

Chapter 11

Personal Health Record

**Artur Krukowski, Carlos Cavero Barca, Juan Mario Rodríguez,
and Emmanouela Vogiatzaki**

Abstract This chapter focusses on the introduction of the Electronic (EHR) and Personal Health Records (PHR) as new technological approaches aimed at standardising electronic management of medical information between the patient and its physicians, as well as among medical organisations collaborating in providing integrated medical care services. It presents combined experiences in developing e-Health platforms and services with respect of supporting medical research into the causes and relationships among physiological parameters and health problems concerning different chronic diseases, cardiovascular, stroke, epilepsy, and others. The Personal Health Records (PHR) is presented as a new technological approach aimed at standardizing electronic management of medical information between the patient and its physicians, as well as among medical organizations collaborating in providing integrated medical care services. On the examples of most common commercial as well as open-source implementations of such system we aim to describe roles and aims behind electronic health recording, follow with applicable legal and standardizations frameworks and European activities in this area, leading towards introduction to most common commercial as well as open-source implementations of such systems and concluding with indication of specific adaptations enabling the use of stored personal health data for scientific research into causes and evaluation of chronic illnesses. We describe also ethical and privacy concerns that are relevant to using and exchanging electronic health information.

A. Krukowski (✉)
Intracom S. A. Telecom Solutions, Athens, Greece
e-mail: krukowa@intracom-telecom.com

C.C. Barca • J.M. Rodríguez
ATOS Research and Innovation (ARI), ATOS, Madrid, Spain

E. Vogiatzaki
Research for Science, Art and Technology (RFSAT) Ltd., Sheffield, UK

11.1 Role and Structure of PHR

The Electronic Health Record (EHR) of a patient can be defined as digitally stored health care information about individual's lifetime with the purpose of supporting continuity of care [1], education and research, and ensuring confidentiality at all times. A patient's healthcare information may be spread out over a number of different institutes that do not interoperate. In order to provide continuity of care, clinicians should be able to capture the complete clinical history of the patient. The Personal Health Record (PHR) is the electronic part of the health-related information of a person (such as diagnoses, medications, allergies, lab test results, immunization records but also administrative tasks such as appointment or prescription renewals) that can be extracted from multiple sources, but always under the control of the consumer, patient or informal caregiver. This is the relevant difference between the PHR and the EHR or electronic medical record, which is maintained by the healthcare providers and payers [2].

The EHR standardisation aims to ensure that patient records are used to support shared care among clinicians with different specialisations, while enabling the mobility within and among countries for people who give and receive healthcare.

From the viewpoint of standardization, the single most important characteristic of the EHR is the ability to share EHR information between different authorized users. In technical terms, this requires interoperability of information in the EHR and interoperability of EHR systems that exchange and share this information. We distinguish two major levels of interoperability (info sharing) of information [3]:

- **Functional interoperability:** it is the ability of two or more systems to exchange information (so that it is human readable by the receiver); and
- **Semantic interoperability:** it is the ability for information shared by systems to be understood at the level of formally defined domain concepts (so that information is digitised by the receiving system). Semantic interoperability is not an all-or-nothing concept. The degree of semantic interoperability depends on the level of agreement on terminology and on the content of archetypes and templates used by the sender and receiver of information.

One of the key requirements for interoperability of the EHR is to break the nexus between the EHR and the EHR system (i.e. the EHR should conform to an information model independent of both the physical database schema used for local storage and the applications, which create, maintain, and retrieve EHR). This EHR information model should be independent of any particular implementation technology (i.e. it should be a logical information model). Technology independence is essential to make EHR 'future proof' to enable a lifetime EHR possibility.

In order to achieve semantic interoperability of EHR information, there are three prerequisites, with the first ones being required for functional interoperability [4]:

1. A standardized EHR reference model, i.e. the EHR information architecture, between the sender (or sharer) and receiver of the information;

2. Standardized service interface models to provide interoperability between the EHR service and other services such as demographics, terminology, access control and security services in a comprehensive clinical information system;
3. A standardized set of domain-specific concept models, i.e. archetypes and templates for clinical, demographic, and other domain-specific concepts; and Standardized terminologies, which underpin the archetypes. This does not mean that there is need to have a single standardized terminology for each health domain but rather, terminologies used should be associated with controlled vocabularies.

11.2 EHR Standardization Bodies

One of the main factors hindering the widespread adoption of integrated PHRs is the lack of technical standards for interoperability, which is the ability of systems to exchange information using the same mechanisms. “The immaturity and slow diffusion of standards for interoperability and data portability are key barriers to the integration and exchange of structured data among PHRs and the range of relevant entities that provide and finance health care” [5]. The success and final adoption of the PHR systems depends on the capability of interacting with Electronic Health Records (EHRs) and other sources of personal health data e.g. Personal Health Records and Personal Health Record Systems published by the U.S. Department of Health and Human Services in 2006. Currently after years of pursuing the interoperability, the EHR standards continue lacking of the public adoption and immaturity mentioned.

A number of standardization efforts are progressing to provide the interoperability of EHRs such as the CEN/TC 251 [6], ENV 13606 HER Communications standard (<http://www.cen251.org>) [7], openEHR (<http://www.openehr.org>) and HL7 Clinical Document Architecture 2.0 (<http://xml.coverpages.org/CDA-20040830v3.pdf>). These standards aim to structure and mark-up the clinical content for the purpose of exchange. A complementary initiative addressing the issue of how to exchange EHR complying with different content standards is the Integrating the Healthcare Enterprise IHE (<http://www.ihe.net>) Cross-Enterprise Document Sharing (XDS) integration profile detailed in its Technical Framework: http://www.ihe.net/Technical_Framework.

11.2.1 ISO/TC215

CEN/TC 251 [6] is the technical committee on Health Informatics of the European Committee for Standardization. Its mission is to achieve compatibility and interoperability between independent health systems and to enable modularity by means of standardization. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality [8].

The CEN pre-standard ENV 13606:2000 “Electronic Healthcare Record Communication” is a message-based standard for the exchange of EHR content [7]. This standard defines an EHR information model, called the “extended architecture” since it is an extension of the earlier pre-standard ENV 12265.

It also defines a list of machine-readable domain terms that can be used to structure EHR content, a method of specifying “distribution rules”, that is, rules under which certain EHR content may be shared with other systems and, finally, request and response messages that allow systems to exchange subsets of an EHR. ENV 13606 does not attempt to specify a complete EHR system; instead, it focuses on the interfaces relevant for a communication between EHR systems.

ENV 13606 [7] was intended to be the first fully implementable EHR standard, and subsets of it were implemented in a number of EHR projects in the UK, Denmark, the Netherlands, Sweden, and Norway. However, none of these projects used the complete ENV 13606 specification; moreover, the implementation experience showed a number of weaknesses in the standard that limited its usefulness and market uptake: the single-level modelling approach made the information model extremely complex, with lot of optionality and a level of abstraction that made quite difficult to comprehend and implement the model.

In 2001, CEN/TC 251 [6] decided to revise ENV 13606 into a full European Standard, taking into account the existing implementation experience and to adopt the openEHR archetype methodology. ENV 13606 is a standard that is now gradually being approved, and consists of five parts:

- **Reference Model:** it defines the hierarchy of generic building blocks of the EHR through a set of classes. It represents the stable characteristics of the EHR entries, how they are aggregated, and the context information required to meet ethical, legal and provenance requirements;
- **Archetype Interchange Specification:** each archetype defines legal combinations of the building block classes defined in the Reference Model for particular clinical domains, organizations. The archetype model is syntactically equivalent to those of the Good Electronic Health Record project, and the openEHR standard;
- **Reference Archetypes and Term Lists:** it includes the vocabularies for attributes, and archetypes to represent HL7 specialized Acts and openEHR specialised ENTRYs;
- **Security Features:** it defines an interoperable specification for EHR disclosure consent, and an interoperable disclosure log;
- **Exchange Models:** this part is still under discussion.

ENV 13606 standard was not intended to specify the internal architecture or database design of EHR systems or components. Nor is it intended to prescribe the kinds of clinical applications that might request or contribute EHR data in particular settings, domains or specialties. For this reason, the information model proposed there was called the *EHR Extract*, and might be used to define a message, an XML document or schema, or an object interface. The information model in this European Standard is an ISO RM-ODP Information Viewpoint of the EHR Extract. This European Standard considers the EHR to be the persistent longitudinal and

potentially multi-enterprise or multi-national record of health and care provision relating to a single subject of care (the patient), created and stored in one or more physical systems in order to inform the subject's future health care and to provide a medico-legal record of care that has been provided.

11.2.2 ISO/EN EN13606

ISO/EN EN13606 [7] is a norm designed to achieve semantic interoperability in EHR-related data communication among different Health Information Systems (HIS). Its main goal is to define a stable and reliable information structure in order to communicate EHR parts of the same patient (CEN/TC251–ISO/TC215 2010).

The first version of the 13606 four-part pre-standard was published in 1999–2000 but attempts to implement this pre-standard in software proved to be difficult and those implementations which were undertaken suffered from the “HL7 v2 problem” of too much optionality. In 2002 CEN made a decision to revise the 13606 pre-standard and upgrade it to a full normative European standard (EN 13606, also called EHRcom). The ISO/EN13606 standard were completed and ratified after Part 5 by ISO and CEN in February 2010. ISO/EN 13606 architecture provides a framework to communicate EHR data using the dual model approach (reference model and archetypes) to provide the semantic interoperability. The ISO/EN 13606 consists of five parts:

1. **Part 1:** CEN 2007: ISO 2008: The Reference Model, the generic common information model. The global characteristics of health record components.
2. **Part 2:** CEN 2007: ISO 2008: Archetype Interchange Specification, information model of the metadata to represent the domain-specific characteristics of electronic health record entries. This chapter defines how to share archetypes, and not how to exchange them within particular systems.
3. **Part 3:** CEN 2008: ISO 2009: Reference Archetypes and Term Lists, establishing the normative terminologies and controlled vocabularies.
4. **Part 4:** CEN 2007: ISO 2009: Security Features, covering security mechanisms and methodology.
5. **Part 5:** CEN/ISO 2010: Exchange Models, interface designed to request specific extracts, archetypes or audit log.

