to/from known, registered, and authenticated destinations/sources (according to applicable healthcare specific rules and relevant standards).
Information attestation	Manage electronic attestation of attestable information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information.
Patient privacy & confidentiality	Enable the enforcement of the applicable jurisdictional and organizational patient privacy rules as they apply to various parts of a PHR-S through the implementation of security mechanisms.
Secure messaging	Enable secure electronic communication between PHR account holders and ESPs.
Manage consents and authorizations	Enable the PHR account holder to manage consents and authorizations. Maintain consents and authorization directives / statements for any entity that may or may not have access to the account holder's PHR.

Manage data masking for sensitive / selective information	Allow the account holder to mask data on a selective records, on field-by-field, or on class basis as one aspect of controlling access to personal health data. The account holder should have the ability to determine what information is available to an authorized account holder of the PHR information.
Manage a registry of actors	Each actor that accesses the PHR should be registered in a directory with their contact information and granted specific access rights.

Table 4: Security aspects of a PHR-S

2.5 Administrative management functions

The administrative side of a PHR-S should support functions such as managing patient's documents and clinical research information, plan processes, manage providers and healthcare facility information, provide public health updates and information resources, as well as administer clinical trial information. The administrative management functions are listed in Table 5.

Functional requirements	Description
Manage account holder demographics	Enable the PHR account holder to manage her demographics information
Manage patient advance care directives	Enable the account holder to create or input advance directives for care under various circumstances.
Manage Documents for Personal Representation	Manage documents that designate those authorized to act on behalf of the account holder.
Manage PHR Output	Enable authorized account holders to manage and generate PHR output.
Manage Information Views	Support account holder-defined information views.
Manage donor information	Provide capability to capture and share needed information as a volunteer donor.
Manage account holder educational material	Receive and validate formatted inbound communications to facilitate and/or perform updating of account holder education material.
Manage access to public health information resources.	Enable access to public health information resources.
Manage access to public Health knowledge bases	Enable access to public health knowledge bases.
PHR information synchronization management	Manage PHR information synchronization across PHR-S applications. Ensure that information entered by or on behalf of the account holder is accurately represented in different applications. Synchronization may involve: • Interaction with entity directories; • Linkage of received data with existing entity records; • Location of each PHR component; and • Communication of changes between key systems.
Administrative management of business rules	Provide the ability to capture, maintain, and version business rules. Apply business rules from necessary points within a PHR-S to control system behaviour. A PHR-S audits changes made to business rules, as well as compliance to and overrides of applied business rules.
Workflow management	Support workflow management functions related to business rules to direct the flow of end user tasks.

Auditable records	Provide audit capabilities for system access and usage indicating who accessed the record, when, what actions were taken, and when the actions occurred. Examples of auditable actions include: created, modified, viewed, extracted or deleted a record. Date and Time stamps require corresponding time zones (see ISO 8601 Standard Time Reference) and consistent time synchronization across complementary information systems (see IETS RFC 1305). Auditable records extend to information exchange, to audit of consent status management and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records. Audit log formats may conform to standards such as IETS RFC 3881 (Security Audit & Access Accountability Message XML Data Definitions for Healthcare Applications).

Table 5: Administrative management aspects of a PHR-S

2.6 External Service Provider related functions

The PHR-S is responsible for handling functions related to ESPs (Table 6). This involves selecting an available External Service Provider, importing / exporting PHR-S information, scheduling encounters between providers or between patients and providers, providing relevant information to providers related to the encounters and store documents related to the encounters.

Functional requirements	Description
Manage Encounters with Providers	Manage information for scheduling, preparation, and assimilation of knowledge gained by encounters with providers.
Manage clinical findings (symptoms)	Manage information related to the assessments of the clinical status of the patient, during the visit
Communications between External Service Provider and patient and / or the patient representative	The system should enable the account holder to capture information in preparation for the encounter. The system should enable the account holder to request appointments with health care providers and capture information in preparation for the encounter.
Data and documentation from External Clinical Sources	The system should capture, index, and store documentation related to the encounter.
ESPs clinical findings capturing	Enable the PHR Account Holder to capture provider assessments and their supporting documentation such that the account holder or another provider may independently verify the assessments.
Manage clinical research Information	The system should support the participation of an account holder in clinical trials via the provision of PHR-S information to be used in mutliparametric research or clinical trials
Manage anonymized data request	Upon approval by the account holder, feed ESPs with anonymized PHR-S data for the needs of mutliparametric research or clinical trials.
Manage administrative data from ESPs	Manage administrative information from external sources such as insurance plans and pharmacy benefit managers.
ESPs profile information	The PHR-S should include functionality that supports obtaining a list of ESPs and then maintain or provide access to provider information

Manage selection of ESPs	Support an account holder in seeking ESPs who may meet their healthcare requirements.
Manage account holder provider's Information	Manage contact information for the PHR Account Holder's current and past ESPs.
Manage PHR data import and export	Allow account holder to manage the import to and export of data from the PHR-S to an External Service Provider

Table 6: ESP related aspects of a PHR-S

2.7 Other resources management functions

In this section (Table 7) we present a set of functionalities that cannot be classified under the above-mentioned categories.

