



European Commission – DG Information Society



European Quality Labelling and Certification
of Electronic Health Record systems

Q-REC

WP3

**Inventory of Relevant Standards for EHR
Systems**

COVER AND CONTROL PAGE OF DOCUMENT	
Project number:	IST-27370-SSA
Project name:	Q-REC
Document id:	
Document name:	Inventory of Relevant Standards for EHR Systems
Document type (PU, INT, RE)	PU
Version:	0.8
Date:	10. January 2007
Author(s):	Bernd Blobel
Organisation:	ProRec Germany, eHealth Competence Center University of Regensburg Medical Center
Address:	Franz-Josef-Strauss-Allee 11, D-93042 Regensburg, Germany

Document type PU = public, INT = internal, RE = restricted

Table of Content

1. Introduction	6
2. Scope and Mission of the Deliverable.....	7
3. Standards Classification Health Informatics	8
4. Standards Developing Organisations	9
4.1. International Organisations	9
4.1.1. IEEE	9
4.1.2. ISO	9
4.1.3. ISO TC 215 Health Informatics	10
4.1.4. HL7	10
4.1.5. DICOM.....	11
4.1.6. IEC	12
4.1.7. IHE	12
4.1.8. OASIS	13
4.1.9. IHC.....	13
4.1.10. OMG	14
4.1.11. UN / CEFACT.....	14
4.1.12. W3C	14
4.1.13. ITU	15
4.1.14. ITU-T	16
4.2. European Organisations.....	16
4.2.1. CEN.....	16
4.2.2. CEN TC 251 Health Informatics	17
4.2.3. CEN / ISSS.....	17
4.2.4. CEN / ISSS eHealth Standardization Focus Group.....	18
4.2.5. ETSI	18
4.2.6. IHE Europe.....	19
4.2.7. CENELEC.....	19
4.3. National Activities to Be Considered.....	19
4.3.1. ANSI	20
4.3.2. ASTM.....	20
4.3.3. NEMA.....	20
4.4. Other Organisations and Initiatives.....	21
4.4.1. Certificate Commission for Healthcare Information Technology	21
5. Standards and Publicly Available Specifications	22
5.1. Domain-Independent Specifications.....	22
5.2. Domain-Specific Specifications.....	22
5.3. General Specifications	22
5.4. Application-Related Specifications.....	23
5.5. Infrastructural Specifications	23
5.5.1. Tokens	23
5.5.2. ID Management.....	23
5.5.3. Privacy Standards	23

5.6.	Requirements and Analysis Standards	24
5.7.	Architecture Standards	26
5.8.	Modelling and Methodology Standards	27
5.9.	Communication Standards.....	42
5.10.	Infrastructure Standards	60
5.11.	Privacy Standards	65
5.12.	Safety Standards	70
5.13.	Token Standards	73
5.14.	Quality Standards	77
5.15.	Policy Standards.....	82
5.16.	Terminology and Ontology Standards.....	82
5.17.	ID Management Security Standards	91
6.	<i>Conclusions</i>.....	94
7.	<i>References</i>	95

Table of Content

Table 1: Requirements and Analysis Standards Overview	24
Table 2: List of Architecture Standards	26
Table 3: List of Modelling and Methodology Standards	27
Table 4: List of Communication Standards	42
Table 5: List of Infrastructure Standards	60
Table 6: List of Privacy Standards	65
Table 7: List of Safety Standards	70
Table 8: List of Token Standards	73
Table 9: List of Quality Standards	77
Table 10: List of Policy Standards	82
Table 11: List of Terminology and Ontology Standards	83
Table 12: List of ID Management Standards related to Security	91

Inventory of Relevant Standards for EHR Systems

1. Introduction

According to ISO/TR 20514 [1], there are four prerequisites for EHR semantic interoperability: i) agreement on a standardized reference model, ii) standardized service interface models to provide interoperability between the health services and other services such as demographics, terminology, access control and security services iii) a standardized set of domain-specific concept models, e.g. archetypes and templates for clinical, demographic, and other domain-specific concepts, and iv) standardized terminologies associated with controlled vocabularies.

These requirements only concern informational aspects of EHR systems, however. In a more comprehensive view, communication and co-operation between different health information systems (including EHR systems) and their components in a complex and highly dynamic environment also requires [2]:

- Openness, scalability, flexibility, portability,
- Distribution at internet level,
- Standard conformance,
- Service-oriented semantic interoperability,
- Consideration of timing aspects of data and information exchanged,
- User acceptance,
- Appropriate security and privacy services.

For achieving the aforementioned characteristics, the health information systems development process (requirement analysis, design, implementation, evaluation, use, and maintenance) has to meet the following paradigms:

- Architecture focus,
- Distribution, component-orientation (flexibility, scalability, reusability),
- Model-driven and service-oriented design (manageability, user acceptance),
- Separation of platform-independent and platform-specific modelling, i.e. separation of logical and technological views (portability),
- Specification of reference and domain models at meta-level (semantic interoperability),
- Interoperability at service level, considering concepts, contexts, knowledge (semantic interoperability, user acceptance),
- Common terminology and ontology (semantic interoperability),
- Advanced security, safety and privacy services (user acceptance).

Because of complex requirements, semantically interoperable EHR systems and components can only be developed by meeting the different paradigms within a unified development process.

2. Scope and Mission of the Deliverable

Considering an EHR system as core application for any health information system, health telematics or even eHealth platform, the characteristics for sustainable health information systems or eHealth applications have to be applied to EHR systems such as

Component-oriented

Architecture-centric

Model-driven architecture

Reference models for information and businesses

Reference terminologies and ontologies

Advanced security and privacy services including ID management

Policy-driven

Semantically interoperable

Service-oriented

Therefore, architecture standards, modelling standards, terminology standards, ontology standards, classification systems and standards, identifier and ID management standards, standards for communication security, standards for application security, privacy standards, standards for infrastructural services, communication protocol standards, standards for formal languages, development process standards, etc. are directly or indirectly related to EHR, EHR systems and EHR architectures.

Because of its centrefold position, the EHR must be able to manage any type of information related to the EHR subject (patient/person) independent of the format, media, protocol, domain terminology, domain ontology, etc. This implies the need for multimedia device communication with an EHR system. Therefore, this Deliverable also deals with standards in an EHR environment, i.e. systems, processes, services, mechanisms, and transactions happening in connection to an EHR or an EHR system.

3. Standards Classification Health Informatics

As it became clear, security services as specialised systems' properties or as services embedded in systems mainly aiming other functionalities have to be described by running through the entire system lifecycle. Therefore, all different specification describing a system, i.e. its architecture, its informational aspects, its computational aggregations, engineering aspects of its implementation or even technical aspects of running the system including education and training of the user community have to be described and managed properly. Therefore, architecture standards, modelling standards, communication standards, infrastructure standards, privacy standards, safety standards, quality standards, and terminology and ontology standards have to be followed. Following, standards directly or indirectly related to security aspects of systems are classified into the aforementioned categories.

- Architecture standards
 - HL7 versions 2.x/3, CORBA, MDA, HISA
- Modelling standards
 - UML, CEN 15300: "CEN Report: Framework for formal modelling of healthcare security policies"
- Communication standards
 - CEN 13608: "Security for healthcare communication", CEN 13606: "Electronic healthcare record communication"
- Infrastructure standards
 - ISO 17090: "Public key infrastructure", ETSI TS 101733: "Electronic Signature Formats"
- Privacy standards
 - ASTM E1987-98: "Standard guide for individual rights regarding health information", CEN 13729: "Secure user identification - Strong authentication using microprocessor cards"; ISO/IEC PDS Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services
- Safety standards
 - CEN 13694: "CEN Report: Safety and security related software quality standards for healthcare"; ISO/DTS 25238 Classification of Safety Risks
- Quality standards
 - ISO 9000:
- Terminology and ontology standards
 - UMLS, SNOMED
- Identifier and identification schemes
 - LOINC, ASTM E1714-00: "Standard guide for properties of a Universal Healthcare Identifier"

4. Standards Developing Organisations

In the following chapter, some of the important organisations for standardisation world-wide will be shortly introduced. Most of the information provided in the following has been taken from the official SDO member information in case, EuroRec members or Q-REC partners take actively part in the work of the respective organisation. In regard in this report, the author is actively involved in, and formally affiliated to, the following SDOs: ISO, CEN, ETSI, HL7, IHE, OASIS, CORBA/OMG, ASTM, DIN, and IETF. In other cases, information is taken from the official web pages of the organisations.

4.1. International Organisations

As markets grow and borders get opened, the potential of EuroRec/Q-REC lays even beyond Europe. In some countries, international standards range first, followed by national ones. From this viewpoint, also international Standards Developing Organisations have to be considered important for the project related work. In the next paragraphs, relevant European SDO will therefore be introduced shortly.

4.1.1.IEEE

The Institute of Electrical and Electronics Engineers (IEEE) resulted from the merging in 1963 of the AIEE (American Institute of Electrical Engineers) and the IRE (Institute of Radio Engineers). Through its predecessors it dates back to 1884. AIEE, addressed wire communications, light and power systems, while IRE, itself resulting from the merging of two largely local organisations (the Society of Wireless and Telegraph Engineers and the Wireless Institute), addressed wireless communications. IEEE has undertaken standardisation activities in the United States via its subsidiary, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), which develops industry standards in a broad-range of industries, including Biomedical and Health care. Collaboration exists between IEEE, CEN TC 251 and ISO TC 215. Working with ISO TC 215, and in accordance with the ISO/IEEE “Pilot Project”, international representatives can participate in ballots via ‘international co-ordination’. The votes are not binding (i.e. they are not counted in the final tally that determines the result of the ballot). A large suite of standards has been developed and published jointly by IEEE, CEN and ISO, respectively.

4.1.2.ISO

The International Organization for Standardization (ISO) is a network of the national standards institutes of 156 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO's principal activity is the development of technical standards.

ISO collaborates with its partners in international standardisation, like the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU-T), particularly in the field of information and communication technology. They have established the World Standards Cooperation (WSC) as the focus for their combined strategic activity. Moreover, ISO has a strategic partnership with the World Trade Organization (WTO) aiming to

promote a free and fair global trading system. Signatories to the WTO Agreement on Technical Barriers to Trade (TBT) commit themselves to promoting and using international standards of the type developed by ISO. ISO cooperates closely with most of the specialized agencies and bodies of the United Nations that are involved in technical harmonization and assistance to developing countries.

New growth areas for ISO standards in the coming years include the environment with standards for meeting new requirements such as sustainable development, the service sectors with standards already being developed for social research and tourism; health and safety, security, good managerial and organisational practice and guidelines ISO is developing on social responsibility. In addition, ISO is well placed to provide voluntary standards for formerly regulated areas such as energy, water supply or transportation.

4.1.3.ISO TC 215 Health Informatics

The Technical Committee TC 215 Health Informatics of ISO was created in 1998. Its scope is defined as the standardisation in the field of information for health, health information and communications technology to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications), and to reduce duplication of effort and redundancies. The number of participating countries is now 25, with 14 observer countries. In 2004, the total number of ISO standards published under the direct responsibility of ISO TC 215 is 14. ISO TC 215 liaises with several other organisations like CEN, DICOM, ICN, IMIA, UN/ECE, W3C, etc. Until 2005, the work of ISO TC 215 is distributed between 6 Working Groups: WG 1 Health records and modelling co-ordination; WG 2 Messaging and communication; WG 3 Health concept representation; WG 4 Security; WG 5 Health cards, and WG 6 Pharmacy and medication business. In 2005, TC 215 created two new Working groups. WG 7 deals with medical devices whereas WG 8 intends to define business models for Electronic Health record (EHR) systems.

4.1.4.HL7

HL7 (Health Level Seven, by reference to the 7 layers of the OSI model) was founded in 1987 by several vendors of software for the health care industry. Their main goal was to develop messages consensual formats to facilitate a better interoperability of Hospital Information Systems (HIS). In 1994, HL7 was officially accredited by ANSI, the American National Standards Institute, as a Standards Developing Organisation (SDO), meaning that HL7 approved specifications are channelled into the official standardisation process. HL7 Message specification ('HL7 standard') version 1.0 was approved in 1987, and was followed by version 2.0 in 1998. Subsequently, version 2 evolved regularly. It still forms the basis for the many HIS systems implemented in the USA and several European countries. An XML-based 'Clinical Document Architecture' (it's a document structure rather than an architecture) set of specifications was approved in 2000 (release 1). The planned successive releases of the CDA will in turn provide specifications to exchange increasingly structured clinical documents. Release 2 is published, and release 3 is in preparation. The CDA is meant to be used together with version 2, as well as with future messages version, and it is included in the HL7 RIM (Reference Information Model). Various other complementary works have also been approved and published over the years.

HL7 version 3 specifications use a formal Message Development Framework (MDF) methodology, using the RIM, to help make messages more consistently implemented than they are for version 2. Current contributors or 'Benefactors' to HL7 include vendors (Siemens, GE Medical Systems, HBOC-McKesson, IBM, Oracle, Microsoft, Philips), USA or non-USA agencies (USA Veterans Affairs), UK NHS, Centres for Disease Control and Prevention (USA CDC), Standards Australia, AFNOR (France). Public-private partnerships have also been established with Infoway (Canada), NICTIZ (The Netherlands). Other 'benefactors' include, amongst others, USA healthcare providers or health insurance funds, such as Mayo Fdn, Duke, and Kaiser Permanente. HL7 has 26 International Affiliates: Argentina, Australia, Brazil, Canada, China, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, India, Ireland, Italy, Japan, Korea, Lithuania, Mexico, New Zealand, Poland, Spain, South Africa, Switzerland, Taiwan, The Netherlands, and the United Kingdom. HL7/USA is said to be under consideration

4.1.5.DICOM

Founded in 1983 by the American College of Radiologists (ACR) and the National Electronic Manufacturers' Association (NEMA), the Digital Imaging and Communications in Medicine (DICOM) Standards Committee is acting as an internationally acknowledged SDO. It is now administered by the Diagnostic Imaging and Therapy Systems Division of NEMA in the USA with a solid European representation and participation of users as well as manufacturers (COCIR members).

Digital medical image sources, and the use of computers to process them after their acquisition, were introduced in the seventies. In 1983 ACR and NEMA formed a joint committee in order to standardize a method for the transmission of medical images and their associated information. In 1985 this committee published the ACR-NEMA Standards Publication No. 300-1985. Version 2.0 was published in 1988. In 1993 version 3.0 marked a major step towards a standard method of communicating digital image information. It also introduced the name DICOM. Since its origin, DICOM has paid much attention to establishing working relationships with other related standard initiatives throughout the world: 1 ASTM for its initial version; 2 the Internet protocol TCP/IP in 1993; 3 CEN in the nineties (this solid co-operation resulting in a number of jointly developed supplements); 4 JIRA (the Japan Industries Association of Radiological Systems) for the convergence of a Japanese interchange media format with DICOM; 5 ANSI-HISBB in the USA, from which DICOM adopted a harmonized patient name structure; 6 HL7 resulting in the creation of a joint DICOM-HL7 working group in 1999; 7 ISO TC 215, with which a Type A liaison has been established in 1999, shortly after its creation. ISO TC 215 is not creating a working group for bio-medical imaging standards, but is relying instead on DICOM.

DICOM has 22 Working Groups: WG-01 Cardiac and Vascular Information, WG-12 Ultrasound, WG-02 Projection Radiography and Angiography, WG-13 Visible Light, WG-03 Nuclear Medicine, WG-14 Security, WG-04 Compression, WG-15 Digital Mammography and CAD, WG-05 Exchange Media, WG-16 Magnetic Resonance, WG-06 Base Standard, WG-17 3D, WG-07 Radiotherapy, WG-18 Clinical Trials and Education, WG-08 Structured Reporting, WG-19 Dermatologic Standards, WG-09 Ophthalmology, WG-20 Integration of Imaging and Information Systems, WG-10 Strategic Advisory, WG-21 Computed Tomography, WG-11

Display Function Standard, WG-22 Dentistry. The current priorities for DICOM are issues relating to security, performance, new modality technology, and workflow management.

4.1.6.IEC

The International Electrotechnical Commission (IEC) is the leading global organisation that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardisation and as references when drafting international tenders and contracts.

Through its members, the IEC promotes international cooperation on all questions of electro-technical standardisation and related matters, such as the assessment of conformity to standards, in the fields of electricity, electronics and related technologies. The IEC charter embraces all electrotechnologies including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines such as terminology and symbols; electromagnetic compatibility; measurement and performance: dependability; design and development; security, safety and the environment.

IEC's international standards facilitate world trade by removing technical barriers to trade, leading to new markets and economic growth. Put simply, a component or system manufactured to IEC standards and manufactured in one country can be sold and used in other countries.

IEC's standards are vital since they also represent the core of the World Trade Organization's Agreement on Technical Barriers to Trade (TBT), whose 100-plus central government members explicitly recognize that international standards play a critical role in improving industrial efficiency and developing world trade. The number of standardisation bodies which have accepted the Code of Good Practice for the Preparation, Adoption and Application of Standards presented in Annex 3 to the WTO's TBT Agreement underlines the global importance and reach of this accord.

IEC standards provide industry and users with the framework for economies of design, greater product and service quality, more inter-operability, and better production and delivery efficiency. At the same time, IEC's standards also encourage an improved quality of life by contributing to safety, human health and the protection of the environment.

4.1.7.IHE

The goal of the Integrating the Healthcare Enterprise (IHE) initiative is to stimulate integration of healthcare information resources to improve clinical care. IHE develops and publishes detailed frameworks for implementing established data standards to meet specific healthcare needs and supports testing, demonstration and educational activities to promote the deployment of these frameworks by vendors and users.

IHE is an initiative by health care professionals and industry to improve the way computer systems in health care share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal

patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively.

Optimal patient care requires efficient access to comprehensive electronic health records (EHR). IHE accelerates the adoption of the information standards needed to support EHR. More than 100 vendors have implemented and tested products based on IHE. IHE improves patient care by harmonizing healthcare information exchange and provides a common standards-based framework for seamlessly passing health information among care providers, enabling local, regional and national health information networks.

IHE enhances the quality of patient care, resulting in benefits for safety through the reduction of medical errors, for savings through lower implementation costs and more efficient workflow, for satisfaction through better informed medical decisions and faster results for both patient and physician

4.1.8.OASIS

Driving the development, convergence, and adoption of e-business standards, OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. The consortium produces more Web services standards than any other organisation along with standards for security, e-business, and standardisation efforts in the public sector and for application-specific markets. Founded in 1993, OASIS has more than 5,000 participants representing over 600 organisations and individual members in 100 countries.