The relevant components of the generic reference model are (Fig. 11.1): an “HER Extract” is the root node of the EHR and contains “Compositions” which can be organised using “Folders” (in the same way as Microsoft Windows explorer folders). The “Entry” can be an observation, medication order, diagnoses and can be organized within “Sections”. The leaf nodes (data) are “Elements” which are included in the “Entry” and optionally organized within “Clusters”.

The ISO/EN 13606 is a subset of the full openEHR specification [9]. Within the shared classes the main difference between with the openEHR reference model is that “Entries” are broken down in the corresponding kind of information stored (Munoz et al. 2011).

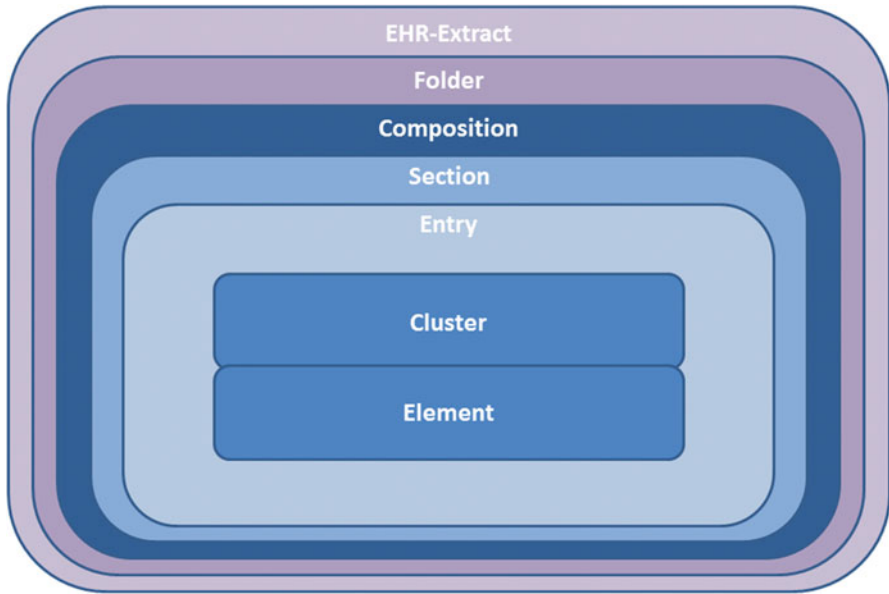


Fig. 11.1 Components of the ISO/EN 13606 association (2009)

11.2.3 GEHR/OpenEHR

The GEHR/openEHR initiative was started in 1992 as an EU research project, called “Good European Health Record”, in the 3rd Framework Program. The initiative was later continued under the name “Good Electronic Health Record” with strong participation from Australia. Currently it is maintained by the openEHR Foundation, a non-profit organization defining itself as “*an international, on-line community whose aim is to promote and facilitate progress towards EHRs of high quality, to support the needs of patients and clinicians everywhere*”. The openEHR is a foundation that supports the development of an open and semantic-connected platform for eHealth systems (www.openehr.org). It is based on 15 years research, focused engineering design and real-world implementation experience, rather than being created as a formal consensus standard. However, over the last years it has had a significant influence over the development of EHR standards by the three main international eHealth standards organisations: CEN, HL7 and ISO. The information model covers the EHR architecture and describes classes such as Folder, Composition, Section and Entry, and of the basic data structure and types. The Care Entry class “define the semantics of all the ‘hard’ information in the record” [10], the Admin Entry represents information recorded during administrative issues. Figure 11.2 shows the ontology leading to the Entry model.

The most noteworthy concept introduced by GEHR/openEHR is the “archetype” concept. This approach uses a two-level methodology to model the EHR structure.

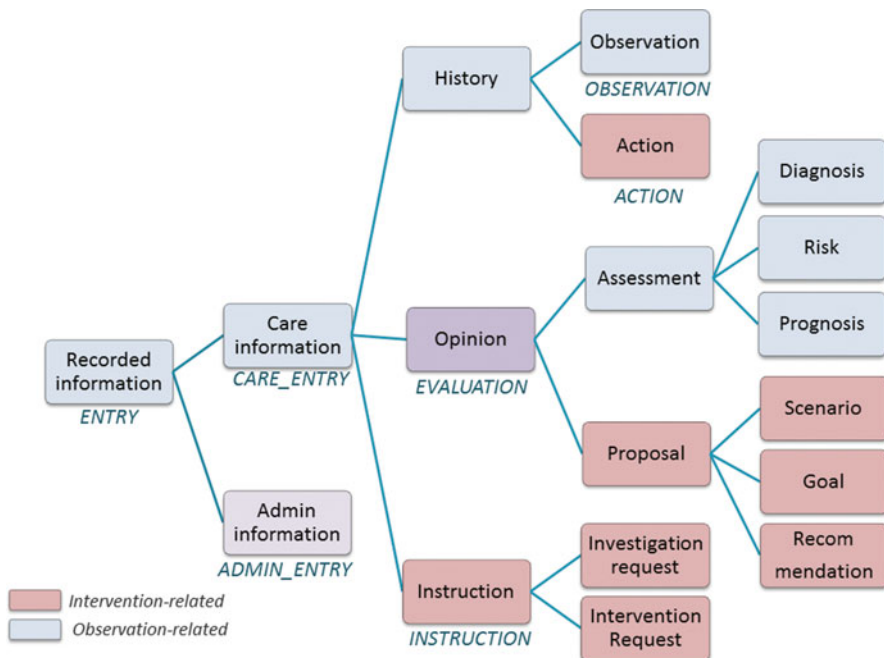


Fig. 11.2 OpenEHR ontology of recorded information [28]

In the first level, a generic reference model that is specific to the healthcare domain but still very general is developed. This model typically contains only a few classes (e.g. role, act, entity, participation) and must be stable over time. In the second level, healthcare and application specific concepts such as blood pressure, lab results etc. are modelled as archetypes, that is, constraint rules that specialize the generic data structures that can be implemented using the reference model. As an example, a constraint may restrict a generic “Observation” class to, e.g., “Blood Pressure” archetype.

An archetype definition consists of three parts: descriptive data, constraint rules and ontological definitions. The descriptive data contains a unique identifier for the archetype, a machine-readable code describing the clinical concept modelled by the archetype and various metadata such as author, version, and purpose. It also states whether an archetype is a specialization of another archetype. The constraint rules are the core of the archetype and define restrictions on the valid structure, cardinality and content of EHR record component instances complying with the archetype. The ontological part defines the controlled vocabulary (that is, machine-readable codes) that may be used in specific places in instances of the archetype. It may contain language translations of code meanings and bindings from the local code values used within the archetype to external vocabularies such as SNOMED or LOINC. It may also define additional constraints on the relationship between coded entries in the archetype based on the code value. As mentioned above the “Care Entry” concept covers the most common and medically relevant information.

In the openEHR four types of entries can be distinguished: observations, evaluations, instructions, and actions. The “observation” and “action” classes represent statements about the past events of the individual subject of record. The “evaluation” classes represent current assessment by the attending health professional, including “diagnosis” and “prognosis”, as well as the representation of the imagined future, like “goals” and “scenarios”. “Instructions” represents future events that should take place as prescribed by the health professional.

The openEHR framework includes a reference information model, the Archetype Definition Language (ADL) for expressing archetypes, an archetype library, implementation technology specifications (XML schemas, IDL specifications etc.) and a collection of open source implementations of the openEHR specifications.

11.2.4 The HL7 Family of Standards

Health Level Seven HL7 (www.hl7.org) is an international organization founded in 1987 and supported by ANSI with the goal of develops global standards related with eHealth. This organization has already defined a set of standards for clinical information interchange, whose name is HL7 standards. Among them HL7 CDA (Clinical Document Architecture) defines the Architecture of electronic documents used within Health domain and it is HL7’s current main strategy for EHR interoperability. Besides, HL7 supports RIM (Reference Information Model), a model of healthcare information as viewed within the scope of HL7 standards, which provides a static view of information needs along with use case models, interaction models, data type models, terminology models, and other types of models to provide a complete view of the requirements and HL7 standards design, thus giving a valid starting point for any HL7-compliant Architecture Design [11].

Meta-classes can be identified in RIM [12], as observed in Fig. 11.3:

- **Act:** actions in the healthcare management
- **Participation:** context for an act: Who? For whom? Where?
- **Entity:** physical things, subjects or targets taking part in healthcare act.
- **Role:** establishes roles that entities play in its participation in healthcare acts.
- **Act Relationship:** represents a relationship between two acts.
- **Role Link:** represents a dependency between roles.

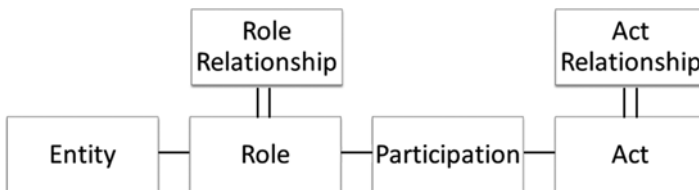


Fig. 11.3 RIM structure

Finally, the HL7 v3 Template is “an expression of a set of constraints on the RIM which is used to apply additional constraints to a portion of an instance of data which is expressed in terms of some other Static Model. Templates are used to further define and refine these existing models within a narrower and focused scope”.

