HSE Design Authority

ISF Programme ICT Asset Base
Workstream 2.4

Standards Catalogue

Delivering eHealth Ireland

Office of the Chief Information Officer



Table of Contents

1 Introduction 7

1.1 Purpose and Objectives 8

2 Standards Organisations and Standards Development Organisations 9

2.1 Standards Organisations 9

2.1.1 HIQA 9

2.1.2 Antilope 10

2.1.3 NSAI 11

2.2 Standards Development Organisations 11

2.2.1 International Organization for Standardization (ISO) 12

2.2.2 Comité Européen de Normalisation (CEN) 12

2.2.3 Health Level Seven (HL7) 13

2.2.4 OpenEHR 13

2.2.5 Integrating the Healthcare Enterprise (IHE) 14

2.2.6 Healthcare Services Specification Program (HSSP) 15

2.2.7 Object Management Group (OMG) 15

2.2.8 NIST National Institute of Standards and Technology 15

2.2.9 Oasis 16

2.2.10 Regions of Europe working together for HEALTH (RENEWING) 16

2.2.11 ETSI European Telecommunications Standards Institute 17

2.2.12 Institute of Electrical and Electronics Engineers (IEEE) 18

2.2.13 Internet Engineering Task Force (IETF) 18

2.2.14 International Health Terminology Standards Development Organisation (IHTSDO) 18

2.2.15 European Health Telematics Association (EHTEL) 19

2.2.16 Continua Health Alliance (CHA) 19

2.2.17 Web Services Interoperability Organisation (WS-I) 20

2.2.18 World Wide Web Consortium (W3C) 20

2.2.19 American Society for Testing and Materials (ASTM) 21

2.2.20 Regenstrief Institute 21

2.2.21 MITA 21

2.2.22 World Health Organisation 22

3 Detailed Standards 23

Section number – Name or identification 24

3.1 IT Standards 25
3.1.1 Operational Standards 25
3.1.1.1 IHE-CT (RFC1305) – Consistent Time 25
3.1.1.2 IHE-ATNA – Audit Trail and Node Authentication 25
3.1.1.3 IHE-XCA - Cross-Community Access 26
3.1.1.4 IHE-BPPC – Basic Patient Privacy Consents 27
3.1.1.5 IHE-XDR – Cross enterprise Document Reliable Interchange 28
3.1.1.6 IHE-XPHR – Exchange of Personal Health Record 29
3.1.1.7 IHE-XDW – Cross Enterprise Document Workflow 30
3.1.1.8 IHE-XDS-I – Cross Enterprise Document Sharing for Imaging 32
3.1.1.9 IHE-XDS - Cross Enterprise Document Sharing 33
3.1.1.10 IHE-XD-LAB – Sharing Laboratory Reports 34
3.1.1.11 IHE-SWF – Scheduled Workflow 35
3.1.1.12 IHE-SVS – Sharing Value Sets 37
3.1.1.13 IHE-RID – Retrieve information for display 38
3.1.1.14 IHE-PRE – Pharmacy Prescription Document 38
3.1.1.15 IHE-PIX – Patient Identifier Cross Referencing 39
3.1.1.16 IHE-PDQ – Patient Demographics Query 40
3.1.1.17 IHE-PAM – Patient Administration Management 41
3.1.1.18 IHE-LTW – Laboratory Testing Workflow 42
3.1.1.19 IHE-LCSD – Laboratory Code Sets Distribution 43
3.1.1.20 IHE-DIS – Pharmacy Dispense Document 44
3.1.1.21 IHE-DEC – Device Enterprise Communication 45
3.1.1.22 IHE-CMPD – Community Medication Prescription and Dispense 46
3.1.1.23 IHE- PADV Pharmacy Pharmaceutical Advice Supplement 47
3.1.1.24 IHE-PML Pharmacy Medication List 48
3.1.1.25 IHE XCPD Cross-Community Patient Discovery 48
3.1.1.26 IHE-XCF Cross Community Fetch 49
3.1.1.27 IHE XUA 50
3.1.1.28 IHE DSG - Document Digital Signature 51
3.1.1.29 ISO 27799 51
3.1.1.30 IHE-XDM - Cross Enterprise Document Media Interchange 52
3.1.1.31 IHE-XPID - Change Management 52
3.1.2 Architectural 54
3.1.2.1 ISO 17090-3:2008 54
3.1.2.2 SAML v2 - Security Assertion Markup Language 55
3.1.2.3 WS-I Basic Profile 56
3.1.2.4 WS-Addressing 57
3.1.2.5 WS-I Basic security 57
3.1.2.6 WS-TRUST V1.3 60

3.1.2.7 WSDL 1.1 60
3.1.2.8 HTTP 1.1 61
3.1.2.9 SOAP 1.2 62
3.1.2.10 UDDI 3 63
3.1.2.11 IEEE 1003.2 POSIX Shell Standard 64
3.1.2.12 ebMS OASIS/ebXML Messaging Services Specifications v3.0 65
3.1.2.13 ebRS OASIS/ebXML Registry Services Specifications v3.0 67
3.1.2.14 XML 67
3.1.2.15 XML XSL 68
3.1.2.16 XML Schema 69
3.1.2.17 ANSI X12 69
3.1.2.18 UN/EDIFACT - ISO 9735 70
3.1.2.19 IEEE 11073 'Personal Health Devices' 70
3.1.2.20 ISO/TR 16056 72
3.1.2.21 MLLP 72
3.2 Syntactical Standards 74
3.2.1 Document Syntax 74
3.2.1.1 ASTM CCD 74
3.2.1.2 ASTM CCR 75
3.2.2 Messaging Syntax 76
3.2.2.1 HL7 v2.x 76
3.2.2.2 HL7 v3 76
3.2.2.3 DICOM 77
3.2.3 Data Model Standards 78
3.2.3.1 HL7 v3 RIM 78
3.2.3.1 ebRIM OASIS/ebXML Registry Information Model v3.0 78
3.2.3.2 HSSP CTS2 80
3.2.3.3 GS1 Healthcare 81
3.2.3.4 OID 81
3.2.3.5 FHIR 82
3.2.3.6 CEN/ISO EN 13606 82
3.2.3.7 OpenEHR Clinical Models 83
3.2.3.8 HL7 v3 Data Types 84
3.2.3.9 ISO 21090 Harmonized data types for information interchange 85
3.2.3.10 ISO/IEC 11404 General-Purpose Datatypes 85
3.2.3.11 ISO/TS 22220 Health informatics -- Identification of subjects of health care 86
3.3 Semantic Standards 87
3.3.1 Terminologies / Classifications 87
3.3.1.1 Terminologies 87