OASIS is distinguished by its transparent governance and operating procedures. Members themselves set the OASIS technical agenda, using a lightweight process expressly designed to promote industry consensus and unite disparate efforts. Completed work is ratified by open ballot. Governance is accountable and unrestricted. Officers of both the OASIS Board of Directors and Technical Advisory Board are chosen by democratic election to serve two-year terms. Consortium leadership is based on individual merit and is not tied to financial contribution, corporate standing, or special appointment.

4.1.9.IHC

IHC is the OASIS International Health Consortium. The IHC Technical Committee aims at providing a forum for the global healthcare community to articulate and coordinate requirements for XML- and Web services-based standards.

The scope of the committee's work will include the use of OASIS and other standards (both health care and non-health care related) for interoperability utilizing web services as practical. There is a clear use case for many of the HL7 standards which are clearly healthcare related, but there are also compelling reasons to adopt and recommend other procedures and guidelines for the standardisation of administrative, and potentially clinical, processes.

The IHE committees do not anticipate the development of standards in the committee unless it becomes clear that there are deficiencies in the existing vertical standards or clear voids in required interoperability across the horizontal interoperability channels. Therefore, the initial

scope of the TC is only to assess the state of Web Services within the healthcare industry, gather requirements for work needed to be done, and only in exceptional cases develop standards.

4.1.10. OMG

OMG is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications. OMG membership includes virtually every large company in the computer industry, and hundreds of smaller ones. Most of the companies that shape enterprise and Internet computing today are represented on OMG Board of Directors. Its flagship specification is the multi-platform Model Driven Architecture (MDA), recently underway but already well known. It is based on the modelling specifications the MOF, the UML, XMI, and CWM. OMG's own middleware platform is CORBA, which includes the Interface Definition Language OMG IDL, and protocol IIOP.

4.1.11. UN / CEFACT

The UN / CEFACT is the United Nations Centre for Trade Facilitation and Electronic Business. It is the organisation responsible for the standardisation of syntax in the field of EDI, as well as for the Electronic Business XML (ebXML) initiative. The European CEN / ISSS is the “European Entry Point” to the UN / CEFACT process. The EDIFACT standard is still widely used. UN / CEFACT has published the Core Components Technical Specification, as part of the overall ebXML framework, drawn up by a UN / CEFACT-OASIS joint initiative discussed in section 11.8.1 below. This specification is meant to be employed wherever business information is being shared or exchanged amongst and between enterprises, governmental agencies, and/or other organisations in an open and worldwide environment. This interoperability enabling specification covers both interactive and batch exchanges of business data between applications through the use of Internet and Web based information exchanges as well as traditional Electronic Data Interchange (EDI) systems. The specification focuses both on human-readable and machine-processable representations of this information. It represents a methodology for developing a common set of semantic building blocks that represent the general types of business data in use today, and provides for the creation of new business vocabularies and restructuring of existing business vocabularies. This specification should form the basis for standards development work of business analysts, business users and information technology specialists supplying the content of and implementing applications that will employ the UN / CEFACT Core Component Library (CCL). The Core Component Library will be stored in a UN / CEFACT repository and identified in an ebXML compliant registry.

4.1.12. W3C

The World Wide Web Consortium (W3C) is an international consortium where Member organisations, a full-time staff, and the public work together to develop Web standards. W3C's mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web.

W3C's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions. W3C is the chief standards body for HTTP, HTML and XML. W3C primarily pursues its mission through the creation of Web standards and

guidelines. Since 1994, W3C has published more than ninety such standards, called W3C Recommendations. W3C also engages in education and outreach, develops software, and serves as an open forum for discussion about the Web. In order for the Web to reach its full potential, the most fundamental Web technologies must be compatible with one another and allow any hardware and software used to access the Web to work together. W3C refers to this goal as Web interoperability. By publishing open (non-proprietary) standards for Web languages and protocols, W3C seeks to avoid market fragmentation and thus Web fragmentation.

Organisations located all over the world and involved in many different fields join W3C to participate in a vendor-neutral forum for the creation of Web standards. W3C Members and a dedicated full-time staff of technical experts have earned W3C international recognition for its contributions to the Web. The W3C Members (e.g. sample testimonials), the W3C staff and Invited experts work together to design technologies to ensure that the Web will continue to thrive in the future, accommodating the growing diversity of people, hardware, and software.

W3C's global initiatives also include nurturing liaisons with national, regional and international organisations around the globe. These contacts help W3C maintain a culture of global participation in the development of the World Wide Web. W3C coordinates particularly closely with other organisations that are developing standards for the Web or Internet in order to enable clear progress.

4.1.13. ITU

The International Telecommunication Union (ITU) was established last century as an impartial, international organisation within which governments and the private sector could work together to co-ordinate the operation of telecommunication networks and services and advance the development of communications technology. Whilst the organisation itself remains relatively unknown to the general public, ITU's work over more than one hundred years has helped create a global communications network which now integrates a huge range of technologies, yet remains one of the most reliable man-made systems ever developed.

As the use of telecommunication technology and radio-communication-based systems spreads to encompass an ever-wider range of activities, the vital work carried out by ITU is taking on growing importance in the day-to-day lives of people all around the world.

The Union's standardisation activities, which have already helped foster the growth of new technologies such as mobile telephony and the Internet, are now being put to use in defining the building blocks of the emerging global information infrastructure, and designing advanced multimedia systems which deftly handle a mix of voice, data, audio and video signals. Meanwhile, ITU's continuing role in managing the radio-frequency spectrum ensures that radio-based systems like cellular phones and pagers, aircraft and maritime navigation systems, scientific research stations, satellite communication systems and radio and television broadcasting all continue to function smoothly and provide reliable wireless services to the world's inhabitants.

Finally, ITU's increasingly important role as a catalyst for forging development partnerships between government and private industry is helping bring about rapid improvements in telecommunication infrastructure in the world's under-developed economies.

Whether in telecommunication development, standards-setting or spectrum sharing, ITU's consensus-building approach helps governments and the telecommunication industries confront and deal with a broad range of issues which would be difficult to resolve bilaterally. The result is real-life, workable agreements which benefit not only the telecommunication industry as a whole but, ultimately, telecommunication users everywhere.

4.1.14. ITU-T

The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the International Telecommunication Union. ITU-T's mission is to ensure an efficient and on-time production of high quality standards (recommendations) covering all fields of telecommunications.

ITU-T was created on 1 March 1993, replacing the former International Telegraph and Telephone Consultative Committee (CCITT) whose origins go back to 1865. The public and the private sectors cooperate within ITU-T for the development of standards that benefit telecommunication users worldwide. Standardisation work is carried out by ITU-T Study Groups in which representatives of the ITU-T membership develop recommendations (standards) for the various fields of international telecommunications.

4.2. European Organisations

For a European institution like the EuroRec Institute and a European project like Q-REC as well as for participating organisations with a potential market in Europe, the European standardisation is a major basis for success. It is important to note that European standardisation can be performed on different levels. European Reports are tentative and describe requirements and possible strategies for solutions. European pre-standards formerly called ENV (now known as Technical Specifications) are only valid for three years before they need to be revised. They do not override national documents dealing with similar subjects. Therefore, they were regarded as purely indicative, and without any constraining value. Conversely, full European standards are systematically incorporated within the corpus of national standards of Member States, and they definitely supersede any similar work taking place at the national level. In the next paragraphs, relevant European SDO will therefore be introduced shortly.

4.2.1. CEN

CEN, the European Committee for Standardisation, was founded in 1961 by the existing national standards bodies in the European Economic Community (EEC) and the EFTA countries. CEN is contributing to the objectives of the European Union and the European Economic Area with voluntary technical standards which promote free trade, the safety of workers and consumers, safety and security, protection of individuals and data, health care and welfare, interoperability of networks, environmental protection, exploitation of research and development programmes, and public procurement.

4.2.2.CEN TC 251 Health Informatics

CEN TC 251 is the sectoral Technical Committee of CEN for Health Informatics. It was instituted in 1990 with the first immediate aim of transferring into the corpus of European standards the biggest possible part of the technical specifications resulting from Health Telematics "pre-competitive" projects co-funded by the European Commission former DG-XIII (now DG-INFOS) through the successive Framework Programmes for Research and Development, or at least those that remained in the public domain. Subsequently CEN TC 251 addressed a variety of other relevant work items. To date, CEN TC 251 has produced over 50 technical documents (standards, pre-standards, and reports). During the first phase, CEN TC 251 produced no full standard, but a series of pre-standards and reports. The resulting flow of publications reached: 25 pre-standards (including 2 multi part) and 4 CEN reports. Later, with the revision of these pre-standards, full standards began to emerge. In a second phase, CEN TC 251 has addressed entirely new issues responding to new needs appearing due to the starting implementation of computerized information systems in the domain of health care. During that second phase, however, 1 standard, 12 pre-standards (including 6 multi-part), and 4 CEN Reports have been published so far.

Until 1997, the work items addressed were spread between 7 working groups, then reduced to just 4: WG-I Information Models; WG-II Terminology and knowledge representation; WG-III Security, safety and quality, and WG-IV Technology for interoperability. From the very beginning, the methodology used in CEN TC 251 was based the development of messages on preliminary modelling. Progressively, however, the need to relate specific domain models within a generic Reference Information Model arose, and this has been achieved within HL7 with its development of the Reference Information Model (RIM). CEN TC 251 has established a Memorandum of Understanding with HL7, in order to foster collaboration and harmonization between the approaches of both organisations.

4.2.3.CEN / ISSS

The CEN Information Society Standardisation System (CEN/ISSS) provides market players with a comprehensive and integrated range of standardisation services and products, in order to contribute to the success of the Information Society in Europe. It was created in mid-1997 by CEN as the focus for its Information and Communications Technologies activities.

CEN/ISSS provides a middle way, an open process combining the tried and tested backing of the formal standardisation environment with a fast, market-driven approach. CEN/ISSS draws on the best of the standardisation worlds, bridging the gap between formal (de jure) and informal (de facto) standardisation, combining the rapid process of informal specification with the security offered by the formal open consensus of traditional standardisation.

In addition to formal CEN TC, CEN/ISSS provides a less formal environment through CEN/ISSS Workshops. These offer the opportunity for direct participation in the standardisation process. They are ongoing working groups that are open to all interested parties, including vendors, service providers, regulators, users and consumer groups. CEN/ISSS Workshops aim to arrive at a European consensus on an issue that can be published as a CEN Workshop Agreement (CWA). These deliverables may take the form of best practice agreements, codes of conduct or

pre-standards, with the formal backing of CEN, one of the three European Standardisation Organisations. Furthermore, CWA prepare drafts of documents on the fields on behalf of the European Commission, the European Parliament and subsidized bodies. In our context, the CEN/ISSS Workshop on Network and Information Security has to be mentioned, which established a Network and Information Security Standards Report in support of the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”.

CEN/ISSS also runs Focus Groups in order to report on the current standards environment in a particular area of public interest, with a view to providing recommendations on necessary standardisation work for the future. These may be set up on request from European legislators in order to carry out public consultation on an issue concerning standards and standardisation.

4.2.4.CEN / ISSS eHealth Standardization Focus Group

As eHealth is a subject given particular importance in the eEurope 2005 Action Plan, CEN/ISSS responded to the need for a specific investigation on related standardisation. There is a long-standing CEN TC 251 on Health Informatics that has produced a series of European pre-standards and standards covering the electronic exchange of medical data. These documents cover a large range of different exchanges of value to organisations providing healthcare services, their industrial and medical suppliers, and public administrations.

The work of a short-term CEN/ISSS Focus Group in the eHealth domain has now been completed. An open activity, with well about 150 participants from 28 countries, has produced a report that provides an overview of eHealth interoperability issues.

4.2.5.ETSI

The availability of digital technologies and broadband infrastructure is providing the basic elements for the convergence between telecommunications, Internet and consumer electronic products to occur and for customers to access freely a large range of services from a wide variety of technology platforms. But these new opportunities come with challenges as ICT systems are complex and diverse. Their success is highly dependant on interoperability that guarantees the quality and reliability of the information exchanged. Interoperability is ultimately what standardisation is about. As a well-respected standardisation body, the European Telecommunications Standards Institute (ETSI) has a good experience in the standardisation of telecommunication systems for fixed and mobile networks and services, TV broadcasting as well as for information technologies. ETSI is therefore ideally positioned as the main ICT standardisation body in Europe.

The mission of ETSI is to produce telecommunications standards for today and for the future. ETSI is officially responsible for standardisation of Information and Communication Technologies within Europe. These technologies include, but are not limited to, telecommunications, technical security and safety, information and communication infrastructures, broadcasting and related areas such as intelligent transportation and medical electronics.

4.2.6.IHE Europe

IHE Europe is the European supporting organisation of the international IHE initiative. The goal of the Integrating the Health care Enterprise (IHE) initiative in general is to stimulate integration of health care information resources to improve clinical care. IHE develops and publishes detailed frameworks and respective profiles for implementing established data standards to meet specific healthcare needs and supports testing, demonstration and educational activities to promote the deployment of these frameworks by vendors and users.

4.2.7.CENELEC

CENELEC, the European Committee for Electrotechnical Standardisation, was created in 1973 as a result of the merger of two previous European organisations: CENELCOM and CENEL. Nowadays, CENELEC is a non-profit technical organisation set up under Belgian law and composed of the National Electrotechnical Committees of 29 European countries. In addition, 9 National Committees from neighbouring countries are participating in CENELEC work with an Affiliate status.

CENELEC members have been working together in the interests of European harmonization since the 1950s, creating both standards requested by the market and harmonized standards in support of European legislation and which helped to shape the European Internal Market. CENELEC works with 15,000 technical experts from 29 European countries. Its work directly increases market potential, encourages technological development and guarantees the safety and health of consumers and workers.

CENELEC's mission is to prepare voluntary electro-technical standards that help develop the Single European Market/European Economic Area for electrical and electronic goods and services removing barriers to trade, creating new markets and cutting compliance costs.

A Resolution of 7th May 1985 of the European Council formally endorsed the principle of reference to European standards within the relevant European regulatory work (Directives), thereby paving the way to a New Approach in the philosophy of regulations and standards in Europe. In the light of this New Approach, CENELEC is developing and achieving a coherent set of voluntary electro-technical standards as a basis for the creation of the Single European Market/European Economic Area without internal frontiers for goods and services.

In addition to the traditional European standard deliverables, the dynamic Workshop (CWA: CENELEC Workshop Agreement) has been included in its portfolio, offering an open platform to foster the development of pre-standards for short lifetime products where time-to-market is critical.

4.3. National Activities to Be Considered

Specific Standards Developing Organisations with specific business fields are sometimes located in a single country but have an international relevance. As EuroRec/Q-REC needs to take care of almost all existing and emerging standardisation domains, some of these national SDO shall be introduced in the following.

4.3.1.ANSI

The American National Standards Institute (ANSI) coordinates both development and use of voluntary consensus standards. It represents the needs and views of U.S. stakeholders in standardisation forums around the globe.

The Institute oversees the creation, promulgation and use of thousands of norms and guidelines that directly impact businesses in nearly every sector: from acoustical devices to construction equipment, from dairy and livestock production to energy distribution, and many more. ANSI is also actively engaged in accrediting programs that assess conformance to standards – including globally-recognized cross-sector programs such as the ISO 9000 (quality) and ISO 14000 (environmental) management systems.

To enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity. Founded October 19, 1918, ANSI is the official U.S. representative to the International Organization for Standardization (ISO) and, via the U.S. National Committee, the International Electrotechnical Commission (IEC). ANSI is also a member of the International Accreditation Forum (IAF).

4.3.2.ASTM

ASTM International, formerly the American Society for Testing Materials (ASTM), is one of several organisations that develop standards under ANSI, the American National Standards Institute. ASTM / E31 is the technical committee responsible for Health care Informatics. It has published several useful standards that have fuelled a variety of international standards. Most recently, ASTM has balloted, and passed, a standard for the Continuity of Care Record (CCR). This is a family of XML-format messages with the original use of supporting electronic patient care referrals among healthcare providers. It is now seen as having archival value within and Electronic Health Records repository. Recently, ASTM and HL7 have agreed to harmonize their CCR with the HL7 work on the Clinical Document Architecture (CDA).

4.3.3.NEMA

The U.S. National Electrical Manufacturers Association NEMA, created in 1926 by the merger of the Electric Power Club and the Associated Manufacturers of Electrical Supplies, provides a forum for the standardisation of electrical equipment, enabling consumers to select from a range of safe, effective, and compatible electrical products. The organisation has also made numerous contributions to the electrical industry by shaping public policy development and operating as a central confidential agency for gathering, compiling, and analyzing market statistics and economics data. NEMA attempts to promote the competitiveness of its member companies by providing a forum for both the development of technical standards that are in the best interests of the industry and the users of its products, and for the establishment and advocacy of industry policies on legislative and regulatory matters that might affect the industry and those it serves. Additionally NEMA aims at collecting, analyzing, and disseminating industry data.

NEMA publishes over 500 standards and offers them through IHS, along with a number of standards originally developed as American National Standards Institute (ANSI) or International

Electrotechnical Commission (IEC) standards. The association promotes safety in the manufacture and use of electrical products, provides information about NEMA to the media and the public, and represents industry interests in new and developing technologies. NEMA, with headquarters in Rosslyn, Virginia, has approximately 430 member companies, including large, medium, and small businesses that manufacture products used in the generation, transmission and distribution, control, and end-use of electricity.

4.4. Other Organisations and Initiatives

Promoting a Nationwide Health Information Network, the US Government in collaboration with national SDOs, provider and vendor organisations and governmental institutions such as DoD / VHA, etc., launched several groups and bodies such as Office of the National Coordinator for Health Information Technology (ONCHIT), the Health Information Technology Standards Panel (HITSP) with its International Landscape Committee or the Certification Commission for Healthcare Information Technology. Because of the global relevance of those organisations, they will be shortly presented.

4.4.1. Certificate Commission for Healthcare Information Technology

The Certification Commission for Healthcare Information Technology's (CCHIT) mission is to accelerate the adoption of healthcare information technology throughout the US by creating a credible mechanism for the certification of healthcare IT (HIT) products. Certification was listed by Dr David Brailer as a key action in delivering the goals of ONCHIT's 2004 Strategic Framework for advancing HIT adoption.