11.2.5 Relationship Between Standards

The openEHR supports the creation, storage, maintenance, and querying of complete EHRs. ISO/EN 13606 is a subset of the full openEHR implementation and it is an appropriate standard for exchange of EHR extracts. At the same time, ISO/EN 13606 offers a partial alignment with HL7 Clinical Document Architecture (CDA) (Fig. 11.4).

Release 2.0, which complies with hl7 RIM. e.g., HL7 CDA is based on the HL7 RIM, but it was designed to represent patient summaries, not thinking on providing decision support capabilities. All the aforementioned reference models are archetype-based. HL7v2.x messaging is an appropriate standard, at least in short/medium term, for transmission of information from clinical information systems to EHR systems.

11.3 Data Structuring Algorithms in PHR

According to European Committee for Standardisation in standards CEN/TC251–ISO/TC215 2010 [6], the EHR is “the persistent longitudinal and potentially multi-enterprise or multinational record of health and care provision relating to a single

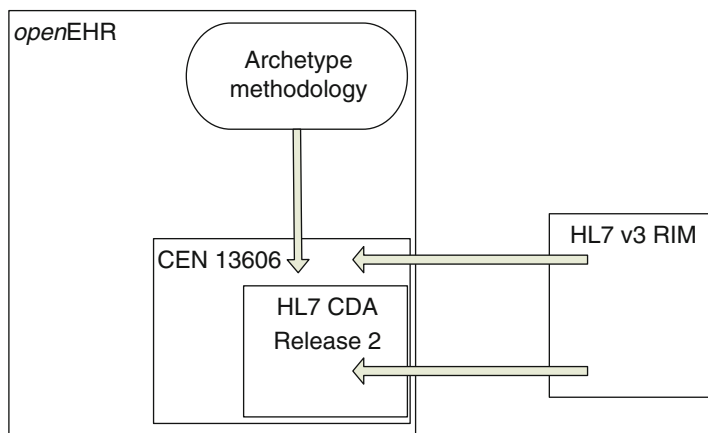


Fig. 11.4 Relationships between standards (openEHR, EN13606 and HL7 CDA)

subject of care (the patient), created and stored in one or more physical systems in order to inform the subject's future health care and to provide a medico-legal record of care that has been provided".

Patient data is managed, in current Hospital Information Systems (HIS), as a digital and well-structured record, which contains all individual-related health data, such as, demographic, diseases, allergies, history and activity during illness periods, etc.

The semantic interoperability of health data can be achieved only with the standardization of EHR. During the last 10 years, the international organizations have been driving great efforts to define the architecture for exchanging properly the health information between EHR coming from diverse systems (Munoz et al. 2011).

11.3.1 The Dual Model Approach

The huge amount of clinical concepts and volatility of the information are the main drawbacks to deploy long-term EHR systems due to the single model approach. The ad-hoc solutions are implemented by technical staff gathering the user requirements from the clinicians providing tools probably perfect at design time but a predictable out-of-date system requiring new releases in the near future if additional information is needed. The “dual model approach”, also called the two-level modelling [13–15] separates out the clinical knowledge (volatile) and the reference model (static).

The medical concepts are modelled using archetypes based on a stable reference model [16]. This approach is attractive for the stake-holders due to its stability, the EHR products are installed once and additional clinical functionalities could be extended using archetypes, on the contrary the ever changing clinical practice jeopardises return on EHR investment in ad-hoc systems.

The dual model approach defines a generic information model, the reference model with domain-invariant classes to be instantiated as well as specific clinical models, which support semantic interoperability, which are called archetypes, containing specific clinical information designed using a common language as it is shown in Fig. 11.5. This approach has been supported by many working groups within different international initiatives.

11.3.2 Detailed Clinical Models (DCM)

The Detailed Clinical Models are actually “a new way to structure medical information. It combines expert knowledge, data specification and terminology and enables various technical applications”. They specify the information models and the way the data is exchanged: user interfaces, data management, decision support systems and so on. It could be considered equivalent to Archetypes, Templates or Clinical Statements. The Clinical Information Modelling Initiative (CIMI) is working to establish those common models from different standards, initially modelling these DCMs in both ADL (archetype definition language) and UML (www.uml.org).

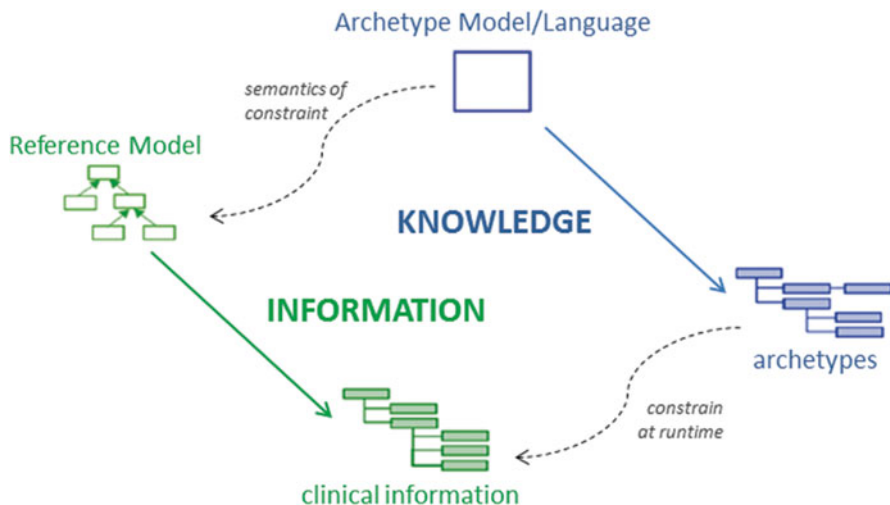


Fig. 11.5 Dual model approach

11.4 Standardisation of User Interfaces to PHR

11.4.1 Continuity of Care Record (CCR)

The American Society for Testing and Materials (ASTM International) Continuity of Care Record (CCR) is a clinical framework that was first developed by health care practitioners to meet the information exchange needs of primary care providers. ASTM defines the CCR as a “summary of the patient’s health status (e.g., problems, medications, allergies) and basic information about insurance, advance directives, care documentation, and care plan recommendations” [17].

11.4.2 CCD (Continuity of Care Document)

A CCD is a joint effort between HL7 International and ASTM approved as an ANSI standard in 2007 in order to use HL7 CDA for sharing the CCR (Continuity of Care Record) patient summary. It represents a complete implementation of CCR, combining the best of HL7 technologies with the richness of CCRs clinical data representation, and does not disrupt the existing data flows in payer, provider or pharmacy organizations.

The Continuity of Care Document (CCD) establishes a detailed set of constraints and templates, covering the main sections of the summary record to be represented as CDA elements, according to the HL7/ASTM Implementation Guide for CDA Release 2-Continuity of Care Document (CCD) Release 1 (2007).

11.4.3 *Integrating the Healthcare Enterprise (IHE)*

International is a global association of healthcare IT vendors, user organisations, clinical professional societies, and advocacy groups that promotes interoperability through the co-ordinated use of established standards such as Digital Imaging and Communications in Medicine (DICOM) and HL7. IHE, more than any other single organisation, paved a way for practical medical interoperability [8].

11.5 Terminologies

Coded elements are used in the healthcare environment to precisely define the clinical concepts language-independently. The use of medical terminology is one of the bases to provide semantic interoperability.

- **Systematised Nomenclature of Medicine Clinical Terms (SNOMED-CT)** <http://www.ihtsdo.org/snomed-ct> consists of controlled medical vocabularies (CMVs),—accumulated medical concepts updated in a rigorous fashion. It has been gaining momentum as the primary coding method for clinical concepts. SNOMED has become the presumptive source of clinical codes and concepts within its member countries.
- **Logical Observation Identifiers Names and Codes (LOINC)** <http://loinc.org> is a database and universal standard for identifying medical laboratory observations. It was developed in 1994 and maintained by Regenstrief Institute, a US non-profit medical research organization. It was created in response to the demand for an electronic database for clinical care and management and is freely available.
- **International Classification of Diseases (ICD)** <http://www.who.int/classifications/icd/en> is the standard diagnostic tool for epidemiology, health management and clinical purposes. This includes the analysis of the general health situation of population groups. It is used to monitor the incidence and prevalence of diseases and other health problems. It is used to classify diseases and other health problems recorded on many types of health and vital records including death certificates and health records. In addition to enabling the storage and retrieval of diagnostic information for clinical, epidemiological and quality purposes, these records also provide the basis for the compilation of national mortality and morbidity statistics by WHO Member States. It is used for reimbursement and resource allocation decision-making by countries.

The crucial issue regarding the deployment of an EHR product in the medical environment is the ease of mapping to existing local data stores, as well as to national specifications (i.e. as an interface specification, for instance from hl7 v3 to archetypes). In order to provide the semantic interoperability the connection with external health terminology bindings is mandatory to be language independent [18].

The term binding is supported for manual or semi-automatic creation between archetypes and the concepts in terminology systems [19, 20] but the main drawbacks still reside in,

- The big amount of clinical concepts and their relationships, which makes necessary to filter out the terms using a powerful and intelligent tool.
- Mapping and translating concepts across vocabularies.

11.6 European R&D Projects Related to EHR Standardization

According to an eHealth ERA report related to eHealth priorities and strategies in European countries [21], the achievement of a European EHR is not yet an overarching goal, but collaboration on developing individual countries' EHR or even basic patient summaries is a first step. Electronic Health Record is a rather fuzzy term, which has various definitions. A long-term objective of most European countries is a system of regional or nationwide summaries, or sometimes even full (occasionally life-long) document-based or deeply structured records for each citizen. Such a summary or record may be viewed by any of the following:

- Either all the necessary persons concerned
- Only by those who need access in order to ensure safe health services
- Only by those who have been directly authorised by the patient.