Functional requirement	Description
Manage account holder preferences	Enable the PHR account holder to modify PHR presentation preferences.
Wellness, preventive medicine, and self care	Enable the account holder to maintain their wellness, nutrition, lifestyle and self care information
Manage tools and functions to assist self care	Provide various functions to allow the account holder to manage their health care related activities and events.
Manage Tasks	Healthcare events or activities that require the account holders participation can be organized as tasks and presented in calendar mode
Manage reminders	Present the account holder with reminders either sent by external sources such as from ESPs, or internally generated from information in the PHR, such as guideline-based reminders, prescription refills, appointment reminders, or other calendar entries.
Manage health alerts	Notify the account holder of an event or situation that may need immediate action.
Account holder configured alerts	Alerts and reminders should be configured by the account holder based on a variety of triggers or conditions.
Manage recommendations	Capture and track ESP originating recommendations for future care.
Manage health educational material	Provide reliable patient education and information customized to the patient based on the information in the PHR to help the account holder explore treatment options.
Account holder decision support	Provide clinical decision support appropriate to the use of the PHR in self-care, home health, and remote settings.
Manage guidelines and protocols	Guidelines for general direction in managing a specific problem or condition can be acquired from a variety of sources for improved decision making.
Drug interaction checking	Display warnings and severity levels of potential adverse interactions based on the data in the PHR account holder's medication and allergy list.
Integration with third parties' clinical decision support services	Provide the ability to query external clinical decision support services.
Manage standard reporting	Enable account holders to request and read pre-configured, packaged reports of PHR information (e.g. according to CCR or CCD standards).
Manage ad hoc reporting	Allow authorized account holders or designees to request and read ad hoc reports of PHR information.
Present personalized views of	Present ad hoc views of the PHR information, in accordance

the PHR	with user preferences, roles, organizational policies and jurisdictional laws as related to privacy and confidentiality.
Extraction of PHR information	Provide data extraction capabilities, including data aggregation, in accordance with data exchange, analysis, reporting and printing requirements.
Registry and Directory Services	Enable the use of registry services and directories to uniquely identify, locate and supply links for retrieval of information related to: • Patients and providers for healthcare purposes; • Payers, health plans, sponsors, and employers for administrative and financial purposes; • Public health agencies for healthcare purposes, and • Related systems and devices for resource management purposes.
Standard terminologies and terminology models	Employ standard terminologies to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally). Support a formal standard terminology model.
Maintenance and versioning of standard terminologies	Enable version control according to customized policies to ensure maintenance of utilized standards. This includes the ability to accommodate changes to terminology sets as the source terminology undergoes its natural update process (new codes, retired codes, redirected codes). Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by local policy.
Terminology mapping	Map or translate one terminology to another as needed by local, regional, national, or international interoperability requirements
Standards based interoperability	Provide automated health care delivery processes and seamless exchange of clinical, administrative, and financial information through standards based solutions.
Interoperability standards	Support the ability to operate seamlessly with other systems, either internal or external, that adhere to recognized interoperability standards. “Other systems” include other PHR and EHR Systems, applications within a PHR-S, or other authorized entities that interact with a PHR-S.
Interoperability standards versioning and maintenance	Enable version control according to local policies to ensure maintenance of utilized interoperability standards.
Standards-based application integration	Enable standards-based application integration.

Table 7: Unclassified functional requirements of a PHR-S

3 PHR-S Reference Architecture

3.1 PHR-S context

In this paragraph we present the context in which the Personal Health Record System is being examined. As showed in Figure 1, we make the discrimination between the pure StrokeBack ecosystem of application, services and their respective clients (left side of the figure) and the external platforms and systems, not directly controlled by the consortium participants (right side of the figure).

While in the context of the project the PHR-S will interact exclusively with entities residing in the left side, the architectural approach to be pursued –and be presented in the subsequent paragraphs- will be generic enough to cover tentative interaction also with entities in the right side. In that sense, the PHR-S is approached as both a service provider and service consumer system. Indicative services that could be consumed –being provided by ESPs- include nation-wide certified medication lists or mapping services, Electronic Health Record and Master Patient Index Service Providers, etc. Indicative services that could be provided by the PHR-S include exercise guidance and videoconference, just to mention two definite objectives of the StrokeBack project.

The exact services to be provided within the project context will be specified in the subsequent phase of collecting and analysing end users' requirements. Some indicative services, though are being presented in this document (paragraph 3.5).