CCHIT was founded in 2004 with sponsorship from three industry associations in HIT:

- The American Health Information Management Association (AHIMA),
- The Healthcare Information and Management Systems Society (HIMSS) and
- The National Alliance for Healthcare Information Technology (the Alliance).

Additional funding support came from the Health and Human Service, an important US Government Department in the healthcare domain, from the American Academy of Family Physicians (AAFP), the American Academy of Pediatrics (AAP), the American College of Physicians (ACP), the California HealthCare Foundation (CHCF), the Hospital Corporation of America, McKesson, Sutter Health, the United Health Foundation, and WellPoint Health Networks, Inc.

5. Standards and Publicly Available Specifications

Standards are definitions and specifications based on common knowledge and broad agreement. This can be provided by a consensus process as happening in international SDOs such as ISO, CEN, HL7, DICOM, etc., leading to **formal standards** or **consent-based standards**, or by market enforcement. The latter is happening in the context of market dominance or even a monopoly leading to **proprietary standards**, e.g., Microsoft Windows. Finally, standards can be established through their acceptance by the user community or the market in general. Examples for the latter – also called **industry standards** – are the TCP/IP protocol or video tape formats.

Distinguishing from formal (de-jure) standards, which have to follow clearly defined as well as open processes and have to be publicly available, the informal (de-facto) standards can also be made publicly available, therefore called Publicly Available Specifications (PAS). Because of the nature, their relevance to the market and their harmonization objectives, formal standard and PAS are managed in our project in a similar way.

Regularly, standards and PAS cannot be enforced. For speeding up harmonization processes and realizing certain environments, specifications can also be enforced by declaring them normative. Such legally binding specifications are called **norms**. This requires however a common jurisdiction, which cannot be established globally. Internal to the European Union, CEN standards can be enforced contrary to ISO specifications. Legal aspects and interests might be different, leading, e.g., to massive interest of globally active industries in ISO standards contrary to European governments pushing CEN standards.

5.1. Domain-Independent Specifications

Considering requirements, processes, services, functionalities, protocols, applications and products, they may serve overarching needs independent of the different domains such as healthcare, financing, transportation, energy supply, etc. Specifications of such requirements, processes, services, functions, protocols, applications and products are called **domain-independent specifications**. Such specifications are, e.g., enumeration schemes.

5.2. Domain-Specific Specifications

Considering requirements, processes, services, functionalities, protocols, applications and products, they may serve special needs of domains such as healthcare, financing, transportation, energy supply, etc. Specifications of such requirements, processes, services, functions, protocols, applications and products are called **domain-specific specifications**. Such specifications are, e.g., application paths for human medications.

5.3. General Specifications

Some of the specifications considered are focused on generic principles of processes, functionalities, etc. Such specifications are called **general specifications**. They are exemplified by the ISO 9000 series on quality management, which is adaptable to any environment and domain.

5.4. Application-Related Specifications

Some of the specifications are dedicated to specific services or applications, therefore called **application-related specifications**. Database access control models are a typical example for such type of specifications.

5.5. Infrastructural Specifications

Specifications for infrastructural services such as ID management or directory services are called **infrastructural specifications**. Services based on infrastructural specification are enabler for other services, providing essential prerequisites or a platform for them. While many security services are infrastructural ones, of interest or a need in different domains, such specifications are frequently domain-independent. Application security services are mainly influenced by the underlying policies. Therefore, application security services are special for the healthcare domain and according to the aforementioned classification domain-specific. As many classifications are based on narrative definitions, they cannot be always classified in a unique and disjunctive way. The given classification helps especially non-experts in the standards domain in orienting through the standards and specification jungle, however.

5.5.1. Tokens

As identification and authentication can be provided based on knowledge, ownership or property, the process definition can be accompanied by the specification of the device needed in the identification/authentication process. In that context, security tokens such as smartcards, security sticks (USB sticks) or any other devices for storing and processing keys and certificates are a matter of security standardisation.

5.5.2. ID Management

Most interaction processes such as communication, cooperation, interoperability are depending on services and mechanisms for reliable identification (and for assurance purposes authentication) of principals involved. This process concerns the creation of identifiers, assignment of identifiers, verification of identifiers, revocation of identifiers, matching of identifiers, etc. This set of services is called ID management.

5.5.3. Privacy Standards

An essential part of standards, specifications, reports and normative references for eHealth and the health sector in general is related to aspects of privacy and related data protection schemes. This group of standards is not a homogeneous one as it combines narrative text documents, specifications, technology reports, and even models.

Following we will deploy the classification scheme introduced already extending it a little towards the main topics the EuroRec Institute and the Q-REC Project is dealing with. **Thereby, the overview has always been restricted to EHR-related specifications.**

5.6. Requirements and Analysis Standards

These specifications aim at analysing business cases, user needs and requested functionalities, and at describing the respective requirements for a high-quality standard-based design, development, implementation, and evaluation.

Table 1: Requirements and Analysis Standards Overview

ASTM E2212-02 ^a	Standard Practice for Healthcare Certificate Policy
ISO 18812:2003	Health informatics - Clinical analyser interfaces to laboratory information systems - Use profiles
ISO 22857:2004	Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information
ISO TR 20514:2005	Health informatics - Electronic health record - Definition, scope and context
ISO TS 18308:2004	Health informatics - Requirements for an electronic health record architecture

In the following, most of the standards listed above shall be explained in more detail.

Name	Standard Practice for Healthcare Certificate Policy
Notation	ASTM E2212-02 ^a
Issuing Organisation	ASTM
Description	Addresses the policy for digital certificates that support the authentication, authorization, confidentiality, integrity, and non-repudiation requirements of persons and organizations that electronically create or transact health information. There are 3 types of certificate: one for computerized entities, one for individual person and the last one for clinical individuals

Name	Clinical analyser interfaces to laboratory information systems
Notation	ISO 18812:2003
Issuing Organisation	ISO
Description	This standard specifies general messages for electronic information exchange between analytical instruments (AI) and laboratory information systems (LIS) within a clinical laboratory. It is applicable to the specialities of clinical chemistry/biochemistry, haematology, toxicology, microbiology, virology and immunology. It is not applicable to the blood transfusion and blood bank

	<p>speciality.</p> <p>The standard is applicable only to character-based message information. It is not applicable to the communication of graphical or image information.</p> <p>The standard covers the specification of messages used by communicating parties and the syntax in which they are communicated. It does not cover the transport mechanisms used for the message interchange.</p>
--	---

Name	Guidelines on data protection to facilitate trans-border flow of personal health information
Notation	ISO TS 22857:2004
Issuing Organisation	ISO
Description	This standard provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organization should adopt to ensure compliance with those principles.

Name	Electronic health record - Definition, scope and context
Notation	ISO TR 20514:2005
Issuing Organisation	ISO
Description	This standard describes a pragmatic classification of electronic health records, provides simple definitions for the main categories of EHR and provides supporting descriptions of the characteristics of electronic health records and record systems.

Name	Requirements for an electronic health record architecture
Notation	ISO TS 18308:2004
Issuing Organisation	ISO
Description	The purpose of this standard is to assemble and collate a set of clinical and technical requirements for an electronic health record architecture (EHRA) that supports using, sharing, and exchanging electronic health records across different health sectors, different countries, and different models of

	healthcare delivery. It gives requirements for the architecture but not the specifications of the architecture itself.
--	--

5.7. Architecture Standards

Based on analysis procedures mentioned above, the architecture standards listed below aim at describing architectural approaches for information systems and applications especially in the domain of healthcare and welfare.

Table 2: List of Architecture Standards

CEN EN 12967-1:2006	Health informatics - Service architecture - Part 1: Enterprise viewpoint (HISA)
CEN EN 12967-2:2006	Health informatics - Service architecture - Part 2: Information viewpoint (HISA)
CEN EN 12967-3:2006	Health informatics - Service architecture - Part 3: Computational viewpoint (HISA)
CEN EN 13606-1:2006	Health informatics - Electronic health record communication - Part 1: Reference model
CEN EN 13606-4:2006	Health Informatics - Electronic health record communication - Part 4: Security requirements and distribution rules

In the following, most of the standards listed above shall be explained in more detail. Standards containing several parts are listed just once.

Name	Service Architecture (former CEN HISA ENV 12967)
Brief Name	CEN prEN 12967:2006
Issuing Organisation	CEN
Description	Describes the Service Architecture (formerly Health Information System Architecture, HISA), which is a description of the middleware layer used in healthcare. This standard is described with diagrams and consists of three parts: Part 1: Enterprise viewpoint Part 2: Information viewpoint Part 3: Computational viewpoint

Name	Health informatics - Electronic health record communication
Brief Name	CEN EN 13606:2006

Issuing Organisation	CEN
Description	<p>Purposes a scheme to define a healthcare record in order the information is recognisable and understandable in different applications.</p> <p>This standard consists of five parts:</p> <p>Part 1: Reference model</p> <p>Part 2: Archetypes</p> <p>Part 3: Reference archetypes and term lists</p> <p>Part 4: Security requirements and distribution rules</p> <p>Part 5: Exchange models</p>

5.8. Modelling and Methodology Standards

After having chosen an appropriate architecture for the new information system to be developed, a comprehensive model of the system methodology needs to be designed based on a specific methodology.

Table 3: List of Modelling and Methodology Standards

ASTM E1715-01	An object-oriented model for registration, admitting, discharge, and transfer functions in computer-based patient record systems
ASTM E2085-00a	Standard guide on security framework for healthcare information
IETF RFC 3281	An Internet Attribute Certificate Profile for Authorization
CEN CR 12587	CEN Report: Medical Informatics - Methodology for the development of healthcare messages
CEN EN 13940-1:2006	Health Informatics - System of concepts to support Continuity of care - Part 1: Basic concepts
CEN EN 14463:2006	Health informatics - A syntax to represent the content of medical classification systems (ClAML)
CEN ENV 13940:2002	Health informatics - System of concepts to support continuity of care
CEN TR 15300	CEN Report: Health Informatics - Framework for formal modelling of healthcare security policies
ISO HL7 21731:2006	Health informatics - HL7 version 3 - Reference information model - Release 1
ISO DIS 27799	Health informatics - Security management in health using ISO/IEC 17799
ISO IEC 10118	Information technology - Security techniques - Hash-functions

ISO IEC 10181	Information technology - Open Systems Interconnection - Security frameworks for open systems
ISO IEC 10736	Information technology, Telecommunications and information exchange between systems, Transport layer security protocol
ISO IEC 10745	Information technology, Open Systems Interconnection, Upper layers security model
ISO IEC 13335-1:2004	Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management
ISO IEC 15408-1:2005	Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
ISO IEC 15408-2:2005	Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
ISO IEC 15408-3:2005	Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
ISO IEC 27001:2005	Information technology - Security techniques - Information security management systems (ISMS) - Requirements
ISO IEC 27002	Previous ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management
ISO IEC 27003	ISMS Implementation guidance
ISO IEC 27004	ISMS measurements
ISO IEC 27005	ISMS Risk assessment
ISO IEC NP 27000	Information technology - Information security management - fundamentals and vocabulary
ISO IEC TR 13335-3:1998	Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security
ISO IEC TR 13335-4:2000	Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards
ISO IEC TR 13335-5:2001	Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security
ISO PAS 28000:2005	Security management systems for the supply chain
ISO PAS 28003:2006	Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems

In the following, most of the standards listed above shall be explained in more detail.

Name	An object-oriented model for registration, admitting, discharge, and transfer functions in computer-based patient record systems
Brief Name	ASTM E1715-01
Issuing Organisation	ASTM
Description	Details the objects that make up the reservation, registration, admitting, discharge, and transfer functional domain of the computer-based record of care. It is intended to amplify guide E1239 with an object-oriented focus.

Name	Standard guide on security framework for healthcare information
Brief Name	ASTM E2085-00a
Issuing Organisation	ASTM
Description	Describes a framework for the protection of healthcare information. It addresses both storage and transmission of information. It makes use of well-known security algorithms such as SHA-1, triple-DES and others.

Name	An Internet Attribute Certificate Profile for Authorization
Brief Name	IETF RFC 3281
Issuing Organisation	IETF
Description	This specification defines a profile for the use of X.509 Attribute Certificates in Internet Protocols. Attribute certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability as well as limited special purpose requirements. The profile places emphasis on attribute certificate support for Internet electronic mail, IPsec, and WWW security applications.

Name	CEN Report: Medical Informatics - Methodology for the development of healthcare messages
Brief Name	CEN CR 12587
Issuing Organisation	CEN

Description	The scope of this CEN report is to specify a method for the development of European Standard message specifications for the electronic exchange of structured character-based information, between autonomous computer systems within and between organisations, for purposes related to healthcare. Such message standards are essential if healthcare services are to obtain the benefits of open systems and avoid the constraints of proprietary interfaces. The method specifies the activities of the message development process and the structure and the components of the resulting deliverables.
--------------------	---

Name	Health Informatics - System of concepts to support continuity of care - Part 1: Basic concepts
Brief Name	CEN EN 13940-1:2006
Issuing Organisation	CEN
Description	Defines the classes of concepts and their descriptive terms regarding all processes of care, especially considering patient centred continuity of care, shared care and seamless care.

Name	A syntax to represent the content of medical classification systems (ClAML)
Brief Name	CEN EN 14463:2006
Issuing Organisation	CEN
Description	The main purpose of this European Standard is to support the safe transfer of the majority of hierarchical healthcare classification systems between organisations and dissimilar software products. It is intended to serve as the core representation, from which all publication forms can be derived. The Standard should therefore be rich enough to uniquely identify and describe the structure and the relevant elements in those systems. This Standard does not intend to prescribe the meaning of structuring elements in classification systems. This Standard is not meant to be a direct format for printing or viewing the contents of a classification system. Views and prints shall be derived from this representation by post processing.

Name	Health Informatics - System of concepts to support continuity of care
Brief Name	CEN ENV 13940:2002
Issuing Organisation	CEN
Description	Defines the classes of concepts and their descriptive terms regarding all processes of care, especially considering patient centred continuity of care, shared care and seamless care.

Name	HL7 version 3 - Reference information model
Brief Name	ISO HL7 21731:2006
Issuing Organisation	ISO
Description	This standard deals with a static model of health and health care information as viewed within the scope of HL7 standards development activities.

Name	Health informatics - Security management in health using ISO/IEC 17799
Brief Name	ISO DIS 27799
Issuing Organisation	ISO
Description	<p>This standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 17799 (Information Technology; Code of practice for information security management) and is a companion to that standard. It specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. Once it is implemented, health organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality integrity and availability of personal health information. Health information exists in many forms. It consists of data expressed not only in words and numbers, but also in sound recordings, drawings, video, and medical images. Health information may be printed or written, and may be stored electronically or on paper. It can be transmitted by hand, via fax, over computer networks, or by post. Whatever form the information takes, and whatever means is used to transmit it, it must always be appropriately protected. This standard and ISO/IEC 17799 taken together define what is required in terms of information security in healthcare; they do not define how these requirements are to be met. That is to say, to the fullest extent possible, this standard is technology-neutral. Neutrality with respect to implementing technologies is an important feature of these standards. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that this standard describes. As noted in the introduction, familiarity with ISO/IEC 17799 is indispensable to an understanding of this standard.</p>

Name	Information technology - Security techniques - Hash-functions
Brief Name	ISO IEC 10118

Issuing Organisation	ISO
Description	<p>This standard consists of four parts:</p> <p>Part 1: General</p> <p>Part 2: Hash-functions using an n-bit block cipher</p> <p>Part 3: Dedicated hash-functions</p> <p>Part 4: Hash-functions using modular arithmetic</p> <p>ISO/IEC 10118 specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map arbitrary strings of bits to fixed-length strings of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, and committing the user to a given string of bits without revealing this string.</p> <p>Part 1 contains definitions, symbols, abbreviations and requirements that are common to all the other parts of ISO/IEC 10118.</p> <p>Part 2 specifies hash-functions which make use of an n-bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented.</p> <p>Four hash-functions are specified. The first provides hash-codes of length smaller than or equal to n, where n is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to 2n; the third provides hash-codes of length equal to 2n; and the fourth provides hash-codes of length 3n. All four of the hash-functions specified in this part of ISO/IEC 10118 conform to the general model specified in ISO/IEC 10118-1.</p> <p>Part 3 specifies the following seven dedicated hash-functions, i.e. specially-designed hash-functions:</p> <ul style="list-style-type: none"> • the first hash-function (RIPEMD-160) in Clause 7 provides hash-codes of lengths up to 160 bits; • the second hash-function (RIPEMD-128) in Clause 8 provides hash-codes of lengths up to 128 bits; • the third hash-function (SHA-1) in Clause 9 provides hash-codes of lengths up to 160 bits; • the fourth hash-function (SHA-256) in Clause 10 provides hash-codes of lengths up to 256 bits; • the fifth hash-function (SHA-512) in Clause 11 provides hash-codes of lengths up to 512 bits; • the sixth hash-function (SHA-384) in Clause 12 provides hash-codes of a fixed length, 384 bits; and • the seventh hash-function (WHIRLPOOL) in Clause 13 provides hash-codes of lengths up to 512 bits. <p>For each of these dedicated hash-functions, part 3 specifies a round-function that consists of a sequence of sub-functions, a padding method, initializing</p>

	<p>values, parameters, constants, and an object identifier as normative information, and also specifies several computation examples as informative information.</p> <p>Part 4 specifies two hash-functions which make use of modular arithmetic. These hash-functions, which are believed to be collision-resistant, compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function defined in 7.3. Thus, the hash-code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).</p> <p>The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function.</p>
--	--

Name	Information technology - Open Systems Interconnection - Security frameworks for open systems
Brief Name	ISO IEC 10181
Issuing Organisation	ISO
Description	<p>This standard consists of seven parts:</p> <ul style="list-style-type: none"> Part 1: Overview Part 2: Authentication framework Part 3: Access control framework Part 4: Non-repudiation framework Part 5: Confidentiality framework Part 6: Integrity framework Part 7: Security audit and alarms framework <p>The security frameworks address the application of security services in an Open Systems environment, where the term Open Systems is taken to include areas such as Database, Distributed Applications, ODP and OSI. The security frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The security frameworks are not concerned with the methodology for constructing systems or mechanisms.</p> <p>The security frameworks address both data elements and sequences of operations (but not protocol elements) which are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.</p> <p>The security frameworks provide the basis for further standardisation, providing consistent terminology and definitions of generic abstract service interfaces for specific security requirements. They also categorize the</p>

	<p>mechanisms that can be used to achieve those requirements.</p> <p>One security service frequently depends on other security services, making it difficult to isolate one part of security from the others. The security frameworks address particular security services, describe the range of mechanisms that can be used to provide the security services, and identify interdependencies between the services and the mechanisms. The description of these mechanisms may involve a reliance on a different security service, and it is in this way that the security frameworks describe the reliance of one security service on another.</p> <p>Part 1 of the security frameworks:</p> <ul style="list-style-type: none"> • describes the organisation of the security frameworks; • defines security concepts which are required in more than one part of the security frameworks; • describes the inter-relationship of the services and mechanisms identified in other parts of the frameworks. <p>Part 2 addresses the application of security services in an Open Systems environment, where the term Open Systems is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI.</p> <p>Part 3 specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system.</p> <p>Part 4:</p> <ul style="list-style-type: none"> • defines the basic concepts of Non-repudiation; • defines general Non-repudiation services; • identifies possible mechanisms to provide the Non-repudiation services; • identifies general management requirements for Non-repudiation services and mechanisms. <p>Part 5 specifies a general framework for the provision of confidentiality services.</p> <p>Part 6 specifies a general framework for the provision of integrity services.</p> <p>Part 7:</p> <ul style="list-style-type: none"> • defines the basic concepts of security audit and alarms; • provides a general model for security audit and alarms; and • identifies the relationship of the Security Audit and Alarms service with other security services.
--	--

Name	Information technology - Telecommunications and information exchange between systems - Transport layer security protocol
Brief Name	ISO IEC 10736:1995
Issuing Organisation	ISO

Description	Defines the transport layer security protocol. Does not specify the management functions and protocols needed to support this security protocol. Defines a protocol which may be used for Security Association establishment. Specifies one algorithm for Authentication and key distribution which is based on public key crypto systems.
--------------------	--

Name	Information technology - Open Systems Interconnection - Upper layers security model
Brief Name	ISO IEC 10745:1995
Issuing Organisation	ISO
Description	Defines a model for security in the upper layers of OSI that provides a basis for the development of application-independent services and protocols, in particular it specifies the security aspects of communication in the upper layers of OSI.