The eventual development of EHR is evident in 25 out of the 32 countries reviewed during the preparation of the above-mentioned report. Six countries report that they currently have widespread local EHR in hospitals and other health provider organisations, which, however, are not yet fully interconnected. Three countries have a national EHR, although they are yet restricted in scope. Luxembourg, for example, maintains radiology records for its citizens; and in Sweden, citizens have a medication record. Germany, Sweden and Turkey are currently developing the structures of a patient summary or minimal data set. Consistent with its regions-based healthcare system, Spain is developing this work on a regional level. Only one country has a fully implemented EHR system of a countrywide scope—the Czech Republic. The Danish MedCom infrastructure supporting the electronic exchange of various healthcare related messages between healthcare and other service providers is expanded towards a countrywide EHR system as well.

Interoperability seems not to be as high on most countries' agendas as one might expect, given that it is one of the key issues in the EU eHealth Action Plan, it is a core element of current discussions among European Member States, and is also vividly present in international discussions. Only about one-third of the countries' fact sheets mention interoperability explicitly. With the exception of Italy, Romania and Spain, which have made technical and semantic interoperability priority issues, interoperability is seen as a challenge that needs to be addressed as part of a larger

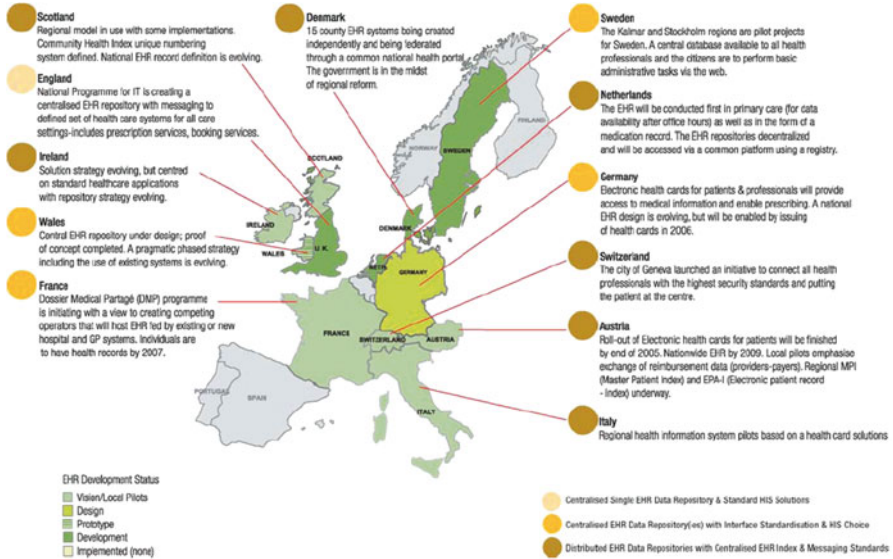


Fig. 11.6 Overview of status of implementation and uptake of hospital information systems and electronic health records throughout Europe (www.capgemini.com)

initiative. In Denmark, for example, MedCom has already developed a platform for technical standards and interoperability for eMessages—the Danish Health Data Network—and SNOMED CT (Systematised Nomenclature of Medicine Clinical Terms) is currently being translated to provide semantic interoperability. Figure 11.6 summarizes the status in several European countries regarding existence of EHR.

11.6.1 European R&D Projects Related to EHR Standardization

The objectives of the EU funded (2007–2010) EHR-IMPLEMENT project (<http://www.ehr-implement.eu>) are to collect, analyse and compare national initiatives of broad scale EHR implementations among European countries focusing on socio-organisational issues and to provide best practice, policy and strategic recommendations to facilitate EHR implementation throughout Europe. The project aimed to:

- Analyse selected national policies, strategies and initiatives for broad scale EHR implementation taking into account cultural and organizational diversities of health systems in six European Member States (Belgium, Denmark, France, Ireland, Slovenia and United Kingdom);

- Carry out a survey of national policy and action plans for broad scale EHR implementation across European Member States;
- Identify the best practices towards broad scale EHR implementations in European countries;
- Raise the awareness of decision and policy makers regarding socio-cultural and organizational issues of broad scale EHR implementation; and
- Support the creation of a multidisciplinary community of scientific experts, technical personnel and National Health System representatives to promote information sharing and mutual learning

11.7 PHR/EHR Implementations

11.7.1 Commercial Implementations

Since the beginning major companies have invested on developing proprietary though freely accessible, own brands of Personal and Electronic Health systems, most well-known ones are listed below.

11.7.1.1 Google Health

Google Health was a personal health information centralization service, introduced by Google in 2008 and cancelled in 2011. Google Health was under development from mid-2006. In 2008, the service underwent a 2-month pilot test with 1600 patients of The Cleveland Clinic. Starting on May 20, 2008, Google Health was released to the public as a service in beta test stage. On 15 of September, 2010 Google updated Google Health with a new look and feel. On 24 of June, 2011 Google announced it was retiring Google Health on 1st of January 2012. The reason Google gave for abandoning the project was a lack of widespread adoption.

The service allowed Google users to volunteer their health records—either manually or by logging into their accounts at partnered health services providers—into the Google Health system, thereby merging potentially separate health records into one centralized Google Health profile.

Volunteered information could include “health conditions, medications, allergies, and lab results”. Once entered, Google Health used the information to provide the user with a merged health record, information on conditions, and possible interactions between drugs, conditions, and allergies. Google Health’s API was based on a subset of the Continuity of Care Record.

Google Health was an opt-in service, meaning it could only access medical information volunteered by individuals. It did not retrieve any part of a person’s medical records without his or her explicit consent and action. However, it did encourage users to set up profiles for other individuals.

11.7.1.2 Microsoft Health Vault

Microsoft HealthVault (<http://www.healthvault.com>) is a WEB-based platform from Microsoft to store and maintain health and fitness information. It started in October 2007 in the US. As of 2013, the website addresses both individuals and healthcare professionals in the UK and Germany and the list of national deployments constantly grows.

A HealthVault record stores an individual's health information. Access to a record is through a HealthVault account, which may be authorized to access records for multiple individuals, so that a mother may manage records for each of her children or a son may have access to his father's record to help the father deal with medical issues. Authorization of the account can be through Windows Live ID, Facebook or a limited set of OpenID providers.

An individual interacts with their HealthVault record through the HealthVault site, or, more typically, through an application that talks to the HealthVault platform. When an individual first uses a HealthVault application, they are asked to authorize the application to access a specific set of data types, and those data types are the only ones the application can use. An individual can also share a part (some data types) or the whole of their health record with another interested individual such as a doctor, a spouse, a parent, etc.

HealthVault Connection Centre allows health and fitness data to be transferred from devices (such as heart rate watches, blood pressure monitors, Withings Wi-Fi body scales etc.) into an individual's HealthVault record. User can find and download drivers for medical devices. A dedicated Device Driver Development Package from Microsoft allows also device manufacturers to develop the software support for their devices such that they can communicate with the Health Vault.

HealthVault supports storage of DICOM (<http://dicom.nema.org>) based medical imaging. Consumers can upload and download medical imaging DVD through HealthVault connection centre. Third parties can also upload and download medical imaging to/from HealthVault. In addition, there has been plethora of HealthVault medical imaging viewers released by the third party to connect to HealthVault even on mobile phones.

HealthVault supports a number of exchange formats including industry standards such as the Continuity of Care Document (CCD), Continuity of Care Record (CCR) and Clinical Document Architecture (CDA). Support for industry standards makes it possible to integrate with diverse personal health record solutions.

A list of WEB applications from 3rd-party providers is available at the HealthVault website. Health service providers can develop their own support for MS Health Vaults via a HealthVault .NET Software Development Kit. Examples include:

- InstantPHR released by Get Real Health (www.getrealhealth.com)
- HealthUnity PHR Gateway (www.healthvault.com) by HealthUnity
- PassportMD developed by PassportMD (www.passportmd.com)
- ActivePHR released by ActiveHealth (www.activehealth.com)

11.7.1.3 World Medical Card

World Medical Card (www.wmc-card.com) is a product and registered trademark belonging to World Medical Centre, a Norwegian company headquartered in Bergen, Norway. The company's business is Health information technology, more specifically a supplier of Personal health records.

The World Medical Centre was established in 1998 for creating a system for improving the safety of people in situations requiring immediate medical treatment by a doctor, not familiar with the person's medical history. The international, personal medical card (World Medical Card) system was developed in cooperation with specialists in acute medicine and the University of Bergen, to allow individuals to carry essential medical information with them at all times and everywhere in the world.

Early versions included smart card and data matrix versions, but were abandoned as they required specific infrastructure to be installed at the facility receiving the patient in order to be useful. The latest generation of cards include the information in printed letters, but is only accessible by physically cutting open the card. This also reveals an emergency code that allows the medical professional access to a read-only web profile describing the cardholder.

Later the product portfolio was extended to include a WEB-based Personal health record, allowing the user to manage personal information while also serving as the source of information for producing the card, and a mobile application. Currently it is offered today in a form of three main elements:

1. Online ("onWeb") health profile for adding and editing personal health data
2. Multilingual ("onMobile") WAP phone application for accessing same data
3. Sealed ("onCard") physical card containing compact holder's health data

The company has been a pioneer in promoting the use of the International Classification of Diseases (ICD) ICD-10 document "Classification of Mental and Behavioural Disorders" and Anatomical Therapeutic Chemical (ATC) codes as defined by World Health Organization (www.who.int) for processing all medical data.