3.3.1.2 Classifications 93
3.3.2 Semantic Standards 96
3.3.2.1 HL7 Version 3 Clinical Document Architecture or CDA v2 96
3.3.2.2 OASIS-XSPA 97
3.3.2.3 BPMN 97
3.4 Security Standards 98
3.5 Business Standards 101
3.5.1.1 ISO/TR 13054 Knowledge management of health information standards 102
3.5.1.2 ISO/DIS 13940 Health informatics -- System of concepts to support continuity of care 102
3.5.1.3 ISO/TS 27527 Health informatics -- Provider identification 102
3.5.1.4 ISO EN 12967 Health Informatics Service Architecture HISA 103
3.5.1.5 HL7 EHR-System Functional Model 103
3.6 Accessibility Standards 104
3.6.1.1 Irish National IT Accessibility Guidelines 104
3.6.1.2 Web Content Accessibility Guidelines 105
4 Policies and Procedures 106
4.1 Standards Management Process Roles & Responsibilities 106
4.1.1 Standards Owner 106
4.1.2 Subject Matter Expert 106
4.1.3 Standards Organisation 106
4.2 Manage use of standards for a procurement process 106
4.3 Update of the standards catalogue 108
5 Health Interoperability initiatives 113
5.1 From US 113
5.1.1 Commonwell health alliance 113
5.2 From UK 113
5.2.1 NHS Connecting for Health 113
5.2.1.1 The Interoperability Toolkit (ITK) 113
5.2.1.2 Spine Services 114
5.2.1.3 Messaging Implementation Manual 114
5.3 From Europe 114
5.3.1 Antilope 114
5.3.2 Expand 114
5.3.3 epSOS 114
6 Appendix A – Standards Matrix 115
7 Appendix B - References 121
8 Glossary 122

8.1 Appendix: Terminology 122
8.2 Appendix: Acronyms 123

1 Introduction

Information communication is a key component in any system. In the health area, information is transferred among healthcare professionals, institutions, and decision support systems.

Effective communication requires that information issuers and recipients share a common "reference framework" that allows for interaction. Standards provide this common framework, promoting uniformity in the definition and identification of health system components, whether they are objects, diagnosis, people, or interventions.

Developing a solution for each problem as it arises can be relatively straightforward and inexpensive in the short term. However, such solutions generally have a very specific use and can be difficult or impossible to adapt to new problems that can arise as a result of (for example) growth in the number of systems, processes and organisations to be integrated. Healthcare standards implement rules that govern the way patient information is electronically stored and interchanged. Ideally, a single set of standards would provide efficient access to text, numeric and image data, allowing information to be shared appropriately by health professionals, payers, administrators and consumers.

Patient records are typically accumulations of interactions involving health professionals, patients, insurance companies and governmental agencies. The data they support is often not uniformly categorised and filled with free text and images. Therefore it's not surprising that clinical data standards are sometimes seen as a complex, confusing assortment of different vocabularies and obscure technical details. It is important, however, for managers, healthcare providers and health policymakers to understand the basics of standards. Key decisions must be made regarding how and when standards are to be implemented to ensure the optimal provision of healthcare.

Managing technology standards for software, hardware, applications, processes and people across the enterprise involves several key challenges:

IT complexity: New technologies are being introduced all the time, and every new purchase seems to involve a different technology or a new server with IT constantly being tasked with re-inventing the wheel with new designs. Current standards and reuse programs often complicate rather than simplify, resulting in a patchwork of overlapping, out-of-date, undocumented and sometimes contradictory technology standards.

Lack of enterprise standards visibility: Because standards are often manually stored and scattered in spreadsheets, Visio programs and PowerPoint presentations, there is no common place in the organisation for technology standards and reusable designs. Even if the teams want to reuse proven assets or designs, they simply don't know where to locate them.

Business risks: Technology standards not catalogued and enforced can mean higher maintenance costs as well as issues with ongoing vendor support. It's easy to run afoul of software-licensing agreements while security vulnerabilities from non-compliant technologies or software can also emerge.

Slow business response times: Complexity and lack of visibility into reusable building blocks means that it takes too long for IT to deliver a plan supporting a business change. A lack of visibility into reliable designs means reinventing the wheel – dramatically increasing project cost, time to delivery and risk.

Weak collaboration: There are few avenues for the stakeholders to communicate about standards and request changes that have become irrelevant. As a result, they ignore standards rather than use them.

The bottom line: The organisation has no formal process for setting and reviewing standards, largely because of a lack of visibility of standards and a lack of analytical tools to gauge the impact of a standards change. As a result, there is not process for managing and approving new standards.

1.1 Purpose and Objectives

The purpose of this document is to clearly articulate the technical, data exchange and security standards supporting the secure interoperable exchange of health information and offer guidance and direction to future standards initiatives so that local and national agencies related to HSE can make informed technical and investment decisions in a collaborative and proactive manner. It is therefore important to provide a practical, clear guide which outlines the most suitable standards for the present and near future, and which follow European and International trends.

Some standards are mature enough to be implemented right now but in some cases the standard is under trial implementation. Currently many of the standards that required for cross border sharing of health information are in the trial stage, however, may become mandatory in the future. As such any implementation based on these trial standards may require upgrades in the future.

This document provides:

- A sufficiently detailed overview of each standard in order to allow the reader to understand how each standard works and why it is listed in this catalogue.
- A brief description of the Standards Organisations and Standards Development Organisations (SDO) for background information.
- A formal procedure and associated policies to support the use and maintenance of this document

This document covers the requirements established by the HSE's Integrated Standard Framework (ISF) Programme, as outlined below:

As well other standards like IHE-RTLS (Real time location system) or IHE's Cardiac Catheterization Workflow Profile are not included in this document because there aren't widely adopted by many SDOs, eHealth initiatives or within legislation which would encourage their use.

2 Standards Organisations and Standards Development Organisations

Healthcare standards are created by a variety of healthcare organisations, including service provider entities, management staff, vendors, and independent advisory bodies.

There are four basic standards development mechanisms:

1. **Ad Hoc** – These standards arise when groups informally agree to use a common process whose details are not generally published.
2. **De facto** – These standards, such as those for computer operating systems, are those imposed by its sheer use or market acceptance.
3. **De Jure** – These standards are determined and imposed by the government to be used in particular scenarios.
4. **Consensus** – This results from all parties interested in using a standard meeting in open sessions to discuss and reach consensus on the definition of the standard.

Healthcare information standards are typically developed by work groups organised around interest communities. Interested parties include clinicians, researchers, bioinformaticists, chief information officers, database managers, information system analysts, and project directors or managers. Moreover, entities with special interests in public health, patient safety, and electronic records work to ensure that the standards will be relevant to their areas of concern.

Development of healthcare standards often involves the coordination of the efforts of many volunteers. The success of any standard depends on the credibility of the organisation developing the standard, some form of accreditation of the organisations balloting processes and balance of interests and the ability of that organisation to achieve industry adoption. Credibility requires having enough members in each applicable sector of the industry.