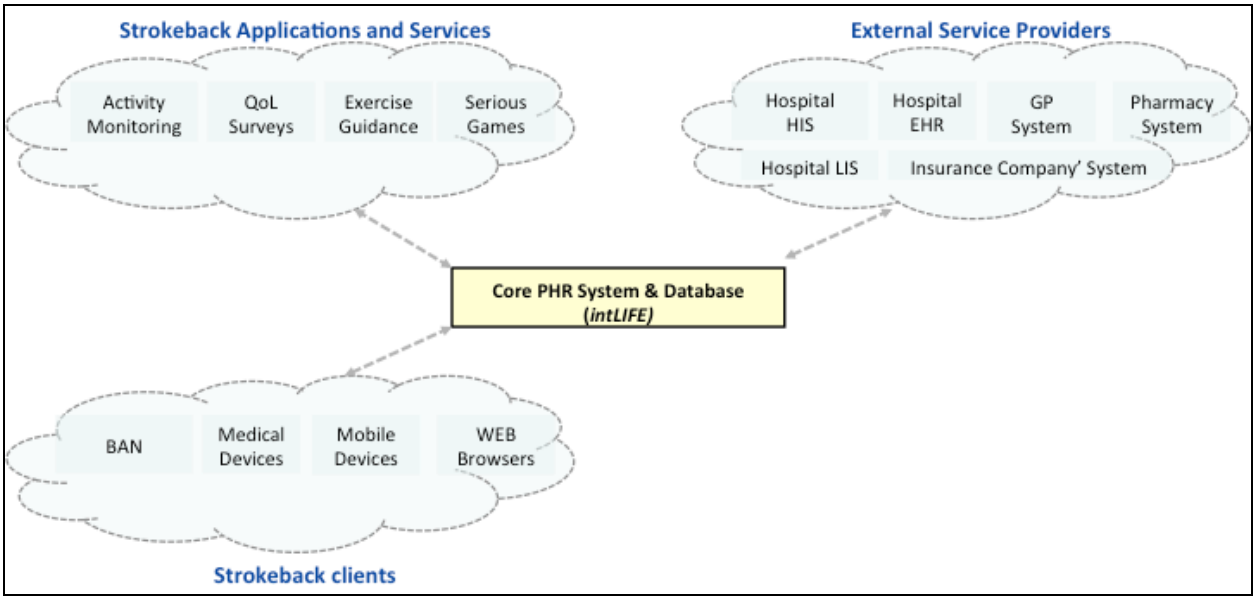

Figure 1 PHR-S context

3.2 PHR-S high level architecture

We propose a tiered architecture for the PHR-S, as indicated in Figure 2. Below we provide a brief overview of the components that comprise this architectural approach.

Business Layer The business layer includes components, which implement business logic in order to support well-defined requirements. These components can be physically allocated in the same or in separate servers, depending on the required system distribution. It encapsulates complex business processes and logic, hiding it from the clients layer. Requests from the clients

are not addressed directly to the business layer, but to its neighbouring integration layer that unifies technical and security aspects. The business layer addresses requests to the database via the database layer that unifies technical, security and database aspects. This approach facilitates great flexibility, both in terms of the underlying database technology and the high-level user applications.

Presentation Layer The presentation layer provides functionality to collect information, which is necessary for a client application in order to properly construct its graphic user interface. Making use of appropriate business services, the presentation layer collects the appropriate information for each individual client application. This approach renders the design of the graphical user interface flexible and configurable. Since the presentation layer obtains all subject's health record related data via the PHR-S core tier, all privacy and security policies are automatically applied: any action that the user interface tries to perform is passed through the middle tier via the API and thus subject to the security policies that are enforced there. The user interface also helps patients configure the policies that the middle tier will enforce.

Integration Layer The integration layer implements a common service that allows clients to access components of the business layer. This common service includes appropriate logic in order to make use of the client info (position, requested service name, parameters, ticket) and select the appropriate component from the business layer. Each such component has to be registered in the integration layer registry. If the common service recognizes the component in the registry, it retrieves the necessary info (server ip, component name, platform, method name etc) in order to contact it. The client can be either an external or an internal business method. The requested component could be a web service, provided by an external application or a business internal component. The common service may have a variation of offered interfaces (RMI, http, SOAP, etc.) giving the ability to external clients to make use of familiar technologies and therefore increasing the flexibility of the design. The integration layer includes aspects of security: in some cases (configurable in the phase of service registration in the integration layer registry), it communicates with the security-related business component prior to deciding on whether to permit access to the requested service, or not.

Finally, the integration layer, being essentially a single access point, it can manage user tracking, logging, and quality of service metering, using a common approach for all the requested services.

Database Layer The database layer implements a common service allowing core system clients to communicate with the system database in order to execute SQL commands. The common service has logic in order to use the appropriate SQL commands depending of the database provider. The database layer includes aspects of security: it communicates with the database prior to deciding on whether to give the ability to execute a requested command, or not.

Application Program Interface (API) The Application Program Interface is a set of well-described interfaces, which give the ability to a client to communicate with selectable system services offered by the business layer.

External Service Provider The external service provider is a provider of a set of services. See paragraph 1.2 for more details.