11.7.2 *FREE and Open Source Implementations*

The popularity of EHR/PHR systems have given raise to development of Open-Source platform too. Their capabilities and features can closely compete with commercial and proprietary implementation, except when it comes to interoperability and flexibility in developing of add-on services and applications. The list of Open Source EHR/PHR solutions (<http://www.goomedic.com/open-source-emr-list#>) suitable for serving as a base for the development of the project solution include:

- **INDIVO Health** (indivohealth.org) original personally controlled health record (PCHR) system. A PCHR enables an individual to own and manage a complete, secure, digital copy of her health and wellness information. INDIVO integrates

health information across sites of care and over time. INDIVO is free and open-source, uses open, unencumbered standards, and is actively deployed in diverse settings, in particular our own Children's Hospital Boston and the Dossia Consortium.

- **TOLVEN Patient/Clinician HR** (www.tolven.org) focusing on delivering:
 - Personal Health Record (ePHR) that enables patients to record and selectively share healthcare information about themselves and their loved ones in a secure manner.
 - Clinician Health Record (eCHR) enables healthcare actors to securely access healthcare information collated from any number of trusted sources relating to individual patients in a structured and accessible way.
 - Healthcare Informatics Platform enables all healthcare data to be stored and accessed via ePHR and eCHR solutions. It uses industry standard technologies and data models.
 - Health Analytics solution that enables all data stored in the TOLVEN Platform to be extracted or analysed for statistical purposes
- **HealthMe** from KRM Associates Inc. (<http://www.krminc.com>), an open source PHR system developed as part of a Medicaid eHealth transformation initiative for use in West Virginia, known also as HealthMountaineer.
- **OpenEMR** (<http://www.open-emr.org>) is a Free and Open Source electronic health records and medical practice management application that can run on Windows, Linux, Mac OS X, and many other platforms. OpenEMR is ONC Complete Ambulatory EHR certified and is one of the most popular open source electronic medical records in use today. OpenEMR is supported by a strong community of volunteers and professionals. The OpenEMR community maintains OpenEMR's as a free, software solution for medical practices.
- **OpenMRS** (<http://www.open-emr.org>) is both software and a community. OpenMRS is a Java-based, web-based electronic medical record. It started from a simple data model, wrapped into an API, and then built a web-based application that uses the API. The OpenMRS API works like a "black box," hiding the complexities of the data model beneath it and ensuring that applications and modules using the API work with a similar set of business rules for managing the electronic medical record system data.

At the heart of OpenMRS is a concept dictionary. It defines all of the unique concepts used throughout the system. Using combinations of questions and answers, observations (observable data) can be defined as well as forms that gather multiple observations within a single encounter.

OpenMRS is constructed to support modules. Using modules, implementations are able to modify the behaviour of the system to meet their local needs without everyone having to agree on a single approach. Modules have full access to the system, so they can add tables in the database, alter behaviour of the API, and/or add or change web pages in the web application as needed to meet their needs

11.7.3 Implementations from European Research Projects

Many EHR platforms have been developed through European activities, funded by the European Commission through programs such as ICT, ICT-PSP, AAL, ARTEMIS and other ones. The list of most commonly known is provided below.

11.7.3.1 LinkCare Platform

It has been developed by the LinkCare Alliance (www.linkcarealliance.org) as part of the eTEN Project. It aimed to deliver proven information systems for chronic care, linking hospital care, primary care and home care. This concept fills a critical unmet need in current healthcare systems that are challenged by the need of different actors to cooperate in specific scenarios, notably those corresponding to the management of chronic patients.

From the end-user standpoint, LinkCare provides a single vendor integrated solution, a computer supported cooperative work environment, targeting core business areas where costs are greatest and where effective, timely and accurate communication between numerous institutions and actors is critical.

In practical terms, this means that healthcare providers can find in LinkCare technology a supporting tool for those services targeting long-term care. LinkCare facilitates professionals' tasks related to chronic case management, clinical documentation, patient tracking, data analysis, customer relationship management, patient education, professional communication as well as performance evaluation.

The market for information services in chronic care management is truly emerging and LinkCare aims at consolidating a position on it, not only based on the ICT platform but also on the accumulated experience on new models of delivery of care services acquired through the project and through other experiences. This is packed as accompanying consultancy services and/or system integration services to those stakeholders interested in adopting LinkCare in their work practices.

The LinkCare services portfolio includes:

- **Electronic case management module and embedded EPR Interface**: Capability to support integration and communication with the existing Customer's systems using industry standard protocol (namely, HL7 and XML)
- **CRM module—"call-centre" support tools**: Core to the LinkCare services is the existence of a single point of access for customers and networked professionals from where the different actions can be decided, ordered and transferred or executed. This requires a call centre supporting advanced CRM (customer relationship management) features. Furthermore, the specificity of the targeted health services means some extra capabilities such as the link to health information resources (corporate HIS, departmental solutions...)
- **Professional's mobile support tools**: Most of the services that LinkCare will support are based on the mobility of the professionals providing the service. The tools incorporated into LinkCare should fully support these new work practices

allowing the professional to minimise the need to contact the institution. Examples of services should include:

- Enhanced off-line communication features: possibility of sending messages to pagers, SMS messages/emails/voices messages...
 - Enhanced online communication features: MMS, video-clips, video-conference
 - Automatic tracking of pending tasks with professional agenda update. Warning systems to help in the avoidances of delays
- Patient's mobile support tools: Similar to the previous point, the potential for deploying healthcare services to patients will depend on the level of monitoring capabilities that LinkCare tools could offer. Dealing with more severe patients directly links to the availability of more continuous, long-term monitoring, and the possibility of summarizing data, such as:
 - Services in the area of sleep disorders in COPD patients
 - Distant on-line supervision of rehab sessions.

Both examples illustrate the need for:

- extended periods of data collection (1–8 h)
 - significant amount of data transmitted simultaneously
 - need for tools for summarizing the information
- Computer Supported Cooperative Work module including workflow: Support for modelling the clinical processes at customer's site, providing the necessary communication and interaction tools among the involved actors
 - On-line education and reference access to current content, docs and research: Emerging models of care provision maximize the importance of patients and care takers as key partners in the management of health conditions. LinkCare should be a comprehensive and trusted repository/broker for information content that could be passively provided (upon user's will, pull paradigm) or actively suggested (push paradigm, in alignment with the program where the patient is currently treated)
 - Performance monitoring and evaluation module ("control panel/dashboard" and reporting tools): a set of decision management tools providing essential information about key indicators of the clinical and business processes, to allow timely intervention for corrective interventions and analytical support to improvement actions

11.7.3.2 intLIFE PHR

It is a platform developed internally by Intracom S. A. Telecom Solutions (<https://146.124.106.153:8181/intLIFEv1>), enhanced and geared to diverse health application through a number of FP7 funded research projects, such as ICT-PSP-NEXES, AAL-PAMAP, FP7-StrokeBack, Artemis-CHIRON, FP7-ARMOR.

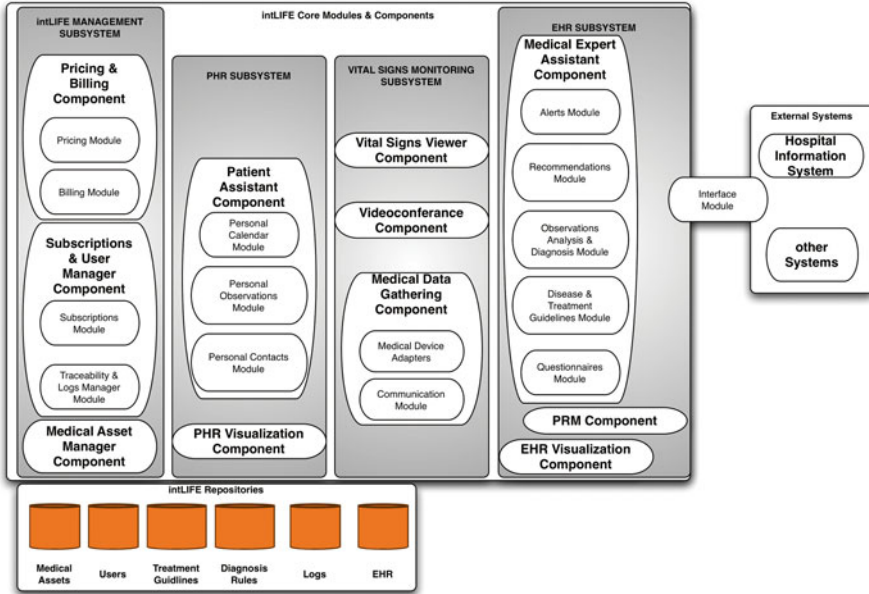


Fig. 11.7 intLIFE core modules and components: electronic health record subsystem

Developed initially with aim to support cardio-vascular services [22], the intLIFE platform has been further enhanced and currently supports the following subsystems (as shown in Fig. 11.7):

- Electronic Health Record Subsystem
- Vital Signs Monitoring Subsystem
- Personal Health Record Subsystem
- intLIFE Management Subsystem

The list features and functionality of the components currently available includes:

- **EHR Subsystem:** the intLIFE EHR application enables clinicians and paramedical personnel to edit/review health related information of the monitored subjects. An Overview tab will provide the user with a quick and printable outline of selected information (e.g. diagnoses, medications, surgeries, specific measurements, etc.). The following information fields are available:
 - Patient’s General Health Profile; family health history, habits and social history (e.g. smoking, alcohol consumption), allergies, vaccinations
 - Visits; organ system findings, manual entry of symptoms and measurements
 - Medical Tests; test orders, manual entry of test results, test results overview and graphic representation
 - Diagnosis Management; insert new diagnoses, using the ICD-10 nomenclature, search for past diagnoses
 - Treatment Management; surgeries, medication