Early adopters generally come from within the standards development group. They validate the adequacy and efficacy of the standard and also serve as industry leaders communicating the standard to the wider audience of users. Ultimately the standard may be accredited or otherwise approved by an external body such as ANSI or ISO (International Standards Organisation)

2.1 Standards Organisations

A standards organisation is any organisation primarily responsible for coordinating, promulgating, reissuing, and interpreting technical standards that are intended to address the needs of some relatively wide base of affected adopters.

2.1.1 HIQA

The Health Information and Quality Authority (HIQA) (Irish: An t-Údarás um Fhaisnéis agus Cáilíocht Sláinte) is a statutory, government-funded agency in Ireland which monitors the safety and quality of the healthcare and social care systems.

The Health Information and Quality Authority is the independent Authority established in May 2007 to drive continuous improvement in Ireland's health and social care services.

Reporting directly to the Minister for Health and the Minister for Children and Youth Affairs, its role is to promote quality and safety in the provision of health and personal social services for the benefit of the health and welfare of the public.

As an independent organisation, the Authority is committed to an open and transparent relationship with its stakeholders. Its independence within the health and social care system is key and central to us being successful in undertaking its functions.

The Authority has four core activities or functions aimed at achieving these outcomes that are organised in Directorates. These activities are:

- **Regulation** – which involves the registration, oversight and scrutiny of designated health and social care services, including children's residential centres, residential services for older people and children and adults with disabilities.

- **Supporting Improvement** – which is achieved through the setting of standards, provision of guidance, building capacity by supporting the implementation of sustainable improvements and promotion of quality and patient safety initiatives.

- **Assessing Health Technologies (HTA)** – which involves the provision of evidence-based advice to inform policy development and how services are delivered.

- **Improving outcomes through information** – which involves promoting the efficient and secure collection, use and sharing of health information.

There are also activities undertaken by its support services which provide the necessary cross-organisational support, coordination and infrastructural services to ensure that the Authority can undertake its work in a well-governed way.

The Authority is governed by a three-year Corporate Plan published in 2013. It is based on four key elements:

- outcomes that it aims to achieve in order to deliver on its mission
- its core activities
- its strategic objectives
- the key enablers to deliver on the Plan

The strategic objectives for the Enablers (people, governance, performance planning and delivery, information, communication and engagement and evidence) are, for the most part, led by these three support Directorates: Corporate Services, Communications and Stakeholder Engagement and the Chief Executive's Office.

The Health Information and Quality Authority derive its mandate from, and undertake its functions pursuant to, the Health Act 2007 and other relevant legislation (the Child Care Act, 1991 and the Children Act, 2001).

HIQA exists to promote sustainable improvements, safeguard people using health and social care services and support informed decisions on how services are delivered. This mission guides and directs all of the activities of the Authority.

Corporate values are intended to express what they believe is important, how they work and how they hope to be viewed by external stakeholders, as well as the ethos and approach which its staff are encouraged to observe. They form the basis of the culture of the organisation.

2.1.2 Antilope

Antilope drives eHealth interoperability in Europe and beyond. Between 2013 and 2015 key national and international organisations will work together to promote and drive adoption of testing guidelines as well as testing tools on a European and national level. Antilope creates, validates and disseminates a common approach for testing and certification of eHealth solutions and

services in Europe. Together with the corresponding testing tools, Antilope gives regional, national and international projects practical guidelines to converge their eHealth platforms and practices.

Antilope supports the dissemination and adoption of the European Interoperability Framework and builds on these recommendations, roadmaps, National/Regional and local Interoperability projects. In particular:

- Drive the adoption of recognised sets of profiles and underlying standards for eHealth interoperability, and improve the impact of the EU and International eHealth standards development process;
- Define and validate testing guidelines and common approaches on Interoperability Labelling and Certification processes at European and at National/Regional level.
- In 2013 the consortium developed a series of material including an overview of use cases, standards and profiles following the eHealth interoperability framework, and testing guidelines to projects and implementers. The material was prepared in consultation with European and international experts and stakeholders.

2.1.3 NSAI

NSAI (National Standards Authority of Ireland) is Ireland's official standards body. It operates under the National Standards Authority of Ireland Act (1996) and are accountable to the Minister for Jobs, Enterprise and Innovation.

It is the national certification authority for CE Marking and provide a certification service to enable business demonstrate that Irish goods and services conform to applicable standards.

As Ireland's Official standards body, NSAI aims to inspire consumer confidence and create the infrastructure for products and services to be recognised and relied on, all over the world. This is achieved by:

- Setting agreed minimum Irish standards for goods and services, benchmarked against international best practice to ensure fair trade nationally and globally
- Issuing certification confirming the quality and safety of goods and services produced and traded in Ireland
- Monitoring and regulating metrology
- Assessing and approving new materials and processes for Ireland's construction industry.
- Providing information, training and technical support to government, consumers and industry.
- NSAI Vision, Mission and Values can be found in the NSAI Mission Statement.

NSAI is involved in a diverse range of activities which are coordinated by six sub-groups within the organisation:

- Certification
- Standards
- Agreement
- Legal Metrology Service
- National Metrology Laboratory
- Training

In addition, NSAI represents Ireland in European and international standards and measurement bodies. The purpose of this international activity is to work with others to develop consistent international written standards and measurements, which in turn can help ensure fair trade.

2.2 Standards Development Organisations

The term standards development organisation (SDO) refers to the thousands of industry- or sector-based standards organisations that develop and publish industry specific standards.

In some cases, international industry-based SDOs such as the IEEE and the Audio Engineering Society (AES) may have direct liaisons with international standards organisations, having input to international standards without going through a national standards body. Below is a list of key standards organisations relevant to the health sector, and most of these organisations have created standards which are listed in this document

2.2.1 International Organization for Standardization (ISO)

ISO (International Organization for Standardization) is an independent, non-governmental membership organisation and the world's largest developer of voluntary International Standards.

ISO International Standards ensure that products and services are safe, reliable and of good quality. For business, they are strategic tools that reduce costs by minimising waste and errors and increasing productivity. They help companies to access new markets, level the playing field for developing countries and facilitate free and fair global trade.
The standards are developed by the people that need them, through a consensus process. Experts from all over the world develop the standards that are required by their sector. This means they reflect a wealth of international experience and knowledge.

The ISO story began in 1946 when delegates from 25 countries met at the Institute of Civil Engineers in London and decided to create a new international organisation 'to facilitate the international coordination and unification of industrial standards'. In February 1947 the new organisation, ISO, officially began operations.

ISO is made up of its 165 member countries who are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland.
International Standards make things work. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO has published more than 19 500 International Standards covering almost every industry, from technology, to food safety, to agriculture and healthcare. ISO International Standards impact everyone, everywhere.

2.2.2 Comité Européen de Normalisation (CEN)

CEN, the European Committee for Standardisation, is an association that brings together the National Standardisation Bodies of 33 European countries.

CEN is one of three European Standardisation Organisations (together with CENELEC and ETSI) that have been officially recognised by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level.

CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes.

CEN supports standardisation activities in relation to a wide range of fields and sectors including: air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

European Standards (ENs) are based on a consensus, which reflects the economic and social interests of 33 CEN Member countries channelled through their National Standardisation Organisations. Most standards are initiated by

industry. Other standardisation projects can come from consumers, Small and Medium-sized Enterprises (SMEs) or associations, or even European legislators.

Besides European Standards, CEN produces other reference documents, which can be developed quickly and easily: Technical Specifications, Technical Reports and Workshop Agreements.

2.2.3 Health Level Seven (HL7)

Founded in 1987, Health Level Seven International (HL7) is a not-for-profit, ANSI-accredited standards developing organisation dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services. HL7's 2,300+ members include approximately 500 corporate members who represent more than 90% of the information systems vendors serving healthcare.

HL7 provides standards for interoperability that improve care delivery, optimise workflow, reduce ambiguity and enhance knowledge transfer among all of its stakeholders, including healthcare providers, government agencies, the vendor community, fellow SDOs and patients. In all of its processes it exhibits timeliness, scientific rigor and technical expertise without compromising transparency, accountability, practicality, or its willingness to put the needs of its stakeholders first.

"Level Seven" refers to the seventh level of the International Organisation for Standardisation (ISO) seven-layer communications model for Open Systems Interconnection (OSI) - the application level. The application level interfaces directly to and performs common application services for the application processes. Although other protocols have largely superseded it, the OSI model remains valuable as a place to begin the study of network architecture.

2.2.4 OpenEHR

The openEHR Foundation is currently a not-for-profit company, limited by guarantee. Its founders were University College London, UK and Ocean Informatics Pty Ltd, Australia. It is regulated under the UK Companies Acts 1985 and 1989.

As part of the new governance, the Foundation will be recreated as a new not-for-profit company, possibly in the form of a UK Community Interest Company, or else in the form of a Private company limited by guarantee (the same as the current form), commonly used for non-profits in the UK. The new organisation will be created by consultation of the interim board and prospective organisational members.

The openEHR Foundation vision is of a world in which healthcare routinely obtains benefit from ICT, in particular:

- life-long interoperable electronic health records (EHRs);
- computing on EHRs to improve the quality of health care and research.

The Foundation is proceeding on the basis of three principles: rigour, engagement and trust. These correspond to the key activities of the Foundation, organised under the four Programs:

- Specification Program:
  - developing rigorous, open specifications, validated by implementation;
  - participating in international standards development;
- Clinical Models Program:
  - developing clinical models (archetypes and templates), terminology interfaces;

  - engaging in clinical implementation projects;
- Software Program:
  - developing open-source software and tools;
  - participating in connectathons and implementation trials;
- Localisation Program:
  - advocacy and locale-based education and dissemination;
  - working with national standards organisations;

Patients and citizens at the centre. At this point the openEHR architecture ensures:

- that information (rather than just authorisation data) can be kept in personal storage such as a memory key or phone;
- that information can be stored with no identifying information within the EHR;
- that information does not have to be centralised, being stored and/or made available only where it is required;
- accountability of users and providers;
- that the owner of the record can partition the information and control access if required.
- The next phase of uptake and implementation will require careful scrutiny by those using the health service and providers of personal health record services.

The success of openEHR is in no small part due to the formal acceptance of CEN 13606 as a European and ISO standard. This standard is based on many aspects of the openEHR design approach, and part 2 of the standard is a snapshot of the openEHR Archetype specifications. The openEHR Foundation will work closely with CEN, ISO, HL7 and OMG and other standards organisations on EHR-related and clinical modelling standards.

As terminology is a key-stone component of semantic interoperability, openEHR archetypes explicitly provide various ways to implement terminology bindings. The Foundation will work closely with IHTSDO on all terminology-related matters, as well as with other terminology maintainers.
This is a proprietary standard as it does not have a CEN/ISO EN imprimatur.

2.2.5 Integrating the Healthcare Enterprise (IHE)

- **Note that IHE is NOT an SDO. IHE defines profiles that leverage existing standards**

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare 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.
IHE improves healthcare by providing specifications, tools and services for interoperability. IHE engages clinicians, health authorities, industry, and users to develop, test, and implement standards-based solutions to vital health information needs.

The initiative produces IHE Profiles to provide a standards-based framework for sharing information within care sites and across networks. They address critical interoperability issues related to information access for care providers and patients, clinical workflow, security, administration and information infrastructure. Each profile defines the actors, transactions and information content required to address the clinical use case by referencing appropriate standards.
See capsule descriptions of current IHE profiles in each domain. IHE Profiles are compiled into IHE Technical Frameworks-detailed technical documents that serve as implementation guides.

IHE has been testing the interoperability of HIT (Health Information Technology) systems for more than a decade. At IHE Connectathons held regularly in several locations internationally, trained technical experts supervise testing of vendor systems, making use of advanced testing software developed by IHE and several partner organisations. More than 250 vendors worldwide have implemented and tested products with IHE capabilities.

2.2.6 Healthcare Services Specification Program (HSSP)

The Healthcare Services Specification Program (HSSP) is an open, global community focused on improving health interoperability within and across organisations through the use of Service-Oriented Architecture (SOA) and standard services. The intention is to reduce implementation complexity, promote effective integration, foster marketplace support, and drive down implementation costs and barriers impacting healthcare solutions.

2.2.7 Object Management Group (OMG)

The Object Management Group® (OMG®) is an international, open membership, not-for-profit technology standards consortium. Founded in 1989, OMG standards are driven by vendors, end-users, academic institutions and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries. OMG's modeling standards, including the Unified Modeling Language (UML) and Model Driven Architecture (MDA), enable powerful visual design, execution and maintenance of software and other processes. OMG also hosts organisations such as the user-driven information-sharing Cloud Standards Customer Council (CSCC) and the IT industry software quality standardisation group, the Consortium for IT Software Quality (CISQ).

Include as members hundreds of organisations including software end-users in over two dozen vertical markets (from finance to healthcare and automotive to insurance) and virtually every large organisation in the technology industry. OMG's one organisation- one vote policy ensures that every member organisation- whether large or small- has an effective voice in its voting process.

At OMG, specification adoption is the starting point rather than the end of the process. Its "No Shelf-ware" policy bars all bidding specifications that do not have an implementation plan from being adopted by OMG. This guarantees that all OMG specifications are immediately useable. Furthermore, it does not just focus on the specification itself, it focuses on the whole product: with corresponding seminars, workshops, certification, books.

OMG maintains liaison relationships with dozens of other organisations including ISO (which publishes many OMG standards without edits), Health Level Seven (HL7), and the Data Transparency Coalition.

2.2.8 NIST National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory, also known as a National Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce.

The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve its quality of life.