Name	Information technology - Security techniques - Management of information and communications technology security
Brief Name	ISO IEC 13335
Issuing Organisation	ISO
Description	<p>This standard consists of several parts:</p> <p>Part 1: Concepts and models for information and communications technology security management</p> <p>Part 2: Managing and planning IT Security</p> <p>Part 3: Techniques for the management of IT Security</p> <p>Part 4: Selection of safeguards</p> <p>Part 5: Management guidance on network security</p> <p>Part 1 of this standard presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. Part 2 of ISO/IEC 13335 (currently 2nd WD) provides operational guidance on ICT security. Together these parts can be used to help identify and manage all aspects of ICT security.</p> <p>The guidelines in part 2 address subjects essential to the management of IT security, and the relationship between those subjects. These guidelines are useful for the identification and the management of all aspects of IT security.</p> <p>Part 3 provides techniques for the management of IT security. The techniques are based on the general guidelines laid out in part 1 and 2. These guidelines are designed to assist the implementation of IT security.</p>

	<p>Part 4 provides guidance on the selection of safeguards, taking into account business needs and security concerns. It describes a process for the selection of safeguards according to security risks and concerns and the specific environment of an organisation. It shows how to achieve appropriate protection, and how this can be supported by the application of baseline security. An explanation is provided on how the approach outlined in this part of the standard supports the techniques for the management of IT security laid out in part 3.</p> <p>Part 5 provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements.</p> <p>Part 5 builds upon Part 4 of this standard by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.</p> <p>It is not within the scope of this standard to provide advice on the detailed design and implementation aspects of the technical safeguard areas.</p>
--	---

Name	Information technology - Security techniques - Evaluation criteria for IT security
Brief Name	ISO IEC 15408:2005
Issuing Organisation	ISO
Description	<p>This standard consists of three parts:</p> <p>Part 1: Introduction and general model</p> <p>Part 2: Security functional requirements</p> <p>Part 3: Security assurance requirements</p> <p>Part 1 of this standard defines two forms for expressing IT security functional and assurance requirements. The protection profile (PP) construct allows creation of generalized reusable sets of these security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs. The security target (ST) expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the target of evaluation (TOE). The ST is used by evaluators as the basis for evaluations conducted in accordance with ISO/IEC 15408.</p> <p>Part 2 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products and systems.</p> <p>Part 3 defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EAL) that define a scale for measuring</p>

	assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of protection profiles and security targets.
--	---

Name	Information technology - Security techniques - Information security management systems - Requirements	
Brief Name	ISO IEC 27001:2005	
Issuing Organisation	ISO	
Description	<p>This standard covers all types of organisations (e.g. commercial enterprises, government agencies, not-for profit organisations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organisations or parts thereof.</p> <p>This standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It is intended to be suitable for several different types of use, including the following:</p> <ul style="list-style-type: none"> • use within organisations to formulate security requirements and objectives; • use within organisations as a way to ensure that security risks are cost effectively managed; • use within organisations to ensure compliance with laws and regulations; • use within an organisation as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organisation are met; • definition of new information security management processes; • identification and clarification of existing information security management processes; • use by the management of organisations to determine the status of information security management activities; • use by the internal and external auditors of organisations to determine the degree of compliance with the policies, directives and standards adopted by an organisation; • use by organisations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organisations with whom they interact for operational or commercial reasons; • implementation of business-enabling information security; • use by organisations to provide relevant information about information 	

	security to customers.
--	------------------------

Name	Information technology - Security techniques - Code of practice for information security management (previous ISO/IEC 17799:2005)
Brief Name	ISO IEC 27002
Issuing Organisation	ISO
Description	<p>This standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The objectives outlined provide general guidance on the commonly accepted goals of information security management. This standard contains best practices of control objectives and controls in the following areas of information security management:</p> <ul style="list-style-type: none"> • security policy; • organisation of information security; • asset management; • human resources security; • physical and environmental security; • communications and operations management; • access control; • information systems acquisition, development and maintenance; • information security incident management; • business continuity management; • compliance. <p>The control objectives and controls in this standard are intended to be implemented to meet the requirements identified by a risk assessment. This standard is intended as a common basis and practical guideline for developing organisational security standards and effective security management practices, and to help build confidence in inter-organisational activities.</p>

Name	Information technology - Security techniques - Information security management system implementation guidance
Brief Name	ISO IEC 27003
Issuing Organisation	ISO
Description	<p>ISO 27003 is a proposed work item for ISO SC27 that will contain implementation guidance to help those implementing the ISO 27000-series standards. Publication is anticipated in October 2008.</p> <p>The proposed scope of ISO 27003 is to provide help and guidance in implementing the Information Security Management System (ISMS)</p>

	requirements in [ISO SC27] project 24743. (It) will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review, and improve the ISMS.
--	---

Name	Information technology - Security techniques - Information security management measurements
Brief Name	ISO IEC 27004
Issuing Organisation	ISO
Description	<p>ISO 27004 will be a new ISO standard on information security management measurements. The standard is currently a Working Draft, being circulated for study and comment.</p> <p>The standard is expected to help organisations measure and report the effectiveness of their information security management systems, covering both the security management processes (defined in ISO 27001) and the controls (ISO 17799 / 27002).</p> <p>The scope is to “provide guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. It is intended to be applicable to a wide range of organisations with a correspondingly wide range of information security management systems. (It) provides guidance for measurement procedures and techniques to determine the effectiveness of information security controls and information security processes applied in ISMS. The purpose of the Information security management measurements development and implementation process, defined in this Standard is to create a base for each organisation to collect, analyse, and communicate data related to ISMS processes. This data is ultimately to be used to base ISMS-related decisions and to improve implementation of ISMS.”</p>

Name	Information technology - Security techniques - Information security management risk assessment
Brief Name	ISO IEC 27005
Issuing Organisation	ISO
Description	<p>This standard is an ISO standard describing the complete process of information security risk management in a generic manner. The annexes contain examples of information security risk assessment approaches as well as lists of possible threats, vulnerabilities and security controls. This standard can be viewed at as the basic information risk management standard at international level, setting a framework for the definition of the</p>

	risk management process.
--	--------------------------

Name	Information technology - Security techniques - Information security management systems - Fundamentals and vocabulary
Brief Name	ISO IEC 27000
Issuing Organisation	ISO
Description	<p>ISO 27000 will contain the fundamentals and vocabulary - in other words definitions - for the specialist terms used throughout the ISO 27000-series standards.</p> <p>The scope is “to specify the fundamental principles, concepts and vocabulary for the ISO/IEC 27000 (information security management system) series of documents.”</p> <p>Information security, like most technical subjects, is evolving a complex web of terminology. Few authors take the trouble to define precisely what they mean, but this is unacceptable in the standards arena as it leads to confusion and devalues formal assessment and certification.</p> <p>ISO 27000 will presumably be similar to other vocabulary and definitions standards but will hopefully become a generally-accepted reference for information security terms amongst the information security profession. It will probably absorb guidelines such as ISO/IEC Guide 2:1996 “Standardization and related activities – General vocabulary” and ISO/IEC Guide 73:2002 “Risk management – Vocabulary – Guidelines for use in standards”.</p>

Name	Security management systems for the supply chain
Brief Name	ISO PAS 28000:2005
Issuing Organisation	ISO
Description	<p>This standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. These aspects include, but are not limited to, financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. Security management is linked to many other aspects of business management. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.</p> <p>This standard is applicable to all sizes of organisations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:</p> <ul style="list-style-type: none"> • establish, implement, maintain and improve a security management

	<p>system;</p> <ul style="list-style-type: none"> • assure compliance with stated security management policy; • demonstrate such compliance to others; • seek certification/registration of its security management system by an Accredited third party Certification Body; or • make a self-determination and self-declaration of compliance with ISO/PAS 28000:2005. <p>There are legislative and regulatory codes that address some of the requirements in this standard. It is not the intention of it to require duplicative demonstration of compliance.</p> <p>Organisations that choose third party certification can further demonstrate that they are contributing significantly to supply chain security.</p>
--	--

Name	Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems
Brief Name	ISO PAS 28003:2006
Issuing Organisation	ISO
Description	<p>This standard contains principles and requirements for bodies providing the audit and certification of supply chain security management systems according to management system specifications and standards such as ISO/PAS 28000.</p> <p>It defines the minimum requirements of a certification body and its associated auditors recognizing the unique need for confidentiality when auditing and certifying/registering a client organisation.</p> <p>Requirements for supply chain security management systems can originate from a number of sources, and this standard has been developed to assist in the certification of supply chain security management systems that fulfil the requirements of ISO/PAS 28000, Specification for security supply chain security management systems for the supply chain. The contents of this standard may also be used to support certification of supply chain security management systems that are based on other sets of specified supply chain security management systems requirements.</p> <p>This standard:</p> <ul style="list-style-type: none"> • provides harmonized guidance for the accreditation of certification bodies applying for ISO/PAS 28000 (or other sets of specified supply chain security management systems requirements) certification/registration; • defines the rules applicable for the audit and certification of a supply chain security management systems complying with the ISO/PAS 28000 requirements (or other sets of specified supply chain security management systems requirements);

	<ul style="list-style-type: none"> provides customers with the necessary information and confidence about the way certification of their suppliers has been granted.
--	---

5.9. Communication Standards

Communication and interoperability services based on an existing and reliable infrastructure are pre-requisites for modern health information systems. So communication and messaging standards rank high in the list of existing and emerging standardisation activities.

Table 4: List of Communication Standards

CEN EN 1064:2006	Health informatics - Standard communication protocol - Computer-assisted electrocardiography
CEN EN 12052:2005	Health informatics - Digital imaging - Communication, workflow and data management
CEN EN 13608-1:2006	Health informatics - Security for healthcare communication - Part 1: Concepts and terminology
CEN EN 13608-2:2006	Health informatics - Security for healthcare communication - Part 2: Secure data objects
CEN EN 13608-3:2006	Health informatics - Security for healthcare communication - Part 3: Secure data channels
CEN EN 13609-1:2005	Health Informatics - Messages for maintenance of supporting information in healthcare systems - Part 1: Updating of coding schemes
CEN EN 14720-1:2006	Health informatics - Service request and report messages - Part 1: Basic services including referral and discharge
CEN EN 14822-1:2006	Health informatics - General purpose information components - Part 1: Overview
CEN EN 14822-2:2006	Health informatics - General purpose information components - Part 2: Non-clinical
CEN EN 14822-3:2006	Health informatics - General purpose information components - Part 3: Clinical
CEN ENV 13607:2000	Health informatics - Messages for the exchange of information on medicine prescriptions
CEN ENV 13609-2:2000	Health informatics - Messages for maintenance of supporting information in healthcare systems - Part 2: Updating of medical laboratory-specific information
CEN ENV 13730-1:2002	Health informatics - Blood transfusion related messages - Part 1: Subject of care related messages

CEN TS 14822-4:2006	Health informatics - General purpose information components - Part 4: Message headers
ETSI ETR 277 (March 1996)	Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems
ETSI ETR 278 (March 1996)	Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2
ETSI SR 002 176 V1.1.1 (2003-03)	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures
ETSI SR 002 298 V1.1.1 (2003-12)	Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"
ETSI TR 101 375 V1.1.1 (1998-09)	Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)
ETSI TR 101 690 V1.1.1 (1999-08)	Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)
ETSI TR 101 740 V1.1.1 (1999-08)	Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)
ETSI TR 102 038 V1.1.1 (2002-04)	TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies
ETSI TR 102 047 V1.2.1 (2005-03)	International Harmonization of Electronic Signature Formats
ETSI TR 102 272 V1.1.1 (2003-12)	Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies
ETSI TS 101 733	Electronic Signature Formats
ETSI TS 101 862 V1.3.3 (2006-01)	Qualified Certificate profile
ETSI TS 101 903 V1.2.2 (2004-04)	XML Advanced Electronic Signatures (XAdES)
ETSI TS 102 023 V1.2.1 (2003-01)	Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
ETSI TS 102 176-1 V1.2.1 (2005-07)	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2 V1.2.1 (2005-07)	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices
ISO 12052:2006	Health informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management
ISO 17432:2004	Health informatics - Messages and communication - Web access to DICOM persistent objects
ISO 18232:2006	Health Informatics - Messages and communication - Format of length limited globally unique string identifiers
ISO IEC 13888	Information technology – Security techniques – Non-repudiation
ISO IEC 14888	Information technology, Security techniques, Digital signature with appendix, multiple Parts (1-3).
ISO IEC 9796	Information technology, Security techniques, Digital signature scheme giving message recovery, multiple Parts (1-2).
ISO IEC 9797	Information technology, Security techniques, Message authentication codes.
ISO IEC 9798	Information technology - Security techniques - Entity authentication
ISO TR 21089:2004	Health informatics - Trusted end-to-end information flows
NEMA DICOM 3.0	Digital Imaging and Communications in Medicine

In the following, most of the standards listed above shall be explained in more detail.

Name	Health informatics - General purpose information components - Part 4: Message headers
Brief Name	CEN EN 14822:2006
Issuing Organisation	CEN
Description	<p>The standard consists of four parts:</p> <ul style="list-style-type: none"> Part 1: Overview Part 2: Non-clinical Part 3: Clinical Part 4: Message headers <p>This European multipart standard defines General Purpose Information Components to be used in standards for information exchange supporting various health specific business requirements. The components defined in this standard are the most commonly needed basic building blocks for such standardization but these components may require further specialisation and</p>

	<p>be complemented by other objects required for specific purposes not met by these generally useful components. Such standardization using these general purpose information components could be performed both on a European (CEN) level or be done nationally or for specific user communities regionally as well as internationally. The part 1 provides an informative overview of this series of standards and includes rules for using the components defined in the other parts and on conformance claims.</p> <p>This standard addresses the definition and structuring of information relating to entities that are commonly encountered in communications with and between clinical information computer systems. Within the scope of part 2 of the multi-part standard is a description of components and their use. In particular, these components relate to the following sub-domains: - Subjects of care - Subject of care related parties - Healthcare agents - Devices - care locations - geographic locations - Transport - Financial.</p> <p>Within the scope of part 3 of the multi-part standard is a description of components and their use. In particular, these components relate to the following sub-domains: - Analysable objects - Clinical information - Medicinal products - Routing aspects of medication treatment or other procedures; - Care Service information.</p> <p>It is now widely or even universally accepted that computer systems that are used within healthcare to record information about the care given to patient's need to share that information with other computer systems and their users. In order that computer systems may share information effectively there is a requirement that the communicating parties and particularly their computer systems have a common understanding of how the information which they are sharing is represented. This sharing of representation needs to take place at a number of levels, most notably at the data representation or syntactic level which is the subject of CEN/TS 14796, but also at the macro or semantic level where groupings of data are used to provide a context or set of contexts for the data. This part 4 of the standard is limited to descriptions of components concerned with messaging, and in particular the message and batch headers.</p>
--	---

Name	Health informatics - Standard communication protocol - Computer-assisted electrocardiography
Brief Name	CEN EN 1064:2006
Issuing Organisation	CEN
Description	The present Standard relates to the conventional recording of the electrocardiogram, i.e. the so called standard 12-lead electrocardiogram and the vector-cardiogram (VCG). Initially, the electric connections used for recording the ECG were made to the limbs only. These connections to the right arm (RA), left arm (LA), left leg (LL) and right leg (RL) were introduced by Einthoven. The electrical variations detected by these leads are

	algebraically combined to form the bipolar leads I, II and III.
--	---

Name	Health informatics - Digital imaging - Communication, workflow and data management (MEDICOM)
Brief Name	CEN EN 12052:2005
Issuing Organisation	CEN
Description	This standard is the European contribution to the well-known DICOM. EN 12052 supersedes the former ENV 12052, ENV12623 and ENV12922-1.