- **EHR Visualization Component** is responsible for presenting the content of the Electronic Health Record of a patient. It stores data to and retrieves data from the Electronic Health Record database of the intLIFE platform. The EHR Visualization component comprises one of the major means of interaction of the Medical Expert User with the intLIFE platform. In order to plan the patient's treatment, a Medical Expert User needs to have current data and information concerning the patient's medical history. Based on data from the patient's EHR the Medical Expert User can decide how to proceed, decide whether intervention is required and determine a success of patient's therapy.
- **Medical Expert Assistant Component** is part of the intLIFE EHR and includes a set of tools that are supportive to the utilization of the intLIFE system by the Medical Expert (Questionnaire Module, Alerts Module, Recommendations Module, Observation Analysis and Diagnosis Module, Disease and Treatment Guidelines Module and Reports Generation Module). It is designed in a modular way, so that new tools can be added in the future. Currently, only the Questionnaire Module is available.
- **Vital Signs Monitoring Subsystem**
 - Medical Data Gathering Component; is responsible for gathering measurements from the peripheral medical devices. It is designed in a modular way, so that new devices can be added in the future. It incorporates a Medical Device Adapter Module for each device to communicate with, and a Comms Module to transfer measurements to intLIFE server.
 - Medical Device Adapters Module; They implement the interfaces between the medical devices and the intLIFE platform, translating the vendor- or even device-specific message structures to a common structure, in order for the measurements to be seamlessly integrated to EHR.
 - Communication Module; It securely transfers the measurements collected from the peripheral medical devices. It can use different protocols (HTTP, FTP, etc.) and different encryption algorithms. It provides graphical user interface for configuring the communication parameters.
 - Vital Signs Viewer Component; The Vital Signs Viewer Component provides the Healthcare Professional User with an effective graphical user interface through which he/she may retrieve from the EHR database and visualize measurements from peripheral Medical Devices.
- **Personal Health Record application**: provides an IP-TV interface to the intLIFE EHR. Automatic login, reveals only those EHR tabs that are relevant to the user (e.g. exclude visits, etc.). Moreover, in addition to the typical EHR the PHR application supports personalized messages, personal reminders, personal rehabilitation plans, questionnaires, personal trainer presenting educational material, and videoconference module. This supports also a novel approach to game-based rehabilitation training [23], developed in the frame of an FP7 project StrokeBack.

- **intLIFE Management Subsystem:** the Administrator Web Interface enables the System administrator to have access to a set of administrative tools:
 - Users Administration; this process activates the necessary web user interface controls that enable the administrator to manage intLIFE users. The administrator is able to add (register), update and deactivate or reactivate intLIFE users.
 - Equipment Administration; This process activates the necessary web interface controls that enable the administrator to manage intLIFE equipment, i.e. it is a device manager that associates medical devices, STBs and other terminal equipment to physical or logical entities (patients/healthcare professionals or network nodes, respectively).

11.8 Adoption Problems

Despite the need for centralizing patient information, the adoption of PHR has been very slow. A study [24] made to assess the functionality and utility of online PHRs, identified 19 websites offering different versions of PHRs. Centralized PHRs should help patients relate accurate history during clinical encounters, check for drug interactions, eliminate unnecessary duplication of laboratory tests and diagnostic studies, and serve as an information hub for patients' health management. An analysis of web-based PHR systems has revealed that most websites did provide access to personal medical information. However, each system demonstrated limited capacity in a different way.

From the 19 sites examined, four were applicable only to certain diseases; another four had recurrent technical problems or connections to a specific hospital's information system. The remaining 11 sites did not provide patients with sufficient guidance as to how they should enter personal data. Some of the sites allowed patients to select medical conditions from categorized lists, which did not cover the patients' complete health condition while others allowed free text entry. To formulate medication history, sites that required patients to choose medication from lists requested them to enter a wide range of descriptive information for each medication such as prescribed dose, administration frequency, start date, name of pharmacy that issued the medication and name of provider that prescribed the medication. With respect to laboratory tests, only two allowed patients to import results from outside sources. From these two sites, only one was functional. Not every site allowed patients to enter insurance coverage information. Majority of the sites required patients to enter date and results of diagnostic tests.

Most people do not keep record of minute details of their healthcare experiences and therefore find it difficult to make use of web-based PHRs. Overall, the sites selected for evaluation offered limited functionality to the public. Low adoption of web-based PHRs can be a direct result of limitations in these applications' data entry, validation and information display methods. Hence, the PHR development needs to be guided in the future by ample patient-oriented research.

11.9 Privacy and Ethical Concerns

One of the most controversial issues for PHRs is how the technology could threaten the privacy of patient information. Network computer break-ins are becoming more common, thus storing medical information online can cause fear of the exposure of health information to unauthorized individuals. In addition to height, weight, blood pressure and other quantitative information about a patient's physical body, medical records can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders, and diseases, etc. Various threats exist to patient information confidentiality, example of are:

- Accidental disclosure: during multiple electronic transfers of data to various entities, medical personnel can make innocent mistakes to cause its disclosure.
- Internal leaks: medical personnel may misuse their access to patient information out of curiosity, or leak out personal medical information for spite, profit, revenge, or other purposes.
- Uncontrolled secondary usage: those who are granted access to patient information solely for the purpose of supporting primary care can exploit that permission for reasons not listed in the contract, such as research.
- External intrusion: Former employees, network intruders, hackers, or others may access information, damage systems or disrupt operations

Unlike paper-based records that require manual control, digital health records are secured by technological tools [25] and [26] identifies three general classes of technological interventions that can improve system security:

Deterrents—These depend on the ethical behaviour of people and include controls such as alerts, reminders and education of users. Another useful form of deterrents has been Audit Trails. The system records identity, times and circumstances of users accessing information. If system users are aware of such a record keeping system, it will discourage them from taking ethically inappropriate actions

Technological obstacles—These directly control the ability of a user to access information and ensure that users only access information they need to know according to their job requirements. Examples of technological obstacles include authorization, authentication, encryption, firewalls and more.

System management precautions—This involves proactively examining the information system to ensure that known sources of vulnerability are eliminated. An example of this would be installing antivirus software in the system. The extent of information security concerns surrounding PHRs extends beyond technological issues. Each transfer of information in the treatment process must be authorized by the patient even if it is for patient's benefit. No set of clearly defined architectural requirements and information use policies is available.

11.9.1 *Ethical Guidelines Regarding Privacy and Using Medical Data*

One of the most controversial issues for PHRs is how the technology could threaten the privacy of patient information. Network computer break-ins are becoming more common, thus storing medical information online can cause fear of the exposure of health information to unauthorized individuals. In addition to height, weight, blood pressure and other quantitative information about a patient's physical body, medical records can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders, and diseases, etc. Various threats exist to patient information confidentiality, example of are:

- *Accidental disclosure*: during multiple electronic transfers of data to various entities, medical personnel can make innocent mistakes to cause its disclosure.
- *Internal leaks*: medical personnel may misuse their access to patient information out of curiosity, or leak out personal medical information for spite, profit, revenge, or other purposes.
- *Uncontrolled secondary usage*: those who are granted access to patient information solely for the purpose of supporting primary care can exploit that permission for reasons not listed in the contract, such as research.
- *External intrusion*: Former employees, network intruders, hackers, or others may access information, damage systems or disrupt operations

Unlike paper-based records that require manual control, digital health records are secured by technological tools. Rindfleisch [25] identifies three general classes of technological interventions that can improve system security:

- *Deterrents*—These depend on the ethical behaviour of people and include controls such as alerts, reminders and education of users. Useful form of deterrents is Audit Trails, recording identity, times and circumstances of users accessing information. Users aware of such a record keeping system, are discouraged from taking ethically inappropriate actions
- *Technological obstacles*—These directly control the ability of a user to access information and ensure that users only access information they need to know according to their job requirements. Examples of technological obstacles include authorization, authentication, encryption, firewalls and more.
- *System management precautions*—This involves proactively examining the information system to ensure that known sources of vulnerability are eliminated. An example of this would be installing antivirus software in the system

The extent of information security concerns surrounding PHRs extends beyond technological issues. Each transfer of information in treatment process must be authorized by patients even if it is for their benefit. No clearly defined architectural requirements and information use policies are yet available. While the trends and developments of ICT in healthcare have given rise to many positive developments, concerns about the use of ICT in user services mainly concentrate on the difficulty

of respecting privacy and confidentiality when third parties may have a strong interest in getting access to personal health data electronically recorded and stored and difficulty in ensuring the security of shared personal data [8]. Therefore the project is dedicated to respecting and protecting the personal data, considered as extremely sensitive since they refer to the identity and private life of the individual. It recognises the intent to create a potential for the circulation of personal data, across local, national and professional borders, giving such data an enhanced European dimension, while respecting the principles of the European Convention of Human Rights, the rules of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and especially the European Directive 95/46/EC, for the protection of personal data will be strictly followed when addressing ethical issues.

11.9.2 Involvement of Adult Healthy Volunteers

Potential ethical issues that are addressed in this research will involve end user interviews, questionnaires and trialling of prototype systems during the development and testing. The right to privacy and data protection is a fundamental right and therefore volunteers have the right to remain anonymous and all research will comply with Data Protection legislation regarding ICT research data related to volunteers. During the research in ARMOR only participant who has sufficient cognitive and physical ability to be able to safely participate and clearly give informed consent are asked to participate. Potential ethical issues arise from the fact that participants, especially those who may tire easily or become distressed. Ethical issues may also arise when the system is used to give participant location or wellbeing information to third parties. Here release of this information is subject to informed consent of participants, and subject to the ethical frameworks to restrict knowledge of this information to only those given consent. All participants in the research are volunteers enrolled from the end user groups connected with this research and all ethical criteria are supervised by ethicists. Participants are ensured privacy and technical platform managing private user data is specially geared to enforce ethics.