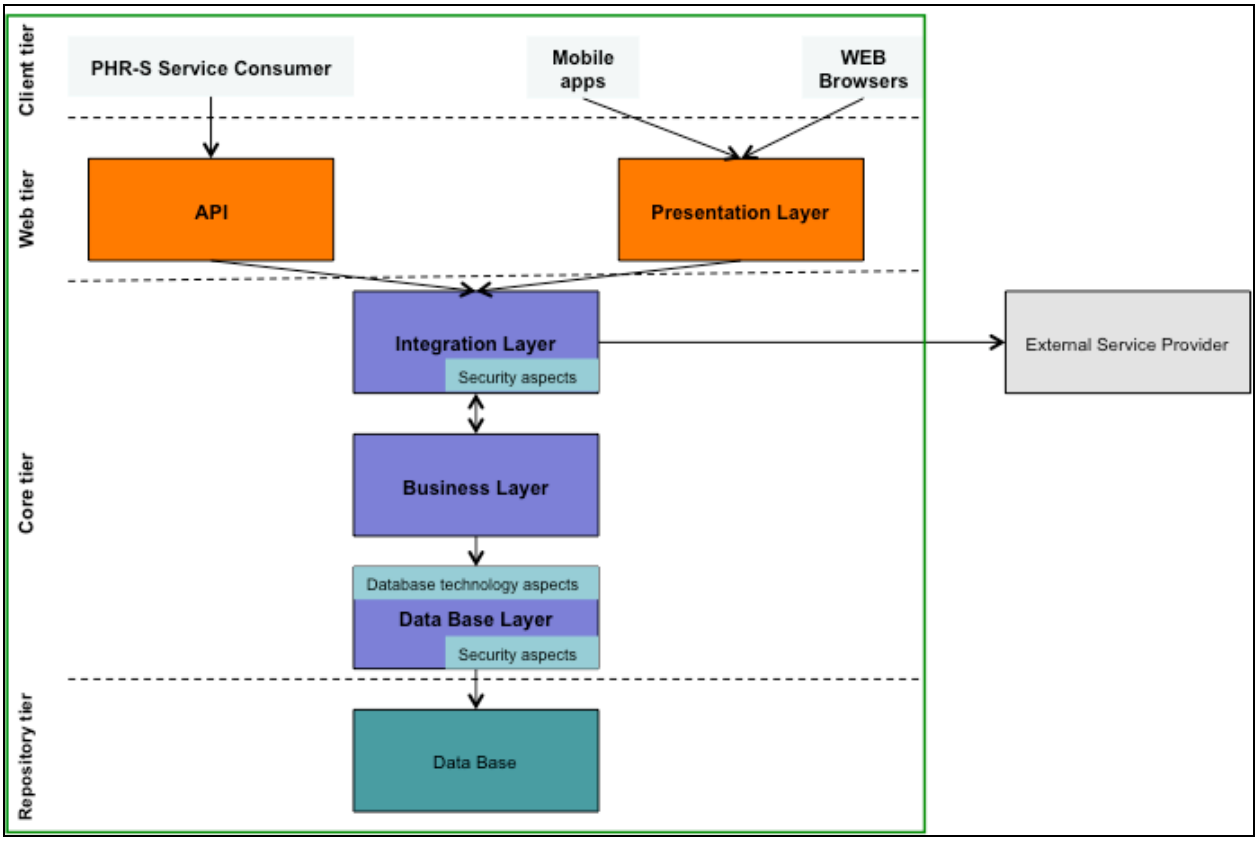

Figure 2: PHR-S architecture

3.3 PHR-S integration layer details

An entity of the client tier can communicate with business components residing in the core tier only by using the integration layer. The exposed services can act either as WSDL or as RMI services. Calls from any client starting from the technology specific interface adapter (WSDL, RMI) pass through the integration layer before they arrive to the business layer component (Figure 3).

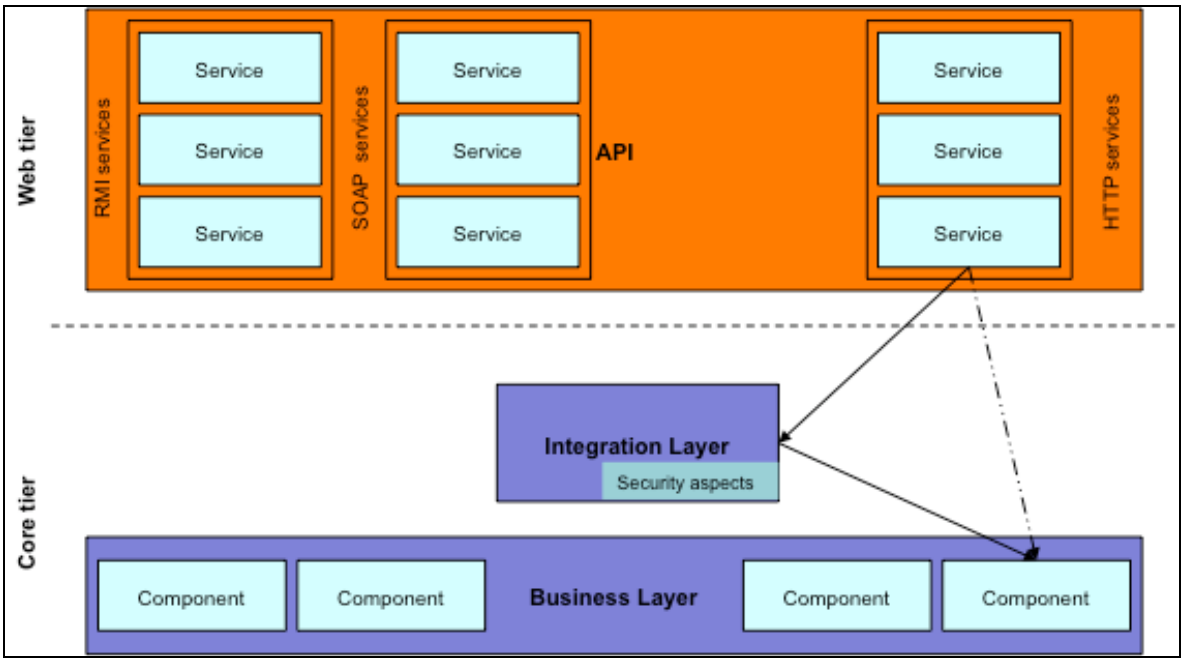

Figure 3: Technologies supported by the integration layer

Using the same generic service description a client may call business layer components by changing specific parameters. For example INT_serviceid='Component_1' or 'Component_2' (Figure 4). The client gets the service information by reading the integration layer registry and decides where to direct the call. The integration layer is responsible for deciding if the client is able to access a component and for directing the call.