Name	Health informatics -- Digital imaging and communication in medicine (DICOM) including workflow and data management
Brief Name	ISO 12052:2006
Issuing Organisation	ISO
Description	<p>Within the field of health informatics this ISO 12052:2006 addresses the exchange of digital images, and information related to the production and management of those images, between both medical imaging equipment and systems concerned with the management and communication of that information.</p> <p>This standard is intended to facilitate interoperability of medical imaging equipment and information systems by specifying a set of protocols to be followed by systems claiming conformance to this International Standard.</p> <p>The syntax and semantics of commands and associated information data models that ensure effective communication between implementations of this International Standard; information that shall be supplied with an implementation for which conformance to this International Standard is claimed.</p>

Name	Health informatics - Security for healthcare communication
Brief Name	CEN EN 13608:2006
Issuing Organisation	CEN
Description	<p>Defines concepts for secure systems. Besides that, secure data objects and secure data channels are addressed.</p> <p>This standard consists of three parts:</p> <p>Part 1: Concepts and terminology</p> <p>Part 2: Secure data objects</p> <p>Part 3: Secure data channels</p>

Name	Health Informatics - Messages for maintenance of supporting information in healthcare systems - Part 1: Updating of coding schemes
Brief Name	CEN EN 13609-1:2005
Issuing Organisation	CEN
Description	This European Standard specifies messages for electronic information exchange between computer systems using coding schemes in healthcare. It describes a message that may be used to populate or update the content of a coding scheme at user applications.

Name	Health informatics - Messages for maintenance of supporting information in healthcare systems - Part 2: Updating of medical laboratory-specific information
Brief Name	CEN EN 13609-2:2000
Issuing Organisation	CEN
Description	The document specifies messages for electronic information exchange between computer systems used by healthcare parties for the purposes of updating supplementary information that is attached to code values within a coding scheme. In particular, this message is intended to provide information to clinicians that are requesting tests within the specialties of haematology, clinical chemistry, cytology, biochemistry and immunology.

Name	Health informatics - Service request and report messages - Part 1: Basic services including referral and discharge
Brief Name	CEN EN 14720-1:2006
Issuing Organisation	CEN
Description	A European Standard specifying messages for requesting and reporting healthcare services. These messages shall cover the requesting and reporting of any pathological diagnostic or specialist service. The scope of these messages shall explicitly exclude prescribing, dispensing and administration of medication, blood products or other specific therapeutic procedures. The Standard should consist of several parts dealing with general issues and more specific variants.

Name	Messages for the exchange of information on medicine prescriptions
Brief Name	CEN ENV 13607:2000
Issuing Organisation	CEN

Description	Specifies a message, called prescription dispensing report message, containing information about prescription items that is sent from the dispensing agent to any other party that is legally permitted to receive such message.
--------------------	--

Name	Health informatics - Blood transfusion related messages - Part 1: Subject of care related messages
Brief Name	CEN ENV 13730-1:2002
Issuing Organisation	CEN
Description	The domain of the blood transfusion related messages includes: -the collection of blood from donor; -preparation; - qualification; -dispensing of Blood components (to be transfused) to the recipient. Transfusion of blood and Blood components to patients is a medical activity that is subject to many legal instructions, regulations and constraints. Immunological conditions transmitted diseases; sustainability and other difficulties due to the fact that the treatment involves many problems, including those cause this. Mistakes and failures may have serious or even fatal consequences.

Name	Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems
Brief Name	ETSI ETR 277 (March 1996)
Issuing Organisation	ETSI
Description	A specification for a confidentiality system for audio visual services is currently being defined by CCITT WP XV. This specification does not contain a cryptographic algorithm, but caters for the use of different algorithms. The algorithms are to be used to encrypt the data streams. This ETR provides the requirements specification for an encryption algorithm which may be used with this CCITT standard.

Name	Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2
Brief Name	ETSI ETR 278 (March 1996)
Issuing Organisation	ETSI
Description	Description of the GSM cipher algorithm A5/2, and to approve its release to the GSM MoU. The report also provides some background information concerning the need for the algorithm and a summary of the procedures that are to be used by the GSM MoU to distribute the algorithm specification and the test data.

Name	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures
Brief Name	ETSI TS 102 176 V1.2.1 (2005-07)
Issuing Organisation	ETSI
Description	<p>The present document defines an initial set of algorithms and the corresponding parameters to be included in a list of approved methods for producing or verifying Electronic Signatures in Secure Signature-Creating Devices (SSCD) (EESSI-work area F: CWA 14168 / 14169 Secure Signature-Creation Devices), to be referenced in the Certificate Policy documents (EESSI-work area A: TS 101 456: Policy requirements for certification authorities issuing qualified certificates), during the signature creation and validation process and environment (EESSI-work area G1/2: CWA 14170: Security Requirements for Signature Creation Systems; CWA 14171 Procedures for Electronic Signature Verification), in trusted CSP components (Certification Service Provider) (EESSI-work-area D: CWA 14167-1:</p> <p>Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) and other technical components and related areas.</p> <p>The present document defines a list of approved cryptographic algorithms combined with the requirements on their parameters, as well as the approved combinations of algorithms in the form of "signature suites". The approved algorithms and parameters shall be referenced in the corresponding Protection Profiles (e.g. for SSCD or trusted CSP components). To support the management activities, a numbering scheme for cryptographic algorithms and their parameters is defined.</p> <p>This standard consists of two parts:</p> <p>Part 1: Hash functions and asymmetric algorithms</p> <p>Part 2: Secure channel protocols and algorithms for signature creation devices</p>

Name	Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"
Brief Name	ETSI SR 002 298 V1.1.1 (2003-12)
Issuing Organisation	ETSI
Description	This report is a draft proposed for issue by CEN and ETSI in response to the European Commission's call for "a comprehensive strategy on security of

	<p>electronic networks including practical implementing action.” The report deals with issues which are relevant to the European Standards Organisations (ESO). It recommends actions on both the ESO and on industry standards bodies that when undertaken will improve the availability of secure electronic communication, including e-commerce and the exchange of information within a European environment and beyond.</p> <p>CEN and ETSI share the aims set forward in the Communication from the Commission. It is agreed that there are comprehensive standards available for secure electronic networks. However, the report notes that there are few security frameworks to guarantee multi-vendor systems will operate securely together. Also it is noted that there is a lack of appropriate certification in some areas. The result is fragmentation and uneven implementation in real networks and insecurities remain despite some parts being very secure.</p> <p>This standard consists of two parts: Part 1: Hash functions and asymmetric algorithms Part 2: Secure channel protocols and algorithms for signature creation devices</p>
--	---

Name	Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)
Brief Name	ETSI TR 101 375 V1.1.1 (1998-09)
Issuing Organisation	ETSI
Description	To prepare the distribution rules for GPRS encryption algorithm and provide an analysis of the GPRS algorithm.

Name	Security Algorithms Group of Experts (SAGE); Rules for the management of the GSM CTS standard Authentication and Key Generation Algorithms (CORDIAL)
Brief Name	ETSI TR 101 690 V1.1.1 (1999-08)
Issuing Organisation	ETSI
Description	Define the rules of management for the CTS algorithm.

Name	Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)
Brief Name	ETSI TR 101 740 V1.1.1 (1999-08)
Issuing Organisation	ETSI

Description	Specify the rules for the management of the Standard GSM GPRS Encryption Algorithm 2 (GEA2). To specify the management structure of GEA2. To specify the procedures for delivering the GEA2 to Approved Recipients and the items to be delivered. To specify the criteria for approving an organisation for receipt6 of the GEA2 and the responsibilities of an Approved Recipient. To define the Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.
--------------------	---

Name	TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies
Brief Name	ETSI TR 102 038 V1.1.1 (2002-04)
Issuing Organisation	ETSI
Description	<p>The present document represents a very first version of a XML format for Signature Policies able to contain information on Signature Policies as specified by TS 101 733. The specifications given being so preliminary, a number of open issues for discussion and even definitions appear throughout the document.</p> <p>Successive versions will gradually improve the new XML types defined aligning them with current efforts in the XML arena.</p>

Name	International Harmonization of Electronic Signature Formats
Brief Name	ETSI TR 102 047 V1.2.1 (2005-03)
Issuing Organisation	ETSI
Description	<p>The present document presents the results of ongoing work to harmonize existing ETSI technical specification on electronic signature formats (TS 101 733 and TS 101 903) with other internationally recognized standards and related activities.</p> <p>The aim of the present document is to identify the way forward to meet the requirements of European Electronic Signature Directive 1999/93/EC for advanced electronic signatures in a manner which maximizes international interoperability.</p>

Name	Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies
Brief Name	ETSI TR 102 272 V1.1.1 (2003-12)
Issuing Organisation	ETSI
Description	No specific format is mandated for a signature policy specification. A

	signature policy may be specified either a) in a free form document for human interpretation; or b) in a structured form using an agreed syntax and encoding. The present document specifies the various components of a signature policy and one specific format using ASN.1 syntax and DER encoding.
--	--

Name	Electronic Signature Formats
Brief Name	ETSI TS 101 733
Issuing Organisation	ETSI
Description	This standard defines a format for Advanced Electronic Signatures based on the existing standard format that dominates the email and document security market (i.e. CMS - Internet specification RFC 2630). It also specifies how time-stamping or trusted archiving services may be used to ensure that the electronic signature remains valid for long periods so that it can be presented later as evidence in case of a dispute. This standard has been submitted to the IETF in two separate parts and approved as RFC 3126 and RFC 3125, respectively, further promoting the globalization of EESSI results.

Name	Qualified Certificate profile
Brief Name	ETSI TS 101 862 V1.3.3 (2006-01)
Issuing Organisation	ETSI
Description	The present document defines a technical format for Qualified Certificates that can be used by issuers of Qualified Certificates to comply with annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. This profile is based on the Qualified Certificate profile standard RFC 3039.

Name	XML Advanced Electronic Signatures (XAAdES)
Brief Name	ETSI TS 101 903 V1.2.2 (2004-04)
Issuing Organisation	ETSI
Description	The present document defines XML formats for advanced electronic signatures that remain valid over long periods, are compliant the European Directive and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature.

	<p>The present document is based on the use of public key cryptography to produce digital signatures, supported by public key certificates.</p> <p>The present document uses a signature policy, implicitly or explicitly referenced by the signer, as one possible basis for establishing the validity of an electronic signature.</p> <p>The present document uses time-stamps or trusted records (e.g. time-marks) to prove the validity of a signature long after the normal lifetime of critical elements of an electronic signature and to support non-repudiation. It also specifies the optional use of additional time-stamps to provide very long-term protection against key compromise or weakened algorithms.</p> <p>The present document then, specifies the use of the corresponding trusted service providers (e.g. time-stamping authorities), and the data that needs to be archived (e.g. cross certificates and revocation lists). An advanced electronic signature aligned with the present document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later.</p>
--	--

Name	Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
Brief Name	ETSI TS 102 023 V1.2.1 (2003-01)
Issuing Organisation	ETSI
Description	<p>The present document specifies policy requirements relating to the operation of Time-stamping Authorities (TSA). The present document defines policy requirements on the operation and management practices of TSA such that subscribers and relying parties may have confidence in the operation of the time-stamping services.</p> <p>These policy requirements are primarily aimed at time-stamping services used in support of qualified electronic signatures (i.e. in line with article 5.1 of the European Directive on a community framework for electronic signatures) but may be applied to any application requiring proving that a datum existed before a particular time.</p> <p>These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.</p> <p>The present document may be used by independent bodies as the basis for confirming that a TSA may be trusted for providing time-stamping services.</p>

Name	Health informatics - Messages and communication - Web access to DICOM persistent objects
Brief Name	ISO 17432:2004
Issuing Organisation	ISO

Description	<p>This standard specifies a web-based service for accessing and presenting DICOM (Digital Imaging and Communications in Medicine) persistent objects (e.g. images, medical imaging reports). This is intended for distribution of results and images to healthcare professionals. It provides a simple mechanism for accessing a DICOM persistent object from HTML pages or XML documents, through HTTP/HTTPS protocol, using DICOM UID (Unique Identifiers). Data may be retrieved either in a presentation-ready form as specified by the requester (e.g. JPEG or GIF) or in a native DICOM format.</p> <p>It does not support facilities for web searching of DICOM images. It relates only to DICOM persistent objects (not to other DICOM objects or to non-DICOM objects). Access control beyond the security mechanisms generally available to web applications is outside the scope of this International Standard.</p>
--------------------	--

Name	Health Informatics - Messages and communication - Format of length limited globally unique string identifiers
Brief Name	ISO 18232:2006
Issuing Organisation	ISO
Description	This standard specifies the encoding and length for globally unique identifiers for data objects used in healthcare exchanged as alphanumeric strings.

Name	Information technology – Security techniques – Non-repudiation
Brief Name	ISO IEC 13888
Issuing Organisation	ISO
Description	<p>This standard consists of three parts:</p> <p>Part 1: General</p> <p>Part 2: Mechanisms using symmetric techniques</p> <p>Part 3: Mechanisms using asymmetric techniques</p> <p>Part 1 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. The goal of the non-repudiation service is to generate, collect, maintain, make available and verify evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. There are two main types of evidence, the nature of which depends on cryptographic techniques employed: the secure envelopes generated by an evidence-generating authority using symmetric cryptographic techniques, and digital signatures generated by an evidence generator or an evidence generating authority using asymmetric cryptographic techniques. Non-</p>

repudiation mechanisms generic to the various non-repudiation services are described first. The different parts of this International Standard provide non-repudiation mechanisms for the following phases of non-repudiation: evidence generation, transfer, storage, retrieval and verification. The non-repudiation mechanisms are then applied to a selection of specific non-repudiation services such as non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport. Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens specific to each non-repudiation service. Non-repudiation tokens consist of secure envelopes and/or digital signatures and, optionally, of additional data.

The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non occurrence of the event or action. Part 2 of ISO/IEC 13888 provides descriptions of generic structures that can be used for non-repudiation services, and of some specific, communication related mechanisms which can be used to provide non-repudiation of origin (NRO), non-repudiation of delivery (NRD), non-repudiation of submission (NRS), and non-repudiation of transport (NRT) services. Other non-repudiation services can be built using the generic structures described in Clause 8 in order to meet the requirements defined by the security policy.

This part of ISO/IEC 13888 relies on the existence of a trusted third party (TTP) to prevent fraudulent repudiation. Usually an on-line trusted third party is needed.

The goal of the Non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non occurrence of the event or action. Part 3 of ISO/IEC 13888 specifies mechanisms for the provision of some specific, communication related non-repudiation services using asymmetric techniques.

Non-repudiation mechanisms are specified to establish the following services: non-repudiation of origin, non-repudiation of delivery, non-repudiation of submission, and non-repudiation of transport.

Non-repudiation mechanisms involve the exchange of non-repudiation tokens specific for each non-repudiation service. Non-repudiation tokens consist of digital signatures and additional data. Non-repudiation tokens shall be stored as non-repudiation information that may be used subsequently in case of disputes.

Depending on the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, additional information may be required to complete the non-repudiation information, e.g., evidence including a trusted time stamp provided by a Time Stamping Authority, evidence provided by a notary which provides assurance about the action or event performed by one or more entities.

	Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are described in the multipart Standard of Security Frameworks for open systems - Part 4: Non-repudiation Framework, ISO/IEC 10181-4.
--	---

Name	Information technology - Security techniques - Digital signature with appendix
Brief Name	ISO IEC 14888
Issuing Organisation	ISO
Description	<p>This standard consists of three parts:</p> <p>Part 1: General</p> <p>Part 2: Identity-based mechanisms</p> <p>Part 3: Discrete logarithm based mechanisms</p> <p>This standard specifies several digital signature mechanisms with appendix for messages of arbitrary length and is applicable in schemes providing entity authentication, data origin authentication, non-repudiation, and integrity of data.. Part 1 contains general principles and requirements for digital signatures with appendix. It also contains definitions and symbols common to all parts of ISO/IEC 14888.</p> <p>Part 2 of ISO/IEC 14888 specifies the general structure and the fundamental procedures which constitute the signature and verification processes of an identity-based digital signature mechanism with appendix for messages of arbitrary length.</p> <p>Part 3 specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem. It provides a general description of a digital signature with appendix mechanism, and a variety of mechanisms that provide digital signatures with appendix.</p> <p>For each mechanism, part 3 specifies the process of generating keys, the process of producing signatures, and the process of verifying signatures.</p> <p>The verification of a digital signature requires the signing entity's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signing entity, or more precisely, with (parts of) the signing entity's identification data. This association may be provided by another means that is not covered in part 3. Whatever the nature of such means the scheme is then said to be 'certificate-based'. If not, the association between the correct verification key and the signing entity's identification data is somehow inherent in the verification key itself. In such a case, the scheme is said to be 'identity-based'. Depending on the two different ways of checking the correctness of the verification keys, the digital signature mechanisms specified in part 3 are categorized in two groups: certificate-based and identity-based.</p>

Name	Information technology - Security techniques - Digital signature schemes giving message recovery
Brief Name	ISO IEC 9796
Issuing Organisation	ISO
Description	<p>This standard consists of two parts (part 1 was withdrawn):</p> <p>Part 2: Integer factorization based mechanisms</p> <p>Part 3: Discrete logarithm based mechanisms</p> <p>Part 2 specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. The security of all three schemes is based on the difficulty of factorizing large numbers. All three schemes can provide either total or partial message recovery.</p> <p>The method for key production for the three signature schemes is specified in this part of ISO/IEC 9796. However, techniques for key management and for random number generation (as required for the randomized signature scheme), are outside the scope of this part of ISO/IEC 9796.</p> <p>Users of this International Standard are, wherever possible, recommended to adopt the second mechanism (Digital signature scheme 2). However, in environments where generation of random variables by the signer is deemed infeasible, then Digital signature scheme 3 is recommended. Digital signature scheme 1 shall only be used in environments where compatibility is required with systems implementing the first edition of this International Standard. However, Digital signature scheme 1 is only compatible with systems implementing the first edition of this International Standard that use hash-codes of at least 160 bits.</p> <p>A digital signature in electronic exchange of information provides the same kind of facilities that are expected from a handwritten signature in paper-based mail. Hence it is applicable to providing entity authentication, data origin authentication, non-repudiation, and integrity of data.</p> <p>Part 3 specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead.</p> <p>It specifies mechanisms based on the discrete logarithm problem of a finite field or an elliptic curve over a finite field.</p> <p>Part 3 defines types of redundancy: natural redundancy, added redundancy, or both.</p> <p>It gives the general model for digital signatures giving partial or total message recovery aiming at reducing storage and transmission overhead.</p> <p>Part 3 specifies six digital signature schemes giving data recovery: NR, ECNR, ECMR, ECAO, ECPV, and ECKNR. NR is defined on a prime field; ECNR, ECMR, ECAO, ECPV, and ECKNR are defined on an elliptic curve over a finite field.</p>