11.9.3 Tracking the Location of People

Tracking the location of people is tightly linked with services delivered at the location of the user. This requires new look at the new socio-legal issues they raise. In the ARMOR project we only consider laws applicable to protecting privacy of the general population and NOT the laws and regulation specific for the case of the employee tracking and localization.

The European legislation has adopted specific rules requiring that the consent of users or subscribers be obtained before location data are processed, and that the users

or subscribers be informed about the terms of such processing. The rule is that the applicable law is that of the Member State where the “controller” is established; and not that of the Member State of which the data subject is a national. If the controller is not established in a Member State, and in that case data protection laws of the 3rd-country should be found adequate by the EU-Commission. Location data collection will be in accordance to some basic principles: finality, transparency, legitimacy, accuracy, proportionality, security and awareness. Access to location data must be restricted to persons who in the course of exercising their duties may legitimately consult them in the light of their purpose. The list of relevant laws includes:

- *Directive 95/46/EC*: Protection of individuals with regard to processing of personal data and free movement of such data
- *Directive 2002/58/EC*: Processing of personal data and the protection of privacy in electronic communications sector
- *Directive 58/2002/EC* of the European Parliament and Council of 12 July 2002

Processing of personal data and the protection of privacy in electronic telecommunications sector is further governed by:

- *Directive 97/66/EC*: Data Protection in the Telecommunications Sector
- *Directive 99/5/EC*: Radio equipment and *telecommunications* terminal equipment and the mutual recognition of their conformity
- *Art. 29—Data Protection Working Party*: Working Document on Privacy on the Internet

11.10 Supporting Medical Research Using PHR

Epilepsy, the propensity for recurrent, unprovoked epileptic seizures, is the most common serious neurological disorder, affecting over 50 million people worldwide. Epileptic seizures manifest with a wide variety of motor, cognitive, affective, and autonomic symptoms and signs and associated changes in the electrical activities of the brain electroencephalography (EEG), heart electrocardiography (ECG), muscle electromyography (EMG), galvanic skin response (GSR), as well as changes in other important measurable biological parameters, such as respiration and blood pressure. Their recognition and full understanding is the basis for their optimal management and treatment, but presently is unsatisfactory in many respects. Epileptic seizures occur unpredictably and typically outside hospital and are often misdiagnosed as other episodic disturbances such as syncope, psychogenic and sleep disorders, with which they may co-exist, blurring the clinical presentation; on the other hand, costs of hospital evaluation are substantial, frequently without the desirable results, due to suboptimal monitoring capabilities.

The consent of users or subscribers shall be obtained before location data needed for supplying a value-added service are processed. Users or subscribers will be informed about the terms of such use. Access to location data must be restricted to persons who in the course of exercising their duties may legitimately consult them

in the light of their purpose. All required user profile data are stored upon his/her mobile device and be securely protected. Relevant preferences relate to his/her diet, physical activities, dietary or transport/tourism related preferences, and, in general, simple everyday task preferences will not be stored locally. The user will have the capacity to view/hear, change or delete, as he/she wishes, all stored data by the system (including his/her profile data), with the help of a very simple and multimodal interaction (touch, buttons and voice input supported).

Types of data to be retained under categories identified in Article 4 of Directive 95/58 of 12th July, 2002. Specific safeguards—issues considered by the Article 29 working parties to be addressed with regard to the retention of data processed in connection with the provision of public electronic communication services (21st October 2005 opinion on the same subject directive proposal issued by the EU Commission on 21st September 2005). Reliable diagnosis requires state of the art monitoring and communication technologies providing real-time, accurate and continuous multi-parametric physiological measurements of the brain and the body, suited to the patient's medical condition and normal environment and facing issues of patient and data security, integrity and privacy.

The purpose of the FP7 projects “Advanced multi-parametric monitoring and analysis for diagnosis and optimal management of epilepsy and related brain disorders” (ARMOR) and StrokeBack is to manage and analyse large number of already acquired and new multimodal and advanced medical data from brain and body activities of epileptic patients and controls (MEG, multichannel EEG, video, ECG, GSR, EMG, etc.) aiming to design a holistic, personalized, medically efficient and affordable system for detecting abnormal condition and aid in efficient rehabilitation. New methods and tools have been already developed for multimodal data pre-processing and fusion of information from various sources. Novel approaches for large scale analysis (both real-time and offline) of multi-parametric streaming and archived data have been developed able to discover patterns and associations between external indicators and mental states, detect correlations among parallel observations, and identify vital signs changing significantly. Methods for automatically summarizing results and efficiently managing medical data are also being developed. The project incorporates models derived from data analysis based on already existing communication platform solutions emphasising on security and ethical issues and performing required adaptations to meet specifications.

ARMOR aims to provide flexible monitoring optimized for each patient and will be tested in several case studies and evaluated as a wide use ambulatory monitoring tool for seizures efficient diagnosis and management including possibilities for detecting premonitory signs and feedback to the patient. Therefore, our goal is to develop a personalized system that assists in diagnosis, prognosis and treatment of the disease. Such system should fulfil the following criteria; it should be non-invasive, mobile, continuous and unobtrusive, whereas all possible security and privacy aspects should be taken into account. Since access to large amounts of medical data is required for deriving all necessary models, a special effort is devoted to ensuring data anonymity, protection and restriction of access to private data in whole system.

The core system dealing with patient medical data in e Health related services and applications, like ARMOR, is the Electronic Health Record (EHR), defined as digitally stored health care information about individual's lifetime with the purpose of supporting continuity of care, education and research, and ensuring confidentiality at all times [27]. A patient's healthcare information may be spread out over a number of different institutes that do not interoperate. In order to provide continuity of care, clinicians should be able to capture the complete clinical history of the patient.

The Personal Health Record (PHR) is the electronic part of the health-related information of a person (such as diagnoses, medications, allergies, lab test results, immunization records but also administrative tasks such as appointment or prescription renewals) that can be extracted from multiple sources, but always under the control of the consumer, patient or informal caregiver.

This is the relevant difference between the PHR and the EHR or electronic medical record, which is maintained by the healthcare providers and payers. The EHR standardisation [2] aims to ensure that patient records are used to support shared care among clinicians with different specialisations, while enabling the mobility within and among countries for people who give and receive healthcare. Since EHR systems commonly store sensitive information of patients, Ethical and privacy regulations apply as defined in the ISO/TC 215 Technical Report: "Electronic Health Record Definition, Scope and Context" [3].

11.10.1 Practical Approach to the Use of PHR

The PHR platform developed internally by Intracom S. A. Telecom Solutions, name intLIFE, has been enhanced and geared to diverse health application through a number of FP7 funded research projects, such as ICT-PSP-NEXES, AAL-PAMAP, FP7-StrokeBack, FP7-ARMOR and others (Maharatna, Bonfiglio et al. 2013). Special adaptations made in ARMOR and StrokeBack have been geared to allow safe sharing of patients' clinical data with appropriate measures, as described earlier, for the protection of private data, ensuring controlled access to it while ensuring that any data distributed cannot be traced back to the person from whom the data has been taken from. This way the intLIFE system could be safely applied in ARMOR for the purpose of deriving clinical models build from large amount of data for subsequently allowing more reliable feature based clinical diagnosis on other patients and detection of conditions not possible earlier. In order to provide necessary privacy and security safeguards EHR/PHR, Vital Signs Monitoring and Management sub-systems are all connected via secure and encrypted interfaces controlled via authentication, authorisation and anonymizing modules.

The introduction of EHR/PHR systems is the response to the inherent problem of the medical community in dealing with growing amount of papers and printed type of medical records. This becomes also a matter of costs as much time and money is wasted on copying, faxing, and retrieving paper files. Move to electronically stored and managed patient records is both a simplification of the past problems, while

adding new ones. Hence, governments demand increasingly secure and standard-compliant health records (<http://www.ihtsdo.org/snomed-ct>). In today's world, it takes more than a simple document to meet national record keeping guidelines.

Electronic Health Records are an obvious solution to all emerging problems in the medical care, offering simplification of growing patient records, stimulates easier exchange of data among medical professionals, contributes to cutting costs of medical care as a whole. Records are accessible by multiple health providers. Subject to providing sufficient safeguards at every level, a complete security of data may be achieved. Through data encryption, password protection, the electronic health record offers a peace of mind that data is kept away from unauthorised eyes. Nevertheless, although the future of e-Health has never looked so bright, there are still several concerns that needs careful attention.

Growth of e-health systems inherently implies that any patient's data may be stored not in one place, but on several diverse systems implying increased risk of leaking information to unauthorised third parties. Cyber security procedures are also not consistent across various systems, implying that some may be easier to break into and increasing vulnerability of data stored there.

What adds to the problem is lack of seamless interoperability among e-health systems based on electronic records. Since early stages of development of HL7 standard, now one of the base reference standards for e-health, it was considered only as a set of guidelines and not a factual standard to follow. This has resulted in systems being built and deployed that had implemented only a part of the HL7 specification (www.hl7.org) suited to particular needs of a given service provider. Interoperability among such restricted systems is a tiresome process, resulting in exchanging in-complete information.

This deficiency has been recently recognised as critical for future e-health and the HL7 is being evolved to define the base set of interoperability criteria for ensuring smooth collaboration among different health systems. However, this process is still ongoing and requires much more research work, including interoperability at the device level and especially for mobile physiological monitoring. In conclusion we can observe a dramatic changes in the e-health do-main with the introduction of electronic health records, boosting the efficiency of medical services at a lower cost, at the same time offering still a vast range of re-search challenges that we may expect to be pursued and hopefully resolved in the near future.