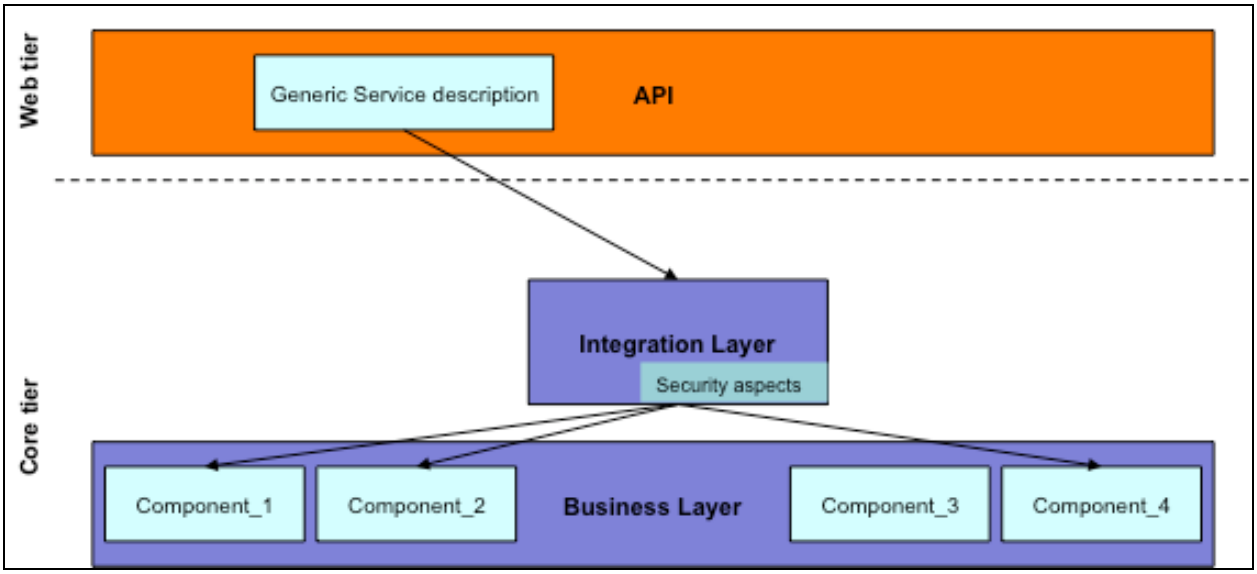

Figure 4: Generalization of the service description provided by the integration layer

Using a specific service description (e.g. service description1 or description3) a client can call only access specific components of the business layer (e.g. component1 or component3, respectively). The integration layer decides if the client is able to access those components.

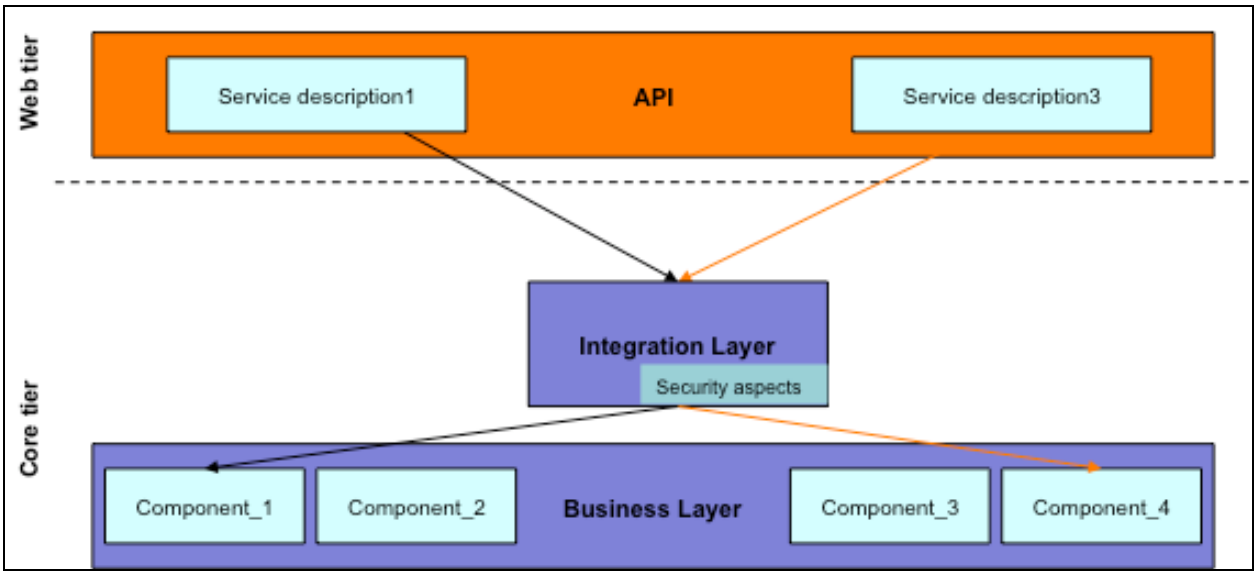

Figure 5: Correlation between service description and business layer components

System business components can use external services without caring about the underlying technology. The integration layer uses registry info in order to direct the call to WSDL or RMI adapters in order to make contact with the external services. An HL7 adapter module intervenes between the integration layer and the ESP to enable communication with systems that support this messaging standard.