Name	Information technology -- Security techniques -- Message Authentication Codes (MAC)
Brief Name	ISO IEC 9797
Issuing Organisation	ISO
Description	<p>This standard consists of two parts:</p> <p>Part 1: Mechanisms using a block cipher</p> <p>Part 2: Mechanisms using a dedicated hash-function</p> <p>Part 1 of ISO/IEC 9797 specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorised manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) k^* and secrecy of the key, on the block length (in bits) n and strength of the block cipher, on the length (in bits) m of the MAC, and on the specific mechanism.</p> <p>Part 2 specifies three MAC algorithms that use a secret key and a hash-function (or its round-function) with an n-bit result to calculate an m-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorised manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) k and secrecy of the key, on the length (in bits) n of a hash-code produced by the hash-function, on the strength of the hash-function, on the length (in bits) m of the MAC, and on the specific mechanism.</p> <p>The three mechanisms specified in part 2 are based on the dedicated hash-functions specified in ISO/IEC 10118-3. The first mechanism specified in part 2 is commonly known as MDx-MAC. It calls the complete hash-function once, but it makes a small modification to the round-function by adding a key to the additive constants in the round-function. The second mechanism specified in part 2 is commonly known as HMAC. It calls the complete hash-function twice. The third mechanism specified in part 2 is a variant of MDx-MAC that takes as input only short strings (at most 256 bits). It offers a higher performance for applications that work with short input strings only.</p> <p>Part 2 can be applied to the security services of any security architecture, process, or application.</p>

Name	Information technology - Security techniques - Entity authentication
-------------	--

Brief Name	ISO IEC 9798
Issuing Organisation	ISO
Description	<p>This standard consists of six parts:</p> <p>Part 1: General</p> <p>Part 2: Mechanisms using symmetric encipherment algorithms</p> <p>Part 3: Mechanisms using digital signature techniques</p> <p>Part 4: Mechanisms using a cryptographic check function</p> <p>Part 5: Mechanisms using zero-knowledge techniques</p> <p>Part 6: Mechanisms using manual data transfer</p> <p>Part 1 specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party.</p> <p>Part 2 specifies entity authentication mechanisms using symmetric encipherment algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require a trusted third party for the establishment of a common secret key, and realize mutual or unilateral entity authentication.</p> <p>Part 3 specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.</p> <p>Part 4 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.</p> <p>Part 5 specifies authentication mechanisms in the form of exchange of information between a claimant and a verifier.</p> <p>Part 6 specifies four entity authentication mechanisms based on manual data transfer between authenticating devices. Such mechanisms may be appropriate in a variety of circumstances. One such application occurs in Personal Area Networks, where the owner of two personal devices capable of wireless communications wishes them to perform an entity authentication procedure as part of the process of preparing them for use in the network.</p>

Name	Trusted end-to-end information flows
Brief Name	ISO TR 21089:2004
Issuing Organisation	ISO
Description	<p>This standard offers a guide to trusted end-to-end information flow for health(care) records and to the key trace points and audit events in the electronic entity/act record lifecycle (from point of record origination to each ultimate point of record access/use). It also offers recommendations regarding the trace/audit detail relevant to each.</p> <p>It offers recommendations of best practice for healthcare providers, health record stewards, software developers and vendors, end users and other stakeholders, including patients.</p>

Name	Digital Imaging and Communications in Medicine
Brief Name	DICOM
Issuing Organisation	NEMA
Description	<p>DICOM (Digital Imaging and Communications in Medicine) defines the coding of medical images, the protocols of interchange between both sides and a security policy to hide information from third people.</p> <p>DICOM 3.0 has added waveform support to allow EEG and ECG interchanges. Website of Reference : http://www.dclunie.com</p>

5.10. Infrastructure Standards

All types of medical, clinical, and administrative information systems need to extensively communicate with each other. An appropriate (security) infrastructure needs to be established. Standards allow for an infrastructure that fulfils the needs of the different application systems.

Table 5: List of Infrastructure Standards

ETSI TS 101 861 V1.3.1 (2006-01)	Time stamping profile
ISO IS 17090-1:2002	Health informatics - Public key infrastructure - Part 1: Framework and overview
ISO IS 17090-2:2002	Health informatics - Public key infrastructure - Part 2: Certificate profile
ISO IS 17090-3:2002	Health informatics - Public key infrastructure - Part 3: Policy management of certification authority
ISO TS 21091:2005	Health informatics - Directory services for security,

	communications and identification of professionals and patients
ISO TS 21298	Functional and structural roles
ISO IEC 27001:2005	Information technology - Security techniques - Information security management systems (ISMS) - Requirements
ISO/IEC 15816:2002 (ITU-T X.841)	Information technology - Security techniques - Security information objects for access control
ISO/IEC TR 14516:2002 (ITU-T X.842)	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services
ISO/IEC 15945:2002 (ITU-T X.843)	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
ITU-T X.1051	Information security management system - Requirements for telecommunications (ISMS-T)
NIST Special Publication 800-61	Computer Security Incident Handling Guide
CORBA	Common Object Request Broker Architecture

In the following, all of the standards listed above shall be explained in more detail. Standards containing more than one part (e.g. 17090) are listed just once.

Name	Time stamping profile
Brief Name	ETSI TS 101 861 V1.3.1 (2006-01)
Issuing Organisation	ETSI
Description	The present document is based on the Time Stamp Protocol (TSP) from IETF RFC 3161. It defines what a Time Stamping client must support and what a Time Stamping Server must support.

Name	Public key infrastructure
Brief Name	ISO IS 17090:2006
Issuing Organisation	ISO
Description	The three parts of the standard are separately usable. Part 1 defines the basic concepts of a healthcare public key infrastructure (PKI) and provides a scheme of interoperability requirements to establish a PKI enabled secure communication of health information. Part 2 specifies the certificate profiles required to interchange healthcare information within a single organization,

	<p>between different organizations and across jurisdictional boundaries. Part 3 gives guidelines for certificate management issues involved in implementing and operating a healthcare public key infrastructure (PKI).</p> <p>This standard consists of three parts:</p> <p>Part 1: Framework and overview</p> <p>Part 2: Certificate profile</p> <p>Part 3: Policy management of certification authority</p>
--	--

Name	Directory services for security, communications and identification of professionals and patients
Brief Name	ISO TS 21091:2005
Issuing Organisation	ISO
Description	<p>This standard defines minimal specifications for directory services for health care using the X.500 framework. This Technical Specification provides the common directory information and services needed to support the secure exchange of health care information over public networks. It addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction and international health care communications.</p> <p>The standard also supports directory services aiming to support identification of health professionals and organizations and the patients/consumers. The latter services include aspects sometimes referred to as master patient indices. The health care directory will only support standard LDAP Client searches. Specific implementation guidance, search criteria and support are out of scope of this document.</p>

Name	Information technology - Security techniques - Security information objects for access control
Brief Name	ISO/IEC 15816:2002 (ITU-T X.841)
Issuing Organisation	ISO
Description	<p>The scope of this standard is:</p> <ul style="list-style-type: none"> • the definition of guidelines for specifying the abstract syntax of generic and specific Security Information Objects (SIOs) for Access Control; • the specification of generic SIOs for Access Control; • the specification of specific SIOs for Access Control. <p>The scope of this standard covers only the “static” of SIOs through syntactic definitions in terms of ASN.1 descriptions and additional semantic explanations. It does not cover the “dynamics” of SIOs, for example rules relating to their creation and deletion. The dynamics of SIOs are a local</p>

	implementation issue.
--	-----------------------

Name	Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services
Brief Name	ISO/IEC TR 14516:2002 (ITU-T X.842)
Issuing Organisation	ISO
Description	<p>Associated with the provision and operation of a Trusted Third Party (TTP) are a number of security-related issues for which general guidance is necessary to assist business entities, developers and providers of systems and services, etc. This includes guidance on issues regarding the roles, positions and relationships of TTPs and the entities using TTP services, the generic security requirements, who should provide what type of security, what the possible security solutions are, and the operational use and management of TTP service security.</p> <p>This Technical Report provides guidance for the use and management of TTPs, a clear definition of the basic duties and services provided, of their description and their purpose, and the roles and liabilities of TTPs and entities using their services. It is intended primarily for system managers, developers, TTP operators and enterprise users to select those TTP services needed for particular requirements, their subsequent management, use and operational deployment, and the establishment of a Security Policy within a TTP. It is not intended to be used as a basis for a formal assessment of a TTP or a comparison of TTPs.</p> <p>This Technical Report identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public. Each of these major categories consists of several services which logically belong together.</p>

Name	Information technology - Security techniques - Specification of TTP services to support the application of digital signatures
Brief Name	ISO/IEC 15945:2002 (ITU-T X.843)
Issuing Organisation	ISO
Description	<p>This standard will define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents. It will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.</p> <p>Definitions of technical services and protocols are required to allow for the implementation of TTP services and related commercial applications.</p> <p>This standard focuses on:</p> <ul style="list-style-type: none"> • implementation and interoperability; • service specifications; and

	<ul style="list-style-type: none"> • technical requirements. <p>It does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in ITU-T Rec. X.842 ISO/IEC TR 14516, Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services.</p>
--	--

Name	Information security management system - Requirements for telecommunications (ISMS-T)
Brief Name	ITU-T X.1051
Issuing Organisation	ITU
Description	<p>This document specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS within the context of the telecommunication's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of individual telecommunications or parts thereof.</p> <p>The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to the customers and business partners of telecommunications organizations as well as to other interested telecommunications parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.</p>

Name	Computer Security Incident Handling Guide
Brief Name	NIST Special Publication 800-61
Issuing Organisation	NIST
Description	<p>This publication seeks to assist organisations in mitigating the risks from information security incidents by providing practical guidance on responding to incidents effectively and efficiently. Agencies are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements. This guide replaces NIST Special Publication 800-3, Establishing a Computer Security Incident Response Capability (CSIRC).</p> <p>This document presents general incident response guidelines that are independent of particular hardware platforms, operating systems, and applications. Specifically, it includes guidance on establishing an effective incident response program, but the primary focus of the document is detecting, analysing, prioritising, and handling incidents.</p>

Name	Common Object Request Broker Architecture
Brief Name	CORBA

Issuing Organisation	OMG
Description	<p>CORBA is an architecture and specification for creating, distributing, and managing distributed program objects in a network. It allows programs at different locations and developed by different vendors to communicate in a network through an "interface broker".</p> <p>CORBA consists of several specifications, amongst others:</p> <ul style="list-style-type: none"> • CORBA Security Services • Common Security Interoperability Services • Resource Access Decision Service • Clinical Observations Access Service

5.11. Privacy Standards

The following list contains relevant privacy standards and respective specifications mainly focused on privacy of patient / citizen and health professional. Privacy includes identity management as well as Anonymisation and Pseudonymisation.

Table 6: List of Privacy Standards

ASTM E1714-00	Standard guide for properties of a Universal Healthcare Identifier
ASTM E1987-98	Standard guide for individual rights regarding health information
CEN EN 14484:2004	Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy
CEN EN 14485:2004	Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive
CEN ENV 12924	Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems
ISO IEC DTS 25237	Health Informatics: Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services
ISO TS 21091	Health Informatics - Directory Services for Security, Communications, and Identification of Professionals and Patients
ISO 22857:2004	Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information
ISO TS 22600-1:2006	Health informatics - Privilege management and access control - Part 1: Overview and policy management
ISO TS 22600-2:2006	Health informatics - Privilege management and access control - Part 2: Formal models

ISO/IEC PDTS 25237	Health Informatics: Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services
OASIS 200201	Directory Services Mark-up Language (DSML) v2.0
OASIS SAML	Security Assertion Mark-up Language (SAML) v2.0
OASIS SPML	Service Provisioning Markup Language (SPML) v2.0
OASIS XACML	eXtensible Access Control Mark-up Language TC v2.0 (XACML)

The majority of these standards and normative references will be explained in more detail below.

Name	Standard guide for properties of a Universal Healthcare Identifier
Brief Name	ASTM E1714-00
Issuing Organisation	ASTM
Description	This guide covers a set of requirements outlining the properties of a national system creating a universal health care identifier (UHID). Use of the UHID is expected to be limited to the population of the United States.

Name	Standard guide for individual rights regarding health information
Brief Name	ASTM E1987-98
Issuing Organisation	ASTM
Description	This guide outlines the rights of individuals, both patients and providers, regarding health information and recommends procedures for the exercise of those rights. This guide is intended to amplify Guide E1869.

Name	Health Informatics - International transfer of personal health data covered by the EU Data Protection Directive - High level security policy
Brief Name	CEN EN 14484:2004
Issuing Organisation	CEN
Description	This item will provide guidance on the data protection policy which should be implemented by organisations which are participants in international applications which involve transfer of person identifiable data across national borders and which require compliance with the EU Data Protection Directive.

Name	Health Informatics - Guidance for handling personal health data in international applications in the context of the EU Data Protection Directive
Brief Name	CEN EN 14485:2004
Issuing Organisation	CEN
Description	This item will provide guidance on the data protection policy which should be implemented by organisations which are participants in international applications which involve transfer of person identifiable data across national borders and which require compliance with the EU Data Protection Directive.

Name	Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems
Brief Name	CEN ENV 12924
Issuing Organisation	CEN
Description	Categorises automated information systems from health care under security considerations.

Name	Health Informatics: Pseudonymisation Practices for the Protection of Personal Health Information and Health Related Services
Brief Name	ISO IEC DTS 25237
Issuing Organisation	ISO
Description	<p>This technical specification contains principles and requirements for privacy protection using pseudonymisation services for the protection of personal health information.</p> <p>The technical specification:</p> <ul style="list-style-type: none"> • defines basic concepts for identification and pseudonymisation, • gives an overview of different use cases for pseudonymisation that can be both reversible and irreversible, • defines at least one methodology for pseudonymisation services including organizational as well as technical aspects, • gives a guide to risk assessment for re-identification, • specifies a policy framework and minimal requirements for trustworthy practices for the operations of a pseudonymisation service, • specifies a policy framework and minimal requirements for controlled re-identification, and • interoperability specification of services interfaces.

Name	Directory services for security, communications and identification of professionals and patients
Brief Name	ISO TS 21091
Issuing Organisation	ISO
Description	<p>This standard defines minimal specifications for directory services for health care using the X.500 framework. This Technical Specification provides the common directory information and services needed to support the secure exchange of health care information over public networks. It addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction and international health care communications.</p> <p>The standard also supports directory services aiming to support identification of health professionals and organizations and the patients/consumers. The latter services include aspects sometimes referred to as master patient indices. The health care directory will only support standard LDAP Client searches. Specific implementation guidance, search criteria and support are out of scope of this document.</p>

Name	Guidelines on data protection to facilitate trans-border flow of personal health information
Brief Name	ISO TS 22857:2004
Issuing Organisation	ISO
Description	<p>This standard provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organization should adopt to ensure compliance with those principles.</p>

Name	Privilege management and access control
Brief Name	ISO TS 22600:2006
Issuing Organisation	ISO

Description	<p>This standard defines privilege management and access control services that are necessary for communication and use of distributed health information across domain and security borders. It establishes principles and specifies needed services for management of authorisations and access control. The standard specifies the required component-based concepts and is intended to support whose technical implementation. It doesn't specify the use of those concepts in the specific clinical process chains.</p> <p>This standard consists of three parts: Part 1: Overview and policy management Part 2: Formal models Part 3: Implementations</p> <p>This document originally was prepared in CEN and then completely revised in ISO with main focus privilege management.</p>
--------------------	--

Name	Directory Services Mark-up Language (DSML) v2.0
Brief Name	OASIS 200201
Issuing Organisation	OASIS
Description	Directory Services Mark-up Language (DSML) is a standard from OASIS for access to directory service via XML and SOAP

Name	Security Assertion Mark-up Language (SAML) v2.0
Brief Name	OASIS SAML
Issuing Organisation	OASIS
Description	SAML is part of the web services and is used for the secure exchange of authentication and authorisation information between security systems and e-business platforms of partners.

Name	Service Provisioning Markup Language (SPML) v2.0
Brief Name	OASIS SPML
Issuing Organisation	OASIS
Description	The Service Provisioning Markup language is the open standard protocol for the integration and interoperation of service provisioning requests. It is an XML-based language that facilitates the exchange of provisioning information among applications and organisations, corporations, or agencies. Provisioning, according to the technical group providing support for it, is "the automation of all the steps required to manage (setup, amend, and revoke) user or system access entitlements or data relative to electronically

	published services."
--	----------------------

Name	eXtensible Access Control Mark-up Language TC v2.0 (XACML)
Brief Name	OASIS XACML
Issuing Organisation	OASIS
Description	XACML is a mark-up language for web services. It is in close connection to SAML and is an enhancement of this language. XACML defines how policy information for access control is structured and will be transferred. For this reason policy developer can define what web services can do with which access privileges for which documents. The advantage of this common rule language is the administration of the compliance of access policies for the whole enterprise.

5.12. Safety Standards

The following list contains relevant medical safety standards and respective specifications mainly focused on medical safety aspects. Technical safety as well as mechanical and electrical safety aspects will be dealt with in chapter 9 of this deliverable.

Table 7: List of Safety Standards

CEN CR 13694	CEN Report: Health Informatics - Safety and security related software quality standards for healthcare (SSQS)
CEN TR 15299	Health informatics - Safety procedures for identification of patients and related objects
CEN TS 15260	Health informatics - Categorisation of risks from health informatics products
ISO DTS 25238	Health Informatics - Classification of safety risks from health informatics products
ISO TR 21730:2005	Health informatics - Use of mobile wireless communication and computing technology in healthcare facilities - Recommendations for the management of unintentional electromagnetic interference with medical devices

The majority of these standards and normative references will be explained in more detail below.

Name	Safety and Security Related Software Quality Standards for Healthcare (SSQS)
-------------	--

Brief Name	CEN CR 13694
Issuing Organisation	CEN
Description	Proposes several quality norms related to security and protection in e-Health software. It associates the system type with the appropriate security measures.