11.10.2 Seamless Authentication and Authorisation

Authentication and authorisation are two main means for allowing access for the user to a resource. Authentication involves such issues like identifying the user by means of either a simple login/password check to elaborate biometric analysis involving fingerprints, retina scans, and voice and/or face recognition etc. Authorisation then performs checks whether a given user may be granted access to a given resource or not. Such processes have been part of any secure system from the beginning of computing systems. Their complication has increased recently

with the rapid growth of the amount of information resources and number of user accounts in each system, platform and/or network. This increases network administrators' work on properly securing their network and databases against un-authorized access at the same time providing users' with uninterrupted access to resources that they should be authorized to access.

However, currently employed methods for performing authentication and authorization, in most cases, require user authentication every time he moves between resources stored on differently protected sites causing annoyance and loss of time. On the other hand approach to authorizing users based on user-resource association requires tedious administrators' job to properly secure access to different resources and gives rise to frequent faults when users are either authorized to access resources that they should not have access to or not being able to access those that they should be able to.

This problem has been identified and addressed in almost all the systems since very long time. Administrators are offered means for specifying access rights per user group, policy definition mechanisms and macros allowing them to simplify management of access right to both existing and new users. Despite the fact that these tools are used the problems of authentication and authorization still contain loop holes attributed mostly to human errors than to machine security as such. Our proposed seamless authentication and authorization is aimed to simplify further the process of securing access to multiple-interconnected systems as well as making authorization less prompt to faults.

Authentication is the process of authenticating a user across multiple account protected resources and platforms, i.e. agreeing between different authentication authorities means of establishing trust relationships and dependability for transferring users authentication status i.e. checking that a user is who they claim to be. The process will include customisation of means of authentication whereby users will not be required to perform authentication while transferring from one trusted party to another using single authentication. In case of moving from a party with lower authentication requirements to one requiring higher level of authentication, user will only be required to perform extra security checks while accessing differently protected resources instead of performing the whole authentication process from the beginning. Approaches like this have been already proposed, most known being Windows Passport where user may move between sites that support this technology. However, such methods do not take into account differences between authentication means required by different sites. This limits applicability of technologies to social WEB sites aiming to keep a record of users accessing their services.

Authorization in computer terms refers to granting access to a resource to a given user. In most computer systems granting access is related to belonging to a specific user group meant to allowing administrators defining single access rights rules for a group of users. However, this makes it very difficult when it comes to more per-user access granting, especially in systems with large number of user accounts. What we propose is to unify and simplify means of granting user access to given resources. The process will define sets of resource authorization dependencies whereby access to one resource may be implicitly granted upon prior-assigned access rights to another resource.

This will allow removing the need for the security administrator to provide access rights to every user to every resource, instead concentrating on defining security interdependencies between resources and defining user access right only to key global resources. Note, that this will not remove a possibility to explicitly grant or block access to a given resource to a given user, if required.

11.11 Conclusions and Potential for Future Research

The introduction of EHR/PHR systems is the response to the inherent problem of the medical community in dealing with growing amount of papers and printed type of medical records. This becomes also a matter of costs as much time and money is wasted on copying, faxing, and retrieving paper files. Movement to electronically stored and managed patient records is both a simplification of the past problems, while adding new ones. Reduction of paper records helps in simplifying records and eases exchange of data, though electronic communication implies stronger focus on preventing access to such data. Hence, governments demand increasingly secure and standard-compliant health records. In today's world, it takes more than a simple document to meet national record keeping guidelines. And an increasing number of optional treatments must easily fit into today's recordkeeping systems, complicating matters even further.

Electronic Health Records are an obvious solution to all emerging problems in the medical care, offering simplification of growing patient records, stimulates easier exchange of data among medical professionals, contributes to cutting costs of medical care as a whole. Records are accessible by multiple health providers. They are also fully integrated with other office functions, and interfaces with multiple vendors and diagnostic equipment, allowing for e.g. easy storage or X-ray, MRI, and other images in a standardised way. Subject to providing sufficient safeguards at every level, a complete security of data may be achieved.

Through data encryption, password protection, the electronic health record offers a peace of mind that data is kept away from unauthorised eyes. Nevertheless, although the future of e-Health has never looked so bright, there are still several concerns that needs careful attention. Growth of e-health systems inherently implies that any patient's data may be stored not in one place, but on several diverse systems implying increased risk of leaking information to unauthorised third parties. The cyber security procedures are also not consistent across various systems, implying that some of them may be easier broke into and increasing vulnerability of data stored.

What adds to the problem is lack of seamless interoperability among e-health systems based on electronic records. Since early stages of development of HL7 standard, now one of the base reference standards for e-health, it was considered only as a set of guidelines and not a factual standard to follow. This has resulted in systems being built and deployed that had implemented only a part of the HL7 specification suited to particular needs of a given service provider. Interoperability among such restricted systems is a tiresome process, resulting in exchanging

incomplete information. This deficiency has been recently recognised as critical for future e-health and the HL7 is being evolved to define the base set of interoperability criteria for ensuring smooth collaboration among different health systems.

However, this process is still ongoing and requires much more research work, including interoperability at the device level and especially for mobile physiological monitoring. In conclusion we can observe a dramatic changes in the e-health domain with the introduction of electronic health records, boosting the efficiency of medical services at a lower cost, at the same time offering still a vast range of research challenges that we may expect to be pursued and hopefully resolved in the near future.

References

1. Kibbe D, Phillips R, Green L (2004) The continuity of care record. *Am Fam Physician* 70:1220–1223
2. Kevin H (2008) Standards for PHRs: Are PHRs ready for standards? Are standards ready for PHRs? *J AHIMA* 79(6):31–36
3. ISO/TC 215 Technical report: electronic health record definition, scope and context, 2nd draft, Aug 2003
4. HL7 (2004) HL7 EHR system functional model: a major development towards consensus on electronic health record system functionality. White Paper. <http://www.hl7.org/ehr>
5. Detmer D, Bloomrosen M et al (2008) Integrated personal health records: transformative tools for consumer centric care. *BMC Med Inform Decis Mak* 8:45
6. CEN/TC-251–ISO/TC-215, I. E. Electronic Healthcare Record (EHR) Communication (2010) Parts 1: reference model, part 2: archetype model, part 3: reference archetypes and term lists, part 4: security and part 5: interface specification
7. Muñoz P et al (2011) The ISO/EN 13606 standard for interoperable exchange of electronic health records. *J Healthc Eng* 2(1):1–24
8. Eichelberg M, Aden T, Riesmeier J, Dogac A, Laleci G (2005) A survey and analysis of electronic healthcare record standards. *ACM Comput Surv* 37(4):277–315
9. Schloeffel P, Beale T et al (2006) The relationship between CEN 13606, HL7, and OpenEHR. Health Informatics Conference
10. Beale T, Heard S, Kalra D, Lloyd D (2007) The openEHR reference model: EHR information model. openEHR Foundation
11. Ferranti JM, Musser RC, Kawamoto K, Hammond WE (2006) The clinical document architecture and the continuity of care record. *J Am Med Inform Assoc* 13(3):245
12. Dolin R et al (2006) HL7 clinical document architecture, release 2. *J Am Med Inform Assoc* 13:30–39
13. Rector A et al (1993) A framework for modelling the electronic medical record. *Methods Inf Med* 32:109–119
14. Johnson S (1996) Generic data modelling for clinical repositories. *J Am Med Inform Assoc* 3:328–339
15. Beale T (2002) Archetypes constraint-based domain models for future-proof information systems. In: OOPSLA-2002 workshop on behavioural semantics, Seattle, WA
16. Goossen W, Goossen-Baremans A et al (2010) Detailed clinical models: a review. *Healthc Inform Res* 16(4):201
17. ASTM International—A century of progress (2005) ASTM international. http://www.astm.org/IMAGES03/Century_of_Progress.pdf
18. McCay C, Kalra D, Worden R (2008) Results of investigating the transformability between HL7 V3, openEHR and EN/ISO 13606. NHS Connecting for Health, Leeds

19. Sundvall E et al (2008) Integration of tools for binding archetypes to SNOMED CT. *BMC Med Inform Decis Mak* 8(Suppl 1):S7
20. Qamar R, Rector A (2007) Semantic issues in integrating data from different models to achieve data interoperability. *Stud Health Technol Inform* 129(Pt 1):674–678
21. European Commission (2007) eHealth priorities and strategies in European countries: eHealth ERA report
22. Maharatna K, Bonfiglio S (2013) Next-generation remote healthcare: a practical system design perspective. In: Artur K, Emmanouela V et al (eds) *Patient health record (PHR) system*. Springer, New York. ISBN 978-1-4614-8842-2
23. Emmanouela V, Krukowski A (2014) Serious games for stroke rehabilitation employing immersive user interfaces in 3D virtual environment. *J Health Inform* 6:105–113, ISSN 2175-4411
24. Kim M, Johnson K (2002) Personal health records: evaluation of functionality and utility. *J Am Med Inform Assoc* 9(2):171–180. doi:[10.1197/jamia.M0978](https://doi.org/10.1197/jamia.M0978), PMC 344574. PMID 11861632
25. Rindfleisch TC (2007) Privacy, information technology and health care. *Commun ACM* 40(8):92–100
26. Ball MJ, Gold J (2006) Banking on health: personal records and information exchange. *J Healthc Inf Manag* 20(2):71–83, PMID 16669591
27. Krukowski A, Charalambides M, Chouchoulis M (2014) Supporting medical research on chronic diseases using integrated health monitoring platform. 4th International Conference on Wireless Mobile Communication and Healthcare—“Transforming healthcare through innovations in mobile and wireless technologies”, special session on “eHealth@Home-Infrastructure and services for remote multi-parametric monitoring, analysis and support”, Athens, Greece, 3–5 Nov 2014
28. Beale T, Heard S (2008) openEHR architecture overview. openEHR Foundation