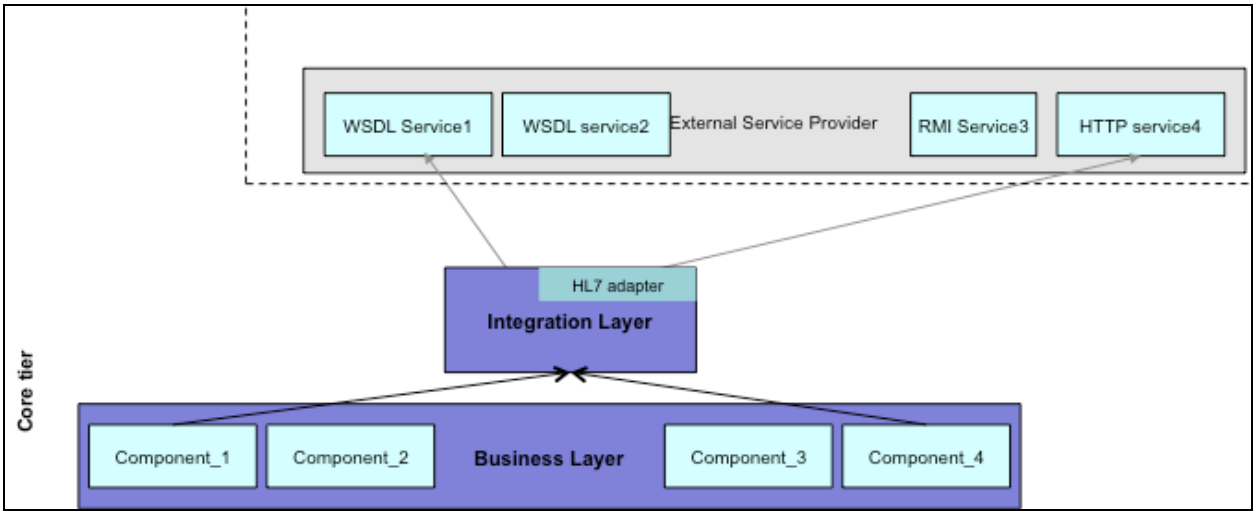

Figure 6: External services being used by the PHR-S business layer, via the integration layer

3.4 PHR-S database layer details

The database layer includes modules (each of which corresponds to different underlying database providers, i.e. Oracle, MySQL, SQL Server) that are responsible for adapting each SQL request originating from the business layer to provider-specific database commands Figure 7. As a consequence, the PHR-S database layer offers seamless integration of the client application and services with the underlying database, irrespective of the database provider[2].

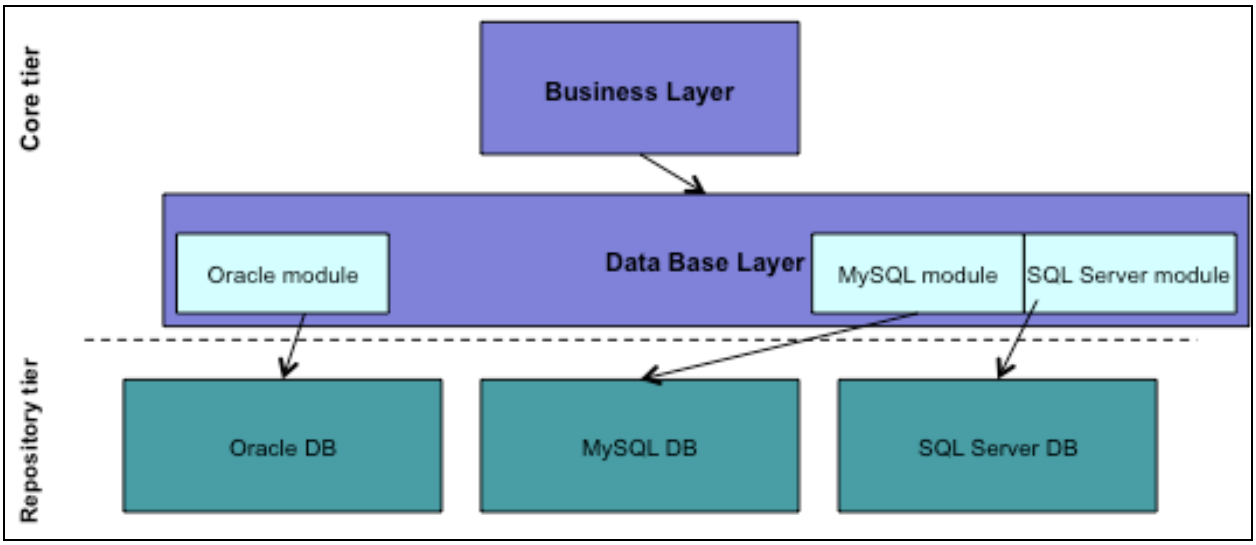

Figure 7 Database layer details

3.5 Core modules and value added PHR-S services

In order to facilitate the independent development of applications and services by third parties that can be easily integrated and glued with the core PHR system, we will follow a modular programming approach. The advantage of this approach is that it provides us with great flexibility in assigning discrete functions to each of the modules and allows easy integration through appropriate interfaces (to be specified in the course of year 1 of the project).