Name	Health informatics - Safety procedures for identification of patients and related objects
Brief Name	CEN TR 15299
Issuing Organisation	CEN
Description	<p>This standard defines a framework for:</p> <ul style="list-style-type: none"> • the definition of safety critical objects in the healthcare process (MOS: Minimum Object Set) and the • related safety critical data (MDS: Minimum Data Set) according to modelling methodologies as IDEF or UML, • the definition of the rules of interaction among safety critical objects in the process, and • the acquisition and processing of safety critical data by health informatics systems. <p>Finally, this standard defines a possible roadmap for a stepwise approach for an effective standardisation activity in the area of patient safety, including the main health sub-processes that involve the hospitalised patient as: Laboratory Medicine and Pathology, Bio-imaging, Drug Therapy Management, Blood Transfusion Management, Surgery Management. Such sub-processes can be considered, from a process modelling perspective, a case-mix that covers most of the process requirements of patient safety for the hospitalised patient and an appropriate starting point for the health processes that involve non-hospitalised patients.</p>

Name	Health informatics - Categorisation of risks from health informatics products
Brief Name	CEN TS 15260:2006
Issuing Organisation	CEN
Description	This document is concerned with the safety of patients and gives guidance on the analysis and categorisation of hazards and risks to patients from health informatics products, to allow any product to be assigned to one of five risk classes. It applies to hazards and risks which could cause harm to a patient. Other risks such as financial or organisational are out of scope unless they have the potential to harm a patient. This document applies to any health

	informatics product whether or not it is placed on the market and whether or not it is for sale or free of charge. Examples of the application of the classification scheme are given. This document does not apply to any software which is encompassed within EU Medical Devices Directives.
--	--

Name	Health Informatics - Classification of safety risks from health informatics products
Brief Name	ISO DTS 25238
Issuing Organisation	ISO
Description	<p>This standard is concerned with the safety of patients and gives guidance on the analysis and categorisation of hazards and risks to patients from health informatics products, to allow any product to be assigned to one of five risk classes. It applies to hazards and risks which could cause harm to a patient. Other risks such as financial or organisational are out of scope unless they have the potential to harm a patient.</p> <p>This standard applies to any health informatics product whether or not it is placed on the market and whether or not it is for sale or free of charge. Examples of the application of the classification scheme are given.</p> <p>This standard does not apply to any software which is necessary for the proper application or functioning of a medical device.</p>

Name	Health informatics - Use of mobile wireless communication and computing technology in healthcare facilities - Recommendations for the management of unintentional electromagnetic interference with medical devices
Brief Name	ISO TR 21730:2005
Issuing Organisation	ISO
Description	<p>This standard provides guidance for the deployment, use and management of mobile wireless communication and computing equipment in the healthcare facility in a way that helps mitigate potential hazards due to electromagnetic interference (EMI) with medical devices. The recommendations recognize the different resources, needs, concerns and environments of healthcare organisations around the world and provide detailed management guidelines for healthcare organisations that desire full deployment of mobile wireless communication and computing technology throughout their facility, as well as selective restrictions for healthcare organisations that have decided comprehensive management procedures are not feasible, practical, or desirable at the present time. The recommendations also distinguish between controlled systems used by doctors and staff for healthcare-specific communication and health informatics transport vs. non-controlled (personal) mobile wireless equipment randomly brought into the facility by visitors,</p>

patients and the healthcare organisation workforce.

5.13. Token Standards

More and more, cards and other security tokens take control of supporting identity management, identification and authentication procedures as well as entitlement functionality. For developing applications that have a relation to human beings (health professional and patient) or a relation to medical devices (those using plug-in card solutions), respective standards, specifications and normative references might be of importance for SENSATION as well. Some of the relevant standards in this respect are listed below.

Table 8: List of Token Standards

CEN ENV13729	Health Informatics - Secure user identification - Strong authentication using microprocessor cards
CEN ENV 1387	Machine readable cards - Health care applications - Cards: General characteristics
CEN ENV 1867	Machine readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers
CEN ENV 13735	Health Informatics - Interoperability of patient connected medical devices
ISO 20301	Health Informatics - Health cards - general characteristics
ISO 20302	Health Informatics - Health cards - numbering system and registration procedure for issuer identifiers
ISO 21549	Health Informatics - Patient health card data

In the following, the standards and specifications will be described in some detail. Most of the standards are either under development or under review. So for SENSATION application, please refer to the information sources of the respective Standards Developing Organisations (SDO).

Name	Secure user identification - Strong authentication using microprocessor cards
Brief Name	CEN ENV 13729
Issuing Organisation	CEN
Description	This standard defines secure user identification procedures respectively a method for strong authentication of the identity of a user of a health information system where the user is equipped with a microprocessor card. By system is meant primarily a general purpose computer system with hardware ranging from a personal computer to a mainframe. Dedicated embedded systems with special operating systems are not considered, nor are

access control to data on a smart card such as a patient data card. However this standard does not preclude the addition of this functionality to a user card. The main focus of consideration is on users who are the healthcare persons, registered professionals and other staff using health information. In situations when patients are allowed to use healthcare information systems directly to access their personal data and secure user identification is needed, this standard may also be used. The authentication method defined in this standard employs a cryptographic challenge-response protocol suitable for both remote authentications over unprotected networks as well as for authentication within a local system. This standard specifies the cryptographic algorithm to be employed and which must be available in the microprocessor card as well as in any authenticating system, remote or local, in the implementation of the defined strong authentication method. This standard defines a local authentication protocol used in the interface between a local system and the microprocessor card. This protocol is based on available ISO/IEC standards. For local authentication in a Windows based environment commonly accepted card terminal layer interfaces should be used. However, the details of the various layers between the different components of the local system such as authentication services, interface device unit (card reader) and the operating system of the local system is outside the scope of this pre-standard. This standard also defines a remote authentication protocol for the interface between a local system and a remote system. The method endorsed by this pre-standard originates from the Internet Engineering Task Force (IETF) work with the TLS protocol (Transport layer Security). A cipher suite profile suitable for healthcare use is added to this basic protocol. The method for strong authentication defined in this standard requires Trusted Third Party (TTP) services. While these are outlined in the authentication reference model and some functional requirements on the TTP services are included, the detailed specifications of these are outside the scope of this pre-standard. The requirements on procedures for the process of the card authenticating the user are also defined, focusing on PIN-code handling. Provision has been made for the possible future addition of biometric techniques. The identity authenticated by the method in this standard is held in a set of data provided in a public key certificate specification based on the ISO/IEC 9594-8 (X.509) standard. This standard includes some additional requirements on such data for cross border use. A national or local implementation profile will frequently be needed for additional specification. This authentication method may also be used to authenticate the role/registered professional class using the same basic technology. This status information may be used for authorisation, access control, accountability (including non-repudiation, data origin authentication, integrity) etc., but such additional functions as these are outside the scope of this standard. One example of a data structure for use in certificates is given in informative annex B. While the technology of asymmetric encryption used for strong authentication can also be used to provide a mechanism for digital signature creation and confidentiality services, these possible services of the

	same card are outside the scope of this standard. This standard defines a mechanism that can be used in provision of the general aspects of security for healthcare communication as described in ENV 13608-1
--	---

Name	Machine readable cards - Health care applications - Cards: General characteristics
Brief Name	CEN ENV 1387
Issuing Organisation	CEN
Description	The document is one of a series of standards describing the characteristics of machine readable cards in the health care sector and the use of such cards for European interchange. It specifies the physical characteristics of cards and the recording techniques, but not the security requirements.

Name	Machine readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers
Brief Name	CEN ENV 1867
Issuing Organisation	CEN
Description	The document specifies the application and registration procedures for numbers assigned to issuers of cards used for health care, health care coverage or health care entitlement, that comply with prEN 1387.

Name	Interoperability of patient connected medical devices
Brief Name	CEN ENV 13735
Issuing Organisation	CEN
Description	The standard sets up the basis of interoperability among patient connected devices taking account of VITAL standard to active device and signal interoperability.

Name	Health Informatics - Health cards - general characteristics
Brief Name	ISO 20301
Issuing Organisation	ISO
Description	This standard is designed to confirm the identities of both the healthcare application provider and the health card holder in order that information may be exchanged by using cards issued for healthcare service. It focuses on the machine-readable cards of ID-1 type defined in ISO/IEC 7810 that are

	<p>issued for healthcare services provided in a service area that crosses the national borders of two or more countries/areas.</p> <p>The standard applies to healthcare data cards where the issuer and the application provider are the same party. It applies directly or refers to existing ISO standards for the physical characteristics and recording techniques. Security issues should follow the requirements of each healthcare data card system.</p> <p>In addition, this International Standard regulates the visual information written on the healthcare data card.</p>
--	--

Name	Health Informatics - Health cards - numbering system and registration procedure for issuer identifiers
Brief Name	ISO 20302
Issuing Organisation	ISO
Description	<p>This standard is designed to confirm, via a numbering system and registration procedure, the identities of both the healthcare application provider and the health card holder in order that information may be exchanged by using cards issued for healthcare service. It focuses on the machine-readable cards of ID-1 type defined in ISO/IEC 7810 that are issued for healthcare services provided in a service area that crosses the national borders of two or more countries/areas.</p> <p>The standard applies to healthcare data cards where the issuer and the application provider are the same party. It applies directly, or refers, to existing ISO standards for physical characteristics and recording techniques. Security issues follow the requirements of each healthcare data card system.</p> <p>In addition, this International Standard regulates the visual information written on the healthcare data card.</p>

Name	Health Informatics - Patient health card data
Brief Name	ISO 21549
Issuing Organisation	ISO
Description	<p>ISO standard for structure and content of identification and medical data sets on the card.</p> <p>This standard consists of eight parts:</p> <p>Part 1: General structure</p> <p>Part 2: Common objects</p> <p>Part 3: Limited clinical data</p> <p>Part 4: Extended clinical data</p> <p>Part 5: Identification data</p>

Part 6: Administrative data Part 7: Electronic prescription Part 8: Links

5.14. Quality Standards

Healthcare and welfare information systems of any type regardless whether they are micro-systems or macro-systems need to fulfil requirements coming from security, safety and privacy as well as requirements in terms of quality and reliability. The well-known standards BS 7799 and the German “BSI-Grundschutzhandbuch” (Manual of Basic Security and Safety Requirements) can be considered such standards.

As far as quality of services and reliability of the information systems are concerned, the respective standards need to contain both technical and administrative parts. Again, some standards might easily be taken to another chapter of this overview as they do not deal with a single orientation but with different views on different aspects.

Table 9: List of Quality Standards

ASTM E2117-00	Standard guide for identification and establishment of a quality assurance program for medical transcription
ISO 13485:2003	Medical devices - Quality management systems - Requirements for regulatory purposes
ISO 14969:2004	Medical devices - Quality management systems - Guidance on the application of ISO 13485
ISO 15378:2006	Primary packaging materials for medicinal products - Particular requirements for the application of ISO 9001:2000, with reference to Good Manufacturing Practice (GMP)
ISO 9000:2005	Quality management systems - Fundamentals and vocabulary
ISO 9001:2000	Quality management systems - Requirements
ISO TR 13352:1997	Guidelines for interpretation of ISO 9000 series for application within the iron ore industry
ISO TS 16949:2002	Quality management systems - Particular requirements for the application of ISO 9001:2000 for automotive production and relevant service part organizations
IWA 4:2005	Quality management systems - Guidelines for the application of ISO 9001:2000 in local government
CEN CR 13694	CEN Report: Health Informatics - Safety and security related software quality standards for healthcare (SSQS)

The majority of these standards and normative references will be explained in more detail below.

Name	Standard guide for identification and establishment of a quality assurance program for medical transcription
Brief Name	ASTM E2117-00
Issuing Organisation	ASTM
Description	<p>It establishes a quality assurance program for dictation, medical transcription, and related processes. Quality assurance is necessary to ensure the accuracy of healthcare documentation.</p> <p>This guide establishes essential and desirable elements for quality healthcare documentation, but it is not purported to be an exhaustive list.</p>

Name	Medical devices - Quality management systems - Requirements for regulatory purposes
Brief Name	ISO 13485:2003
Issuing Organisation	ISO
Description	<p>ISO 13485:2003 specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer requirements and regulatory requirements applicable to medical devices and related services.</p> <p>The primary objective of ISO 13485:2003 is to facilitate harmonized medical device regulatory requirements for quality management systems. As a result, it includes some particular requirements for medical devices and excludes some of the requirements of ISO 9001 that are not appropriate as regulatory requirements. Because of these exclusions, organizations whose quality management systems conform to this International Standard cannot claim conformity to ISO 9001 unless their quality management systems conform to all the requirements of ISO 9001.</p> <p>All requirements of ISO 13485:2003 are specific to organizations providing medical devices, regardless of the type or size of the organization.</p> <p>If regulatory requirements permit exclusions of design and development controls, this can be used as a justification for their exclusion from the quality management system. These regulations can provide alternative arrangements that are to be addressed in the quality management system. It is the responsibility of the organization to ensure that claims of conformity with ISO 13485:2003 reflect exclusion of design and development controls.</p> <p>If any requirement(s) in Clause 7 of ISO 13485:2003 is(are) not applicable due to the nature of the medical device(s) for which the quality management system is applied, the organization does not need to include such a requirement(s) in its quality management system.</p>

	The processes required by ISO 13485:2003, which are applicable to the medical device(s), but which are not performed by the organization, are the responsibility of the organization and are accounted for in the organization's quality management system.
--	---

Name	Medical devices - Quality management systems - Guidance on the application of ISO 13485
Brief Name	14969:2004
Issuing Organisation	ISO
Description	<p>This standard provides guidance for the application of the requirements for quality management systems contained in ISO 13485. It does not add to, or otherwise change, the requirements of ISO 13485. It does not include requirements to be used as the basis of regulatory inspection or certification assessment activities.</p> <p>This guidance can be used to better understand the requirements of ISO 13485 and to illustrate some of the variety of methods and approaches available for meeting the requirements of ISO 13485.</p>

Name	Primary packaging materials for medicinal products - Particular requirements for the application of ISO 9001:2000, with reference to Good Manufacturing Practice (GMP)
Brief Name	ISO 15378:2006
Issuing Organisation	ISO
Description	<p>This standard specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide primary packaging materials for medicinal products, which consistently meet customer requirements, including regulatory requirements and International Standards applicable to primary packaging materials.</p> <p>It is an application standard for the design, manufacture and supply of primary packaging materials for medicinal products. It is also applicable for certification purposes.</p>

Name	Quality management systems - Fundamentals and vocabulary
Brief Name	ISO 9000:2005
Issuing Organisation	ISO
Description	This standard describes fundamentals of quality management systems, which form the subject of the ISO 9000 family, and defines related terms.

	<p>It is applicable to the following:</p> <ul style="list-style-type: none"> a) organizations seeking advantage through the implementation of a quality management system; b) organizations seeking confidence from their suppliers that their product requirements will be satisfied; c) users of the products; d) those concerned with a mutual understanding of the terminology used in quality management (e.g. suppliers, customers, regulators); e) those internal or external to the organization who assess the quality management system or audit it for conformity with the requirements of ISO 9001 (e.g. auditors, regulators, certification/registration bodies); f) those internal or external to the organization who give advice or training on the quality management system appropriate to that organization; g) developers of related standards.
--	--

Name	Quality management systems - Requirements
Brief Name	ISO 9001:2000
Issuing Organisation	ISO
Description	<p>This standard specifies requirements for a quality management system where an organization needs to demonstrate its ability to consistently provide product that meets customer and applicable regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable regulatory requirements.</p> <p>All requirements of this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and product provided.</p> <p>Where any requirement(s) of this International Standard cannot be applied due to the nature of an organization and its product, this can be considered for exclusion.</p> <p>Where exclusions are made, claims of conformity to this International Standard are not acceptable unless these exclusions are limited to requirements within clause 7, and such exclusions do not affect the organization's ability, or responsibility, to provide product that meets customer and applicable regulatory requirements.</p>

Name	Guidelines for interpretation of ISO 9000 series for application within the iron ore industry
Brief Name	ISO TR 13352:1997

Issuing Organisation	ISO
Description	<p>This Technical Report gives guidelines for the interpretation of the ISO 9000 series for application within the iron ore industry, including the mining, concentrating, palletising and shipping processes.</p> <p>This Technical Report will serve as a guide to help iron ore producers develop a quality system that can be registered to the ISO 9000 series of quality management standards. The quality system elements have been directly matched to ISO 9001 that includes all quality system elements of ISO 9001, ISO 9002 and ISO 9003. It is assumed that ISO 9001 is appropriate to the iron ore industry only when a strong design element for new product development exists.</p>

Name	Quality management systems - Particular requirements for the application of ISO 9001:2000 for automotive production and relevant service part organizations
Brief Name	ISO TS 16949:2002
Issuing Organisation	ISO
Description	<p>This Technical Specification, in conjunction with ISO 9001:2000, defines the quality management system requirements for the design and development, production and, when relevant, installation and service of automotive-related products.</p> <p>This Technical Specification is applicable to sites of the organization where customer-specified parts, for production and/or service, are manufactured.</p> <p>Supporting functions, whether on-site or remote (such as design centres, corporate headquarters and distribution centres), form part of the site audit as they support the site, but cannot obtain stand-alone certification to this Technical Specification.</p> <p>This Technical Specification can be applied throughout the automotive supply chain.</p>

Name	Quality management systems - Guidelines for the application of ISO 9001:2000 in local government
Brief Name	ISO IWA 4:2005
Issuing Organisation	ISO
Description	The objective of International Workshop Agreement IWA 4:2005 is to provide local governments with guidelines for the voluntary application of ISO 9001:2000 on an integral basis. These guidelines do not, however, add, change or modify the requirements of ISO 9001:2000.

	<p>For a local government to be considered reliable, it should guarantee minimum conditions of reliability for the processes that are necessary to provide all the services needed by its citizens in a consistent and reliable manner. All the local government's processes, including management, core, operational and support processes, should constitute a single, integral, quality management system. The integral character of this system is important because, otherwise, although a local government could be reliable in some areas of activity, it may be unreliable in others. For a government to be considered reliable, it should guarantee minimum conditions of reliability for all key processes and services. To achieve this, it is advisable that the local government clearly identify the management, core and support processes that, together, make it reliable (see Annex A). Annex B provides a diagnostic tool for local governments to evaluate the scope and maturity of their processes and services.</p>
--	---

5.15. Policy Standards

Almost all activities in healthcare and welfare are related to certain security aspects, and almost all security aspects are based on specific security policies. So policies are the very basis for each and every single activity in eHealth according to the scope of this deliverable. Policies can be described verbally, in templates, or model-based.