NIST employs about 2,900 scientists, engineers, technicians, and support and administrative personnel. About 1,800 NIST associates (guest researchers and engineers from American companies and foreign countries) complement the staff. In addition, NIST partners with 1,400 manufacturing specialists and staff at nearly 350 affiliated centres around the country. NIST publishes the Handbook 44 that provides the "Specifications, tolerances, and other technical requirements for weighing and measuring devices

Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the US' oldest physical science laboratories. Congress established the agency to remove a major handicap to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of England, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

2.2.9 Oasis

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organisations and individual members in more than 65 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.

OASIS was founded under the name "SGML Open" in 1993. It began as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalised Markup Language (SGML). The consortium changed its name to "OASIS" (Organisation for the Advancement of Structured Information Standards) in 1998 to reflect an expanded scope of technical work.

2.2.10 Regions of Europe working together for HEALTH (RENEWING)

RENEWING HEALTH (REgioNs of Europe WorkINg toGether for HEALTH) is an European project, partially funded under the ICT Policy Support Programme, by the European Community.

RENEWING HEALTH aims at implementing large-scale real-life test beds for the validation and subsequent evaluation of innovative telemedicine services using a patient-centred approach and a common rigorous assessment methodology.

It involves a Consortium of 9 of the most advanced European regions in the implementation of health-related ICT services. In those regions the service solutions are already operational at local level for the tele-monitoring and the treatment of chronic patients suffering from diabetes, chronic obstructive pulmonary or cardiovascular diseases. The

services are designed to give patients a central role in the management of their own diseases, fine-tuning the choice and dosage of medications, promoting compliance to treatment, and helping healthcare professionals to detect early signs of worsening in the monitored pathologies.

These services will be scaled up, integrated with mainstream Health Information Systems, grouped into a limited number of clusters bringing together services with similar features, trialled and assessed with a rigorous and common assessment methodology, and using a common set of primary indicators.

Although integration of the service solutions at regional level is the highest priority for the Project partners, the use of international standards and the progressive convergence towards common interoperable architectures will be equally sought to prepare and facilitate their scaling up at national and European levels. Each cluster of pilots will operate as a multi-centre clinical trial measuring the efficiency and the cost effectiveness of the implemented solutions.

The Project is supported by the Health Authorities of the partners and they are fully committed to deploy the telemedicine services in their territory, cooperating in a network that let them an overview not only among partners, but even on other European initiatives with similar objectives.

2.2.11 ETSI European Telecommunications Standards Institute

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

It is officially recognised by the European Union as a European Standards Organisation.
The high quality of its work and its open approach to standardisation has helped it evolve into a European roots - global branches operation with a solid reputation for technical excellence.

ETSI produces globally-applicable standards for ICT (Information and Communications Technologies), including fixed, mobile, radio, converged, broadcast and internet technologies. It has over 750 members from 63 countries and across five continents. ETIS is also active in vital areas related to standardisation such as interoperability, including protocol testing and methodology and it also offers forum-hosting services.

ETSI unites:

- Manufacturers
- Network operators
- National Administrations
- Service providers
- Research bodies
- User groups
- Consultancies

This cooperation has resulted in a steady stream of highly successful ICT standards in mobile, fixed, and radio communications and a range of other standards that cross these boundaries, including:

- Security
- Satellite
- Broadcast
- Human Factors
- Testing & Protocols
- Intelligent transport
- Power-line telecoms
- eHealth

- Smart Cards
- Emergency communications
- GRID & Clouds
- Aeronautical
- and many more

ETSI is consensus-based and conducts its work through Technical Committees, which produce its standards and specifications, with the ETSI General Assembly and Board guiding the Secretariat towards its Vision and Mission.

2.2.12 Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a professional association with its corporate office in New York City and its operations centre in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers. Today it is the world's largest association of technical professionals with more than 400,000 members in chapters around the world. Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and allied disciplines.

IEEE Advancing Technology for Humanity

IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

2.2.13 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935.

IETF®

The actual technical work of the IETF is done in its working groups, which are organised by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

The IETF working groups are grouped into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters.

2.2.14 International Health Terminology Standards Development Organisation (IHTSDO)

IHTSDO – The International Health Terminology Standards Development Organisation – determines global standards for health terms, an essential part of improving the health of humankind. It is committed to maintain and grow its leadership as the global experts in healthcare terminology, ensuring SNOMED CT, its world-leading product, is accepted as the global

ihtsdo Leading healthcare terminology, worldwide

common language for health terms.

Owned and governed by 27 international members, it is a not-for-profit organisation that works on behalf of the healthcare system and provides full support to its global members and licensees, ensuring that its combined resources achieve significant shared benefits that resonate around the world.

The purpose of the IHTSDO is the development of a global language for health, uniting health systems from around the world and enabling them to communicate with and understand one another, should not be the job of one or two organisations or companies. It should be an international endeavour, utilising the skills and efforts of experts from around the world.

IHTSDO was founded on that principle. In 2007, nine charter nations established IHTSDO for the purposes of building and strengthening SNOMED CT, other health terminologies and related terminology products, and developing, maintaining, promoting and enabling the uptake and correct use of its terminology products in health systems, services and products around the world. It is a strong and proud membership organisation, serving and responding to the needs of its Member countries.

2.2.15 European Health Telematics Association (EHTEL)

The European Health Telematics Association (EHTEL) is a European non-profit organisation, which provides a platform to all European eHealth stakeholders to exchange information on eHealth.

Within EHTEL's Vision, eHealth is a cooperative process intensifying and changing the interactions of all stakeholders in health and social care for the purpose of improving Continuity of Care and Patient Safety. eHealth is a tool to ensure information, choice and empowerment, as requested by European consumers and patients eHealth must comprise multiple communication channels for ensuring both equal access to services and their ubiquity.

EHTEL: The European eHealth Multidisciplinary Stakeholder Platform Through its growing membership of currently 60 organisations, it enables its members to voice their views throughout the eHealth ecosystem. It also facilitates the sharing of experience with colleagues and representatives across Europe and beyond.

As such it collaborates closely with European associations representing Hospitals (HOPE and EHMA), health insurers (AIM), Physicians (CPME, UEMS), Pharmacists (PGEU, EAHP), Nurses (EFN), patient and citizens (AGE Platform, European Patients' Forum), as well as professional associations dedicated to quality and certification to care processes and eHealth services (ESQH, EuroRec).

The multitude of backgrounds and interests of these stakeholders enable EHTEL, as a neutral forum, to draw a more complete picture of the benefits and challenges of the deployment of ICT in the fields of health and social care, thereby also identifying topics requiring particular attention and further developments at European level.

2.2.16 Continua Health Alliance (CHA)

Continua is a non-profit, open industry organisation of healthcare and technology companies joining together in collaboration to improve the quality of personal healthcare. With more than 200 member companies around the world, Continua is dedicated to establishing a system of interoperable personal connected health solutions with the knowledge that extending those solutions into the home fosters independence, empowers individuals and provides the opportunity for truly personalised health and wellness management.