[2] The only limitation is the requirement for support of SQL commands

The PHR-S includes a set of core modules that are necessary independently of the value added services that will be provided to the end users. Such core modules include the following:

- **External adapter controller module** this module is responsible for directing calls to appropriate ESPs components; it also includes libraries for translation to HL7 messages, so as to support standard based communication with external systems.
- **User management module** This module provides functionality related to the administration and management of the users who have access to the PHR-S and the various applications and services built on top of it. It includes aspects related to access rules and user roles (see paragraph 3.6 below for the supported role based security model). Appropriate interfaces of the User Management Module enable access by third party applications and facilitate a centralized approach in users management.
- **Permission management module** This module enables account holders (health record owners or their designees) to manage access rights (permissions) to their PHR. and controls access to protected resources.
- **Audit management module** This module enables logging of information related to the transactions being executed in the PHR-S. Such transactions may include log in attempts, modifications of permissions, modification of the PHR content, etc. The module logs the timestamp and the respective user that is involved for each transaction.

On top of the above, one can easily build independent business services around the core PHR-S. The exact services to be built will be based on the outcome of the end user requirements collection and elicitation process. Nevertheless, we can rather safely present in this paragraph some indicative services that are in line with the general objectives of the project as apposed in the Description of Work:

- **General Health Record Service** This service provides the patients with access to their general medical data (general demographics, family history data, vaccinations, allergies, etc.).
- **General Health Record Service Extension** These extensions provide extra functionality to the patients, correlated with disease-specific aspects. Indicative such extensions provide functionality related to the management of post-stroke health interventions, diabetes, COPD, nutrition and general lifestyle, etc.
- **Exercise Guidance Service** The purpose of this service is to guide the patient while executing a predefined set of activities and/or physical exercises –possibly set up by the clinician using the Care Management Service Module *see below-.* It may provide direct –online- feedback to the subject, during the execution of the activities or offline feedback, after the end of an activity session.
- **Care Management Service** This service provides the clinicians with the necessary functionality in order to set up and monitor plans related to the management of the disease of their patient. This module has different extensions, depending on the disease: e.g. it is different for stroke patients, diabetics, COPDs, etc.
- **Videoconference Service** This service enables patients and clinicians to keep undergo live videoconference sessions. Service configuration parameters are dedicated to defining who and how often can establish such a session. This feature addresses the

need described by the clinicians to be able to put relatively strict rules as to how often their patients may call them in the course of the day.

- **Quality of Life Surveys Service** This service enables the patient to participate in questionnaire-based surveys related to her quality of life.

3.6 Security aspects

The model to be adopted for the security aspects of the proposed PHR-S is a Role Based Security Model (Figure 8).

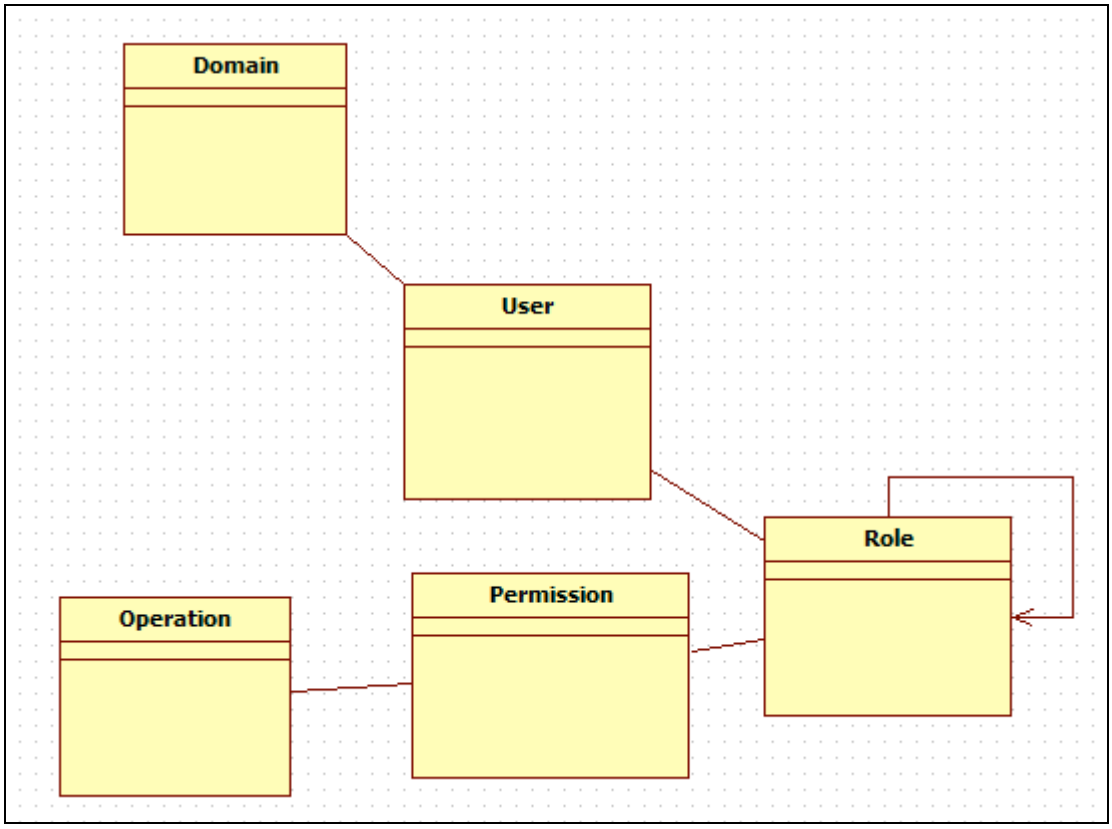

Figure 8: Role based security model: basic relations

The components of this model are the following:

- User = A person or automated agent
- Role = A set of permissions that defines an authority level
- Permission = An approval of action to a resource
- Operation = A system task

The relations between components are the following:

- A user can have multiple roles
- A role can have many permissions
- An operation may have multiple permissions

The following rules are covered with the above approach:

- Operations can be executed only by users with specific assigned permissions
- Users can execute only operations for which they are authorized

The idea behind this model is to restrict system access to authorized users only. The permissions to perform certain operations are assigned to specific roles. Users are assigned particular roles, and through those role assignments acquire the computer permissions to

perform particular computer-system operations. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's role.

We extend the above mentioned Role Based Security Model in order to cover basic needs of the system requirements, by using the term Data Query, i.e. an SQL select statement that is used to retrieve information from the database (Figure 9). In our approach of the role based security model there are several Data Queries, which are related with specific parameters and can be used only from assigned users.

- A data query can be assigned with multiple parameters
- A relation between a data query and a parameter can be assigned to multiple users.
- A data query related with a specific parameter, can be used only by assigned users

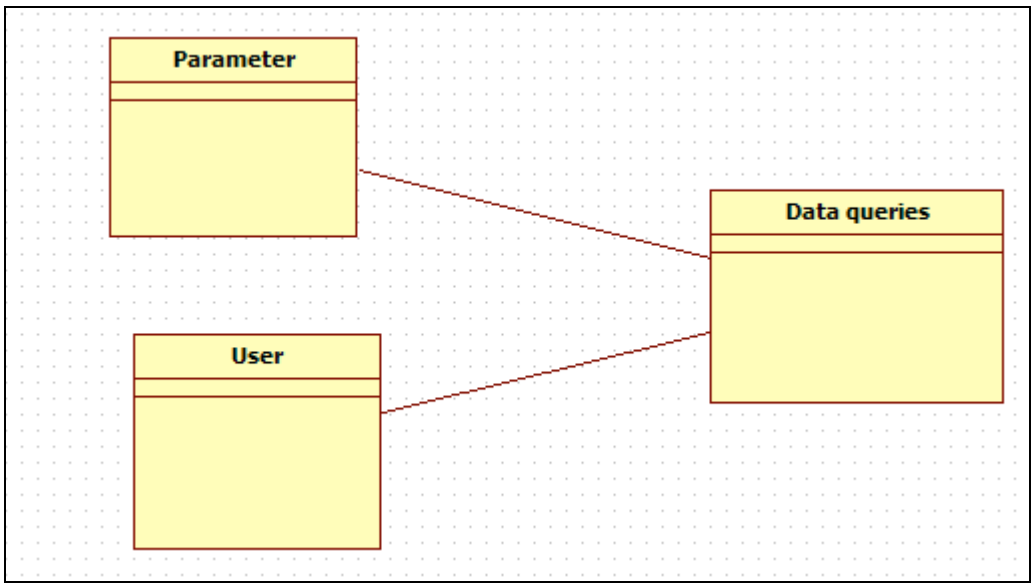

Figure 9: Data queries can only be executed by assigned users

4 Conclusions

In this document we presented a set of generic functional requirements related to a universal PHR-S and introduced our architectural approach related to this system. Emphasis was given in the introduction and presentation of the integration layer that will facilitate the interoperation of the core PHR-S with third party value added services and applications to be developed within the context of the project, but also after the lifetime of the project. It is our intention to revisit the document and align our approach with the StrokeBack end user requirements. The process for collecting them runs on parallel with the preparation of this document. Hence, this document will be sophisticated throughout lifetime of the project.

5 References

[1] The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms, April 28, 2008

[2] HL7 EHR Technical Committee, PHR-System Functional Model, Release 1, DSTU November 2007 Chapter One: Overview

[3] http://code.google.com/apis/health/ccrg_reference.html

[4] http://blogs.msdn.com/familyhealthguy/archive/2008/07/13/again-with-the-standards-thing.aspx

[5] HL7 EHR Technical Committee, PHR-System Functional Model, Release 1 DSTU, November 2007, Chapter Three: Personal Health Functions

[6] http://social.msdn.microsoft.com/Forums/en-US/healthvault/thread/ffc7794d-e7ad-467c-9432-89c42db75495

6 Appendix A: Risk Assessment Table

WP	TOPIC/TARGET	RISK	IMPACT	PROBABILITY			SEVERITY			RISK CLASS
				L	M	H	L	M	H	
5	System Integration	Difficulty in integrating third party services to the core PHR-S	Fragmented applications.		M				H	M

7 Appendix II: Risk Management Audit Log

No.	Risk	Participants involved	Potential Mitigation Actions
1	Difficulty in integrating third party services to the core PHR-S	**ICOM, MEYTEC, IHP, RFSAT, UPA**	Detailed specification of the interfaces Integration of early prototypes will be pursued to facilitate the identification of tentative integration issues