Table 10: List of Policy Standards

ASTM E2212-02 ^a	Standard Practice for Healthcare Certificate Policy
Name	Standard Practice for Healthcare Certificate Policy
Brief Name	ASTM E2212-02 ^a
Issuing Organisation	ASTM
Description	<p>Addresses the policy for digital certificates that support the authentication, authorization, confidentiality, integrity, and non-repudiation requirements of persons and organizations that electronically create or transact health information.</p> <p>There are 3 types of certificate: one for computerized entities, one for individual person and the last one for clinical individuals</p>

5.16. Terminology and Ontology Standards

Medical knowledge appeared first about 5,000 years ago. Since then, this knowledge has permanently improved and enhanced. Medical concepts apply world-wide. In order to ensure an adequate diagnosis and treatment level in all part of the globe, respective terminology and

ontology services need to be established. Coding allows for an internationally harmonised set of considerations of diseases, morbidity and mortality.

Table 11: List of Terminology and Ontology Standards

ASTM E1633-02a	Standard Specification for Coded Values Used in the Electronic Health Record
ASTM E2457-06	Standard Terminology for Healthcare Informatics
CCOW v1.5	Clinical Context Object Workgroup Version 1.5
CEN EN 1068:2006	Health informatics - Registration of coding systems
CEN EN 12264:2005	Health informatics - Categorical structures of systems of concepts - Model for representation of semantics
CEN EN 12435:2006	Health Informatics - Expression of the results of measurements in health sciences
CEN EN 15521:2006	Health informatics - Categorical structure for terminologies of human anatomy
CEN EN 1614:2005	Health Informatics - Structure for nomenclature, classification, and coding of properties in clinical laboratory sciences
CEN EN 1828	Categorical structure for classifications and coding systems of surgical procedures
CEN EN 1828:2002	Health informatics - Categorical structure for classification and coding systems of surgical procedures
CEN ENV 12017	Medical Informatics Vocabulary (MIVoc)
CEN ENV 12611	Categorical structure of systems of concepts - medical devices
CEN TS 14463:2006	Health informatics - A syntax to represent the content of medical classification systems (ClAML)
HL7v2.XML	HL7 Version 2.5
ISO 15225:2000	Specification for a nomenclature system for medical devices for the purpose of regulatory data exchange
ISO 18104:2003	Health informatics - Integration of a reference terminology model for nursing
ISO 19218	Medical devices - Coding structure for adverse event type and cause
ISO 20225	Global medical device nomenclature for the purpose of regulatory data exchange
ISO 21731	HL7 version 3 - Reference information model
ISO TS 17117:2002	Health informatics - Controlled health terminology - Structure and

	high-level indicators
ISO TS 21667:2004	Health informatics - Health indicators conceptual framework
LOINC	Logical Observation Identifiers Names and Codes

The majority of these standards and normative references will be explained in more detail below.

Name	Standard Specification for Coded Values Used in the Electronic Health Record
Brief Name	ASTM E1633-02a
Issuing Organisation	ASTM
Description	<p>This specification covers the identification of the lexicons to be used for the data elements identified in Appendix X1 of Guide E 1384. It is intended to unify the representations for:</p> <ol style="list-style-type: none"> 1. primary record of care data elements 2. the data elements identified in other standard statistical data sets 3. data elements Used in other healthcare data message exchange format standards, or 4. in data gathering forms for this purpose, and 5. in data derived from these elements in order that data recorded in the course of patient care be exchangeable and be the source of accurate statistical and resource management data. <p>This specification is applicable to all paper and automated systems.</p>

Name	Standard Terminology for Healthcare Informatics
Brief Name	ASTM E2457-06
Issuing Organisation	ASTM
Description	<p>This terminology is intended to name and document the principal concepts, and their associated terms, that are utilized in the healthcare information domain and all of its specialized sub-domains. It is applicable to all areas of healthcare about which information is kept or utilized. It is intended to complement and utilize those concepts already identified by other national and international standards bodies. It will identify alternate accepted terms for the same concept and its elected term. Its terms are intended to clarify and simplify usage in the dialog and documentation about the concepts, processes and data that are used to schedule, conduct and manage all phases of healthcare. This common usage will improve the quality and management of all facets of healthcare by means of explicit information used in referring to each of these facets. These health informatics terms</p>

	<p>have been collected here specifically in order to facilitate the consistent use of common concepts in informatics standards development and use throughout healthcare. A separate process from this standard that is described in ISO 15188 will manage the approval of biomedical and healthcare terms.</p> <p>This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.</p>
--	--

Name	Clinical Context Object Workgroup Version 1.5
Brief Name	CCOW V1.5
Issuing Organisation	HL7
Description	<p>CCOW V1.0 defines the overall technology-neutral context management architecture (CMA), a core set of data definitions, rules for application user interfaces, and the translation of the CMA to Microsoft's COM/ActiveX technology.</p> <p>This version also support technology mapping to SOAP.</p>

Name	Health informatics - Registration of coding systems
Brief Name	CEN EN 1068:2006
Issuing Organisation	CEN
Description	<p>The standard specifies a procedure for the registration of coding schemes used in health care for any purpose. It also specifies the allocation of a unique Health Care Coding Scheme Designator (HCD) to each registered coding scheme. A code value can thus be given an unambiguous meaning by association with an HCD. The method by which an HCD and a code value are associated is not defined by this standard. The association is achieved in any manner appropriate to the syntax used.</p>

Name	Categorical structures of systems of concepts - Model for representation of semantics
Brief Name	ENV 12264:2005
Issuing Organisation	CEN
Description	<p>The standard provides the vocabulary and the guidelines to describe the categorial structure of a concept system: the structure consists in practice of a list of involved categories with reference to the available authoritative</p>

	<p>sources for detailed value.</p> <p>Medical Informatics deals with a great number of large, overlapping coding systems that are facing each other and conflicting in the coming Integrated Healthcare Information Environment. This standard tries to solve these conflicts.</p>
--	--

Name	Health Informatics - Expression of the results of measurements in health sciences
Brief Name	CEN EN 12435:2006
Issuing Organisation	CEN
Description	<p>This standard is intended for use by parties to the design, development, acquisition, use and monitoring of health-care related information and information systems. It provides a list of units of measurement to be used in representing values of measurable quantities in health sciences. The International System of Units forms the basis for this EN. Units with their associated kinds-of-quantity are arranged in order of dimension in Tables 1, 2 and 4 (Clause 5), and in Annex A. Different kinds-of-quantity may apply to a given combination of component(s) and system. Often the different quantities are inter-convertible and examples of such inter-convertibility are given in Annex C. Tables of conversion factors (Annex A) are provided from units in current use to SI units or their multiples. To represent the result of a measurement (Clause 6), this EN addresses requirements for the following: - relational operator (Clause 4) - numerical value (Sub-clause 6.1) - uncertainty of measurement (Sub-clause 6.2; Annex D) - unit of measurement (Clause 5). This EN covers the requirements for representation of these data elements in displayed and printed form, and provides an approach for support of languages in non-Roman alphabets (Clause 7). The scope of this standard is limited to textual representation. Support is not provided for the display or printing of images or graphs. This standard does not cover the requirements for expression of the results of measurements in speech, speech synthesis or handwriting. It does not cover the form and syntax of requests for clinical measurements, nor detailed aspects of data transmission. It refers the user to other CEN standards that address the detailed specification of the interchange format. It does not address the syntax for recording of natural-language statements about quantities, such as those used in recording information about drugs dispensed or about treatment of patients. It does not cover the units of financial quantities, which are covered by ISO 4217.</p>

Name	A syntax to represent the content of medical classification systems (ClaML)
Brief Name	CEN EN 14463:2006
Issuing	CEN

Organisation	
Description	The main purpose of this European Standard is to support the safe transfer of the majority of hierarchical healthcare classification systems between organisations and dissimilar software products. It is intended to serve as the core representation, from which all publication forms can be derived. The Standard should therefore be rich enough to uniquely identify and describe the structure and the relevant elements in those systems. This Standard does not intend to prescribe the meaning of structuring elements in classification systems. This Standard is not meant to be a direct format for printing or viewing the contents of a classification system. Views and prints shall be derived from this representation by post processing.

Name	Health informatics - Categorical structure for terminologies of human anatomy
Brief Name	CEN EN 15521:2006
Issuing Organisation	CEN
Description	To define the characteristics required to synthetically describe the organisation and content of human anatomy within a terminological system. The proposed European Standard is primarily intended for use with computer-based applications such as clinical electronic health records, decision support and for various bio-medical research purposes. It does not include categorical structures that may be necessary for the description of development anatomy.

Name	Health Informatics - Structure for nomenclature, classification, and coding of properties in clinical laboratory sciences
Brief Name	CEN EN 1614:2005
Issuing Organisation	CEN
Description	This standard provides a coherent system of concepts underlying systematic names, classifications, and coding for properties, including quantities, in clinical laboratory sciences. The system is intended to facilitate the communication of messages about such properties through computing and telecommunications equipment. This work item consists of the revision of the published ENV 1614.

Name	Categorical structure for classifications and coding systems of surgical procedures
Brief Name	CEN EN 1828:2002
Issuing	CEN

Organisation	
Description	This European Standard specifies the characteristics of a categorial structure and the combinatorial rules required for compliance, in order to support the exchange of meaningful surgical procedure information between different national classifications or coding systems of surgical procedures using different national languages within Europe. It is applicable to: organisations involved with the development or maintenance of classifications and coding systems for medical procedures namely for multipurpose coding systems on a national or international level as well as organisations developing and maintaining software tools allowing natural clinical language expressions analysis, generation and mapping to the main existing classifications of surgical procedures. The standard has been developed for use as an integrated part of computer-based applications and for the electronic healthcare record. It would be of limited value for manual use. The standard itself is not suitable for or intended for use by, the individual clinician or hospital administrator. It is not the purpose of this standard to standardise the end user classification or to conflict with the concept systems embedded in national practice and languages. This standard is applicable to surgical procedures in all surgical disciplines.

Name	Medical Informatics Vocabulary (MIVoc)
Brief Name	CEN ENV 12017
Issuing Organisation	CEN
Description	This standard is applicable to international communication in the field for medical informatics standardisation. It presents a core list of concepts with their definitions which have been approved in CEN TC 251 pre-standards. Although this version contains only English terms, provision has been made for accommodation of European language and culture specific concepts of medical informatics.

Name	Categorial structure of systems of concepts - medical devices
Brief Name	CEN ENV 12611
Issuing Organisation	CEN
Description	This pre-standard specifies the necessary requirements (clause 5, 6 and 7) for the categorial structure of systems of concepts for medical device groups (clause 4). This pre-standard is meant to be used by organisations involved with the development or maintenance of nomenclatures and coding systems for medical devices, and by designers of databases of information systems involving medical devices.

Name	HL7 Version 2.5
Brief Name	HL7 v2.XML
Issuing Organisation	ANSI
Description	Old HL7 standards were focused on medical information exchange. With the addition of XML support, multimedia capabilities are now reliable. Better support for imaging has been introduced in version 2.5 compared with the previous one.

Name	Specification for a nomenclature system for medical devices for the purpose of regulatory data exchange
Brief Name	ISO 15225:2000
Issuing Organisation	ISO
Description	Specifies requirements and guidance for the construction of a nomenclature for medical devices to facilitate cooperation and exchange of regulatory data on an international level between such interested parties as regulatory authorities, manufacturers, suppliers, health care providers, and end users.

Name	Health informatics - Integration of a reference terminology model for nursing
Brief Name	ISO 18104:2003
Issuing Organisation	ISO
Description	<p>The purpose of this standard is to establish a nursing reference terminology model consistent with the goals and objectives of other specific health terminology models in order to provide a more unified reference health model. This International Standard includes the development of reference terminology models for nursing diagnoses and nursing actions and relevant terminology and definitions for its implementation.</p> <p>The potential uses for this reference terminology model are to support the intentional definition of nursing diagnosis and nursing action concepts reflective of a broad range of roles and practice settings, facilitate the representation of nursing diagnosis and nursing action concepts and their relationships in a manner suitable for computer processing, provide a framework for the generation of compositional expressions from atomic concepts within a reference terminology, facilitate the construction of nursing terminologies in a regular form which will make mapping among them easier, facilitate the mapping among nursing diagnosis and nursing action concepts from various terminologies including those developed as interface terminologies and statistical classifications, enable the systematic evaluation of terminologies and associated terminology models for purposes</p>

	of harmonisation, and provide a language to describe the structure of nursing diagnosis and nursing action concepts in order to enable appropriate integration with other reference terminology models and with information models.
--	---

Name	Medical devices - Coding structure for adverse event type and cause
Brief Name	ISO 19218
Issuing Organisation	ISO
Description	This standard specifies requirements for a coding structure for describing adverse events related to medical devices. This code is intended for use by medical device users, manufacturers and regulatory authorities.

Name	Global medical device nomenclature for the purpose of regulatory data exchange
Brief Name	ISO 20225
Issuing Organisation	ISO
Description	This report lists terms, definitions and codes for medical devices; the listing is structured such that it can be used for the purpose of regulatory data exchange.

Name	HL7 version 3 - Reference information model
Brief Name	ISO HL7 21731:2006
Issuing Organisation	ISO
Description	This standard deals with a static model of health and health care information as viewed within the scope of HL7 standards development activities.

Name	Health informatics - Controlled health terminology - Structure and high-level indicators
Brief Name	ISO TS 17117:2002
Issuing Organisation	ISO
Description	This technical specification specifies the principal ideas which are necessary and sufficient to assign value to a controlled health terminology. It is applicable to all areas of healthcare about which information is kept or utilized.

Name	Health informatics - Health indicators conceptual framework
Brief Name	ISO TS 21667:2004
Issuing Organisation	ISO
Description	This standard establishes a common health indicators conceptual framework for the field of health informatics. It is intended to foster a common vocabulary and conceptual definitions for a framework which defines the appropriate dimensions and sub-dimensions required to describe the health of the population and performance of a health care system, which is sufficiently broad (high-level) to accommodate a variety of health care systems, and which is comprehensive, encapsulating all of the factors that are related to health outcomes and health system performance and utilisation, and regional and national variations. ISO/TS 21667:2004 does not identify or describe individual indicators or specific data elements for the health indicators conceptual framework. The definition of benchmarks and/or approaches used in the definition of benchmarks is outside its scope.

Name	Logical Observation Identifiers Names and Codes
Brief Name	LOINC
Issuing Organisation	Regenstrief Institute
Description	The purpose of the LOINC database is to facilitate the exchange and pooling of results, such as blood haemoglobin, serum potassium, or vital signs, for clinical care, outcomes management, and research. The Regenstrief Institute provides mapping utility called the Regenstrief LOINC Mapping Assistant (RELMA) to facilitate searches through the LOINC database.

5.17. ID Management Security Standards

Management of identities in the electronic world is a very complex area. IDs need to be allocated not only to human beings but to all principals and even to specific items. Different organisations have dealt with identifying items uniquely. A few important examples are listed below.

Table 12: List of ID Management Standards related to Security

CORBA PIDS	Person Identification Service
HL7/CORBA EIS	Entity Identification Service
HL7 MPI	Master Patient Index

ISO	Digital Object Identifier
LOINC	Logical Observation Identifiers Names and Codes
ASTM E1714-00	Standard guide for properties of a Universal Healthcare Identifier

Name	Person Identification Service
Brief Name	CORBA PIDS
Issuing Organisation	OMG
Description	<p>This specification defines the interfaces that organises person ID management functionality to meet healthcare needs. The PIDS is designed to:</p> <ul style="list-style-type: none"> • Support both the assignment of IDs within a particular ID Domain and the correlation of IDs among multiple ID Domains • Support searching and matching of people in both attended-interactive and message-driven-unattended modes, independent of matching algorithm. • Support federation of PIDS services in a topology-independent fashion. • Permit PIDS implementations to protect person confidentiality under the broadest variety of confidentiality policies and security mechanisms. • Enable plug-and-play PIDS interoperability by means of a “core” set of profile elements, yet still support site-specific and implementation-specific extensions and customization of profile elements. • Define the appropriate meaningful compliance levels for several degrees of sophistication, ranging from small, query-only single ID Domains to large federated correlating ID Domains.

Name	Entity Identification Service
Brief Name	HL7/CORBA EIS
Issuing Organisation	OMG
Description	<p>The Entity Identification Service (EIS) provides a set of service interfaces to uniquely identify various kinds of entities (e.g. people: patients, providers etc., devices) within disparate systems within a single enterprise and/or across a set of collaborating enterprises.</p>

Name	Master Patient Index
Brief Name	HL7 MPI
Issuing Organisation	HL7
Description	Master Patient Index is an electronic index that enables lookup of patient

	data distributed across multiple systems, to provide an aggregated view of patient's EHR.
--	---

Name	ISO/IEC 9834 Information Technology – Open Systems Interconnection: Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree.
Brief Name	ISO OID
Issuing Organisation	ISO
Description	<p>ISO/IEC 9834-1:2005:</p> <ul style="list-style-type: none"> • specifies a Registration-Hierarchical-name-tree (RH-name-tree), which is a generic tree structure for allocations made by Registration Authorities, and the ASN.1 object identifier tree, which is a specific instance of the RH-name-tree; • registers the three top-level arcs of the ASN.1 object identifier tree; • specifies procedures which are generally applicable to registration in the context of an RH-name-tree; • provides guidelines for the establishment and operation of International Registration Authorities; • provides guidelines for additional International Standards which reference the procedures in ISO/IEC 9834-1:2004. <p>ISO/IEC 9834-1:2005 does not exclude or disallow the use of any syntactic forms of names or any naming domains for registration purposes provided that the domains ensure non-ambiguity within their scope. It is intended to cover those cases in which the registration-hierarchical-name is appropriate. Information about registration for specific objects is contained in separate International Standards.</p> <p>ISO/IEC 9834-1:2005 applies to registration by International Standards, by International Registration Authorities, and by any other Registration Authority.</p>

6. Conclusions

The Deliverables provides a rather comprehensive overview on a highly dynamic domain. It covers standards and publicly available specifications directly related to Electronic Health Records (EHR), EHR systems, EHR architectures, and EHR communication. Because of the pivotal character an EHR / EHR systems plays as core application in any health telematics platform or eHealth environment, interfaces, exchange formats, terminologies, classification and coding systems including ID schemata, or other issues of systems or components connected to an EHR system have to be considered too. The aforementioned nature of the topic the Deliverable is dealing with requires that the overview has to be permanently maintained. In that context, the direct involvement in SDOs is a fundamental prerequisite for correctly and consistently describing and evaluating the specifications needed to be considered by the stakeholders addressed.

7. **References**

- [1] ISO/DTR 20514; Health informatics - electronic health record: definition, scope and context: 2005.
- [2] B. Blobel, Advanced EHR architectures – promises or reality, *Methods Inf Med.* 25 (2006) 95-101.