Continua is comprised of technology, medical device and health care industry leaders dedicated to making personal telehealth a reality. Continua has objectives that include:

- Developing design guidelines that will enable vendors to build interoperable sensors, home networks, telehealth platforms, and health and wellness services.
- Establishing a product certification program with a consumer-recognisable logo signifying the promise of interoperability across certified products.
- Collaborating with government regulatory agencies to provide methods for safe and effective management of diverse vendor solutions.
- Working with leaders in the health care industries to develop new ways to address the costs of providing personal telehealth systems.

2.2.17 Web Services Interoperability Organisation (WS-I)

The Web Services Interoperability Organisation (WS-I) is an open industry organisation chartered to establish Best Practices for Web services interoperability, for selected groups of Web services standards, across platforms, operating systems and programming languages.

WS-I comprises a diverse community of Web services leaders from a wide range of companies and standards development organisations (SDOs). WS-I committees and working groups create Profiles and supporting Testing Tools based on Best Practices for selected sets of Web services standards. The Profiles and Testing Tools are available for use by the Web Services community to aid in developing and deploying interoperable Web services. Companies interested in helping to establish Best Practices for Web Services are encouraged to join WS-I. It has recently become part of OASIS.

2.2.18 World Wide Web Consortium (W3C)

The World Wide Web Consortium (W3C) is an international community where member organisations, full-time staff and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. Below are important aspects of this mission, all of which further W3C's vision of One Web.

Design Principles

The following design principles guide W3C's work.

- Web for All
  The social value of the Web is that it enables human communication, commerce, and opportunities to share knowledge. One of W3C's primary goals is to make these benefits available to all people, whatever their hardware, software, network infrastructure, native language, culture, geographical location, or physical or mental ability.
    - Web Accessibility Initiative
    - Internationalisation
    - Mobile Web for Social Development

- Web on Everything
  The number of different kinds of devices that can access the Web has grown immensely. Mobile phones, smart phones, personal digital assistants, interactive television systems, voice response systems, kiosks and even certain domestic appliances can all access the Web:
    - Web of Devices
    - Mobile Web Initiative
    - Browsers and Other Agents

2.2.19 American Society for Testing and Materials (ASTM)

ASTM International, formerly known as the American Society for Testing and Materials (ASTM), is a globally recognised leader in the development and delivery of international voluntary consensus standards. Today, some 12,000 ASTM standards are used around the world to improve product quality, enhance safety, facilitate market access and trade, and build consumer confidence.

ASTM's leadership in international standards development is driven by the contributions of its members: more than 30,000 of the world's top technical experts and business professionals representing 150 countries. Working in an open and transparent process and using ASTM's advanced electronic infrastructure, ASTM members deliver the test methods, specifications, guides and practices that support industries and governments worldwide. Learn more about ASTM International.

2.2.20 Regenstrief Institute

An international informatics and healthcare research organisation, the Regenstrief Institute is recognised for its role in improving quality of care, increasing efficiency of healthcare delivery, preventing medical errors and enhancing patient safety. Established in 1969 by Sam Regenstrief on the Indiana University --- Purdue University Indianapolis campus, the Institute is supported by the Regenstrief Foundation and closely affiliated with the Indiana University School of Medicine and the Health and Hospital Corporation of Marion County, Indiana.

The Regenstrief Institute, Inc. initiated and continues to direct development of LOINC (Logical Obeservation Identifier Names and Codes), leading the LOINC Committee of volunteers from academia, industry, and government who advise and collaborate on its evolution. LOINC is a coding system for laboratory and other clinical measures and documents used in electronic transactions between independent computer systems. LOINC codes are universal identifiers for the "question" (or variable) in measurement or laboratory test results, survey questionnaire items, and packages of such items. When LOINC codes are used in electronic messages, the receiving systems can automatically file and use results from many sources to build electronic medical record systems or research databases.

Regenstrief Institute also manages the Unified Code for Units of Measure (UCUM), a code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. A typical application of the Unified Code for Units of Measure is electronic data interchange (EDI) protocols, but there is nothing that prevents it from being used in other types of machine communication.

2.2.21 MITA

The Medical Imaging & Technology Alliance (MITA), a division of the National Electrical Manufacturers Association (NEMA), is the leading organisation and collective voice of medical imaging equipment, radiation therapy and radiopharmaceutical manufacturers, innovators and product developers. It represents companies whose sales comprise more than 90 percent of the global market for medical imaging technology. These technologies include:

- Medical X-ray equipment
- Computed tomography (CT) scanners
- Ultrasound
- Nuclear imaging
- Radiopharmaceuticals

- Radiation therapy equipment
- Magnetic resonance imaging (MRI)
- Imaging information systems

MITA provides leadership for the medical imaging and radiation therapy industries on legislative and regulatory issues at the state, federal and international levels. It serves as an advocate for fair legislative and regulatory proposals that encourage innovation, investment in research and development, as well as the continued global competitiveness of the medical imaging and radiation therapy industries.
Through NEMA, MITA is also a leading standards-development organisation for medical imaging and radiation therapy equipment. These standards are voluntary guidelines that establish commonly accepted methods of design, production, testing and communication for imaging and cancer treatment products. Sound technical standards of this kind improve safety and foster efficiencies in how care is delivered. Goals:

- Increase awareness and understanding of the value of medical imaging
- Achieve efficient and reasonable regulation of medical imaging technologies
- Interact with appropriate government agencies on reimbursement and technology assessment policies
- Expand the global acceptance of the digital communications standard (DICOM) that allows digital imaging technologies to interact seamlessly
- Improve regulatory harmonisation of the global market for medical imaging products
- Develop and represent industry positions in technical, trade and other issues
- Provide market data unique to this industry

2.2.22 World Health Organisation

WHO is the directing and coordinating authority for health within the United Nations system. It is responsible for providing leadership on global health matters, shaping the health research agenda, setting norms and standards, articulating evidence-based policy options, providing technical support to countries and monitoring and assessing health trends.

3 Detailed Standards

This section covers the key standards that have been identified as relevant to the Irish health sector. They are described in enough detail to enable an understanding the standard itself and the context that supports it.

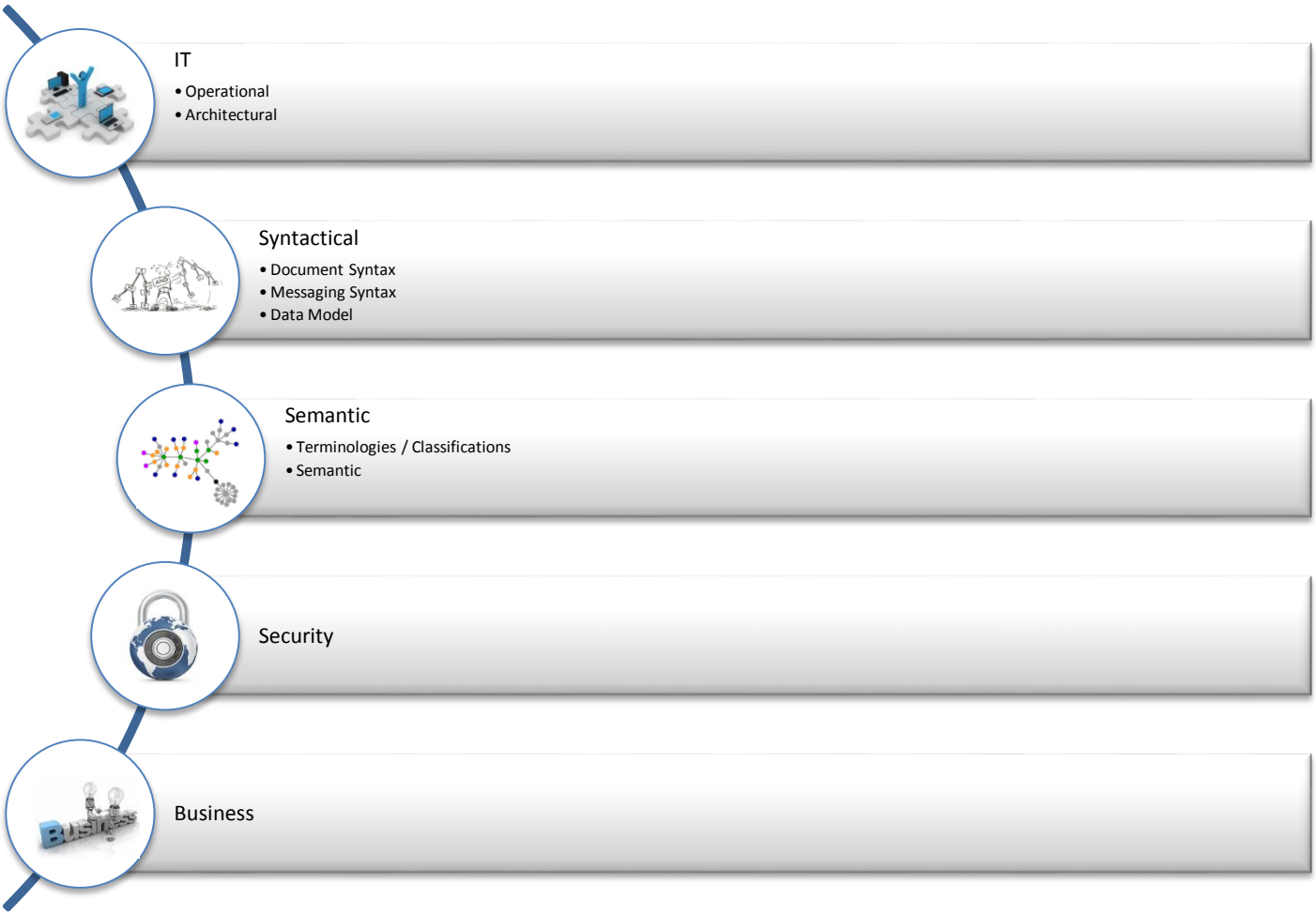
Interoperability is one of the key factors that should guide the specification, development, acquisition, implementation and use of health technology. As such these standards have been chosen based on their interoperability capability. Interoperability depends upon two significant concepts:

- Syntactic (functional) interoperability
- Semantic interoperability

Syntax refers to the structure of a communication; it can be thought of as equivalent to spelling and grammar rules. The Health Level Seven (HL7) Version 2.x messaging standard is an example of a standard for syntactic interoperability.

Semantics hold the meaning of a communication, the equivalent of a dictionary or thesaurus. Terminologies such as SNOMED and LOINC and standards such as the HL7 Clinical Document Architecture (CDA) are examples of semantic standards. Without semantic interoperability, data can be interchanged but there is no certainty that they can be used or understood by the person receiving them.

The classification established for the categorisation of the standards is based on the following categories:



Every standard is detailed based on the following template:

<table>
<tr><th colspan="3">Section number – Name or identification</th></tr>
<tr><td colspan="2">Adoption Level

This criteria is defined based on:

• If it is used in a health system
• If it is covered by a platform
• If it is used in a key interoperability initiative.

Categorise by the following criteria:

  Widely adopted: Big national projects/ systems use the standard.

  There is an important adoption: The standard is used in numerous systems but is not implemented in a health system of a country.

  Starting to be adopted widely: The standard is starting to be implemented in key systems in different countries.

  Barely adopted. The standard is proposed in some systems but it is not implemented.</td><td>Maturity

Measure the current state of the specification or standard.

Only standards that have reached a certain level of maturity are suitable for use. Therefore only three levels have been identified for categorisation.

Categorise by the following criteria:

  Final specification with at least one final version released.

  Trial is nearing completion and is currently being tested in a real environment.

  Draft for public use.</td></tr>
<tr><td colspan="2">Standard Organisation

Organisation responsible</td><td>Version

This field is filled if there is more than one version. In some cases specifies the state of the standard (i.e. trial or draft for public use).</td></tr>
<tr><td>Description</td><td colspan="2">Offers an overview of the standard with enough detail to understand the value of the standard.</td></tr>
<tr><td>Dependencies</td><td colspan="2">Describes the dependencies that need to be covered if the standard is used.</td></tr>
<tr><td>Example of Use Case</td><td colspan="2">Provides use case(s) in which the standard could apply.</td></tr>
</table>

3.1 IT Standards

The IT management should be a key part of a healthcare organisation's overall service delivery strategy, which focuses on information technology systems, their performance, and the management of risk across them. The primary goal of IT standards is to assure that investments in IT generate business value and to mitigate risks associated with IT.

3.1.1 Operational Standards

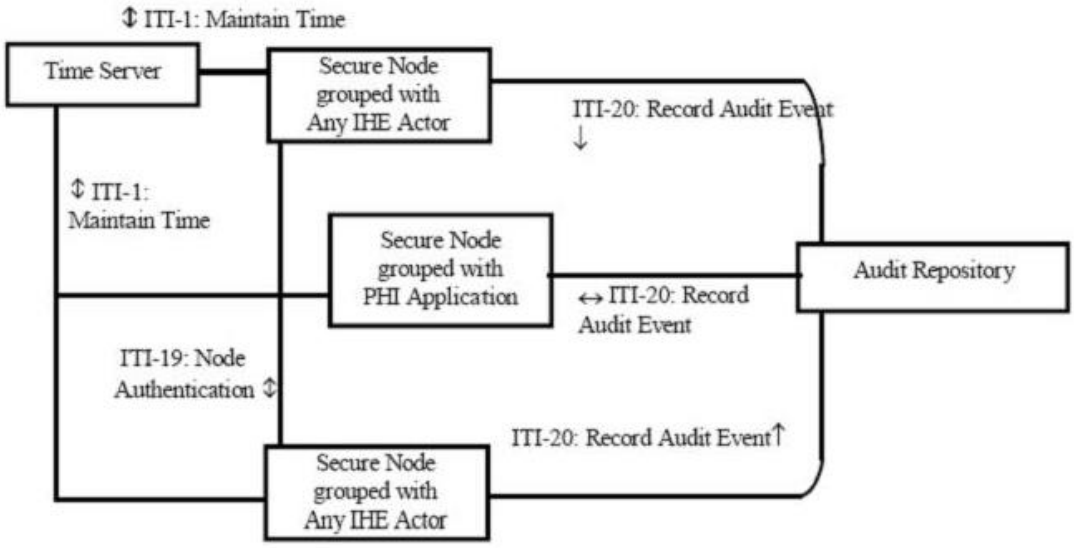
These standards provide a framework for understanding the concept of clinical data and how it can be moved between systems without losing meaning or context.

3.1.1.1 IHE-CT (RFC1305) – Consistent Time

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Consistent Time Integration Profile (CT) provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronised. This profile specifies synchronisation with a median error less than 1 second. This is sufficient for most purposes.		
Dependencies	Network Time Protocol (NTP)		
Example of Use Case	All interactions between systems		

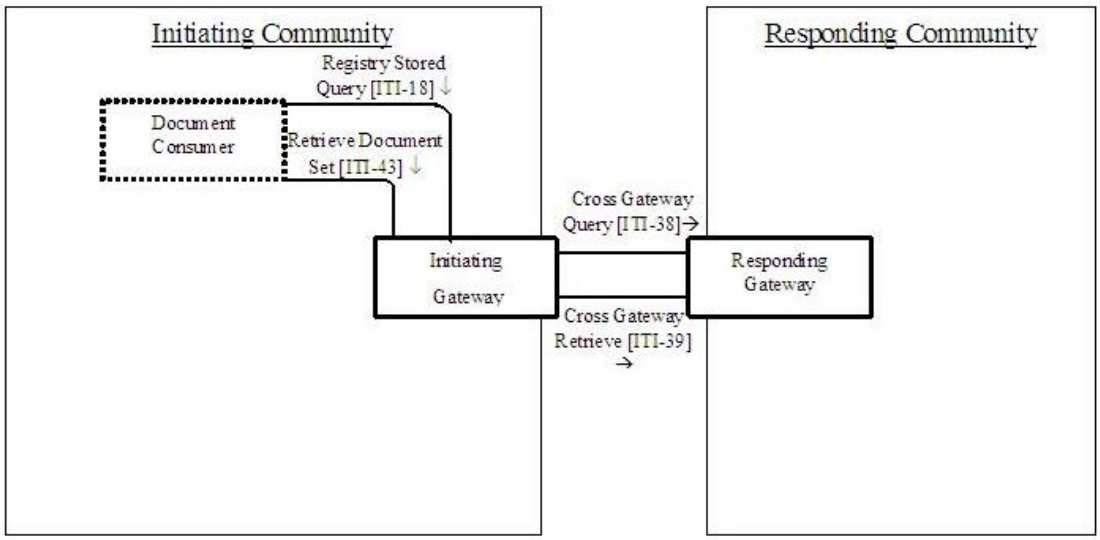
3.1.1.2 IHE-ATNA – Audit Trail and Node Authentication

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures, provide patient information confidentiality, data integrity and user accountability. The Audit Trail and Node Authentication (ATNA) Integration Profile: contributes to access control by limiting network access between nodes and limiting access to each node to authorised users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorised users as specified by the local authentication and access control policy. • User Authentication The Audit Trail and Node Authentication Integration Profile requires only local user		

	authentication. The profile allows each secure node to use the access control technology of its choice to authenticate users. The use of Enterprise User Authentication is one such choice, but it is not necessary to use this profile. • Connection Authentication The Audit Trail and Node Authentication Integration Profile requires the use of bi-directional certificate-based node authentication for connections to and from each node. The DICOM, HL7, and HTML protocols all have certificate-based authentication mechanisms defined. These authenticate the nodes, rather than the user. Connections to these machines that are not bi-directionally node-authenticated shall either be prohibited, or be designed and verified to prevent access to PHI. • Audit Trails User Accountability is provided through Audit Trail. The Audit Trail needs to allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). 
Dependencies	IHE-CT
Example of Use Case	e-Prescription and e-Dispensing on a national/regional scale

3.1.1.3 IHE-XCA - Cross-Community Access

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	

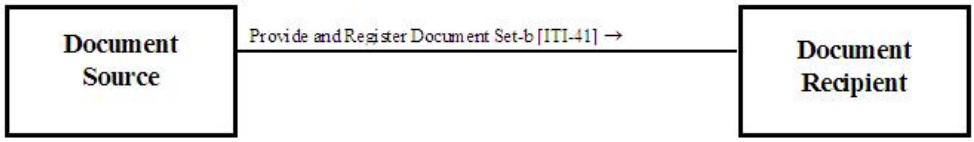
Description	The Cross-Community Access profile supports the means to query and retrieve patient relevant medical data held by other communities. A community is defined as a coupling of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing clinical information via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc. A community is identifiable by a globally unique id called the homeCommunityId. Membership of a facility/enterprise in one community does not preclude it from being a member in another community. Such communities may be XDS Affinity Domains which define document sharing using the XDS profile or any other communities, no matter what their internal sharing structure. 
Dependencies	
Example of Use Case	Sharing a Patient Summary with a healthcare provider. National Contact Point

3.1.1.4 IHE-BPPC – Basic Patient Privacy Consents

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	Basic Patient Privacy Consents (BPPC) provides a mechanism to record the patient privacy consent(s) and a method for Content Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. EHR systems). First: The Affinity Domain organisers create a set of policies. Each of the policies is each given an OID. This OID now is an Affinity Domain specific vocabulary. Each OID can		

	clearly identify one of the policies defined by the HIE. There are examples of how one might build these policies in a way that allows the patient to select appropriately the type of sharing they agree to. This is important as it allows the Affinity Domain to define their own policies in a clear of language as necessary for the patients, providers, and systems to understand. This level of policy writing is necessary before one can even hope to commit the logic to computer encoding. Second: The BPPC profile shows how to capture a patient's acknowledgment and/or signature of one or more of these policies. This is captured using a CDA document with optionally a scanned copy or optionally a digitally signature. The scanned copy might be the patient's ink on paper acknowledgment. This capability has been very well received as providers like to see that ink was put to paper. Third: When a document is used, the document consumer Actors are obligated to enforce the acceptable use. The document consumer Actor is required to block access to documents that are not authorised. Any OIDs that are not understood by the document consumer Actor must not be used to enable access.
Dependencies	
Example of Use Case	Sharing a Patient Summary with a healthcare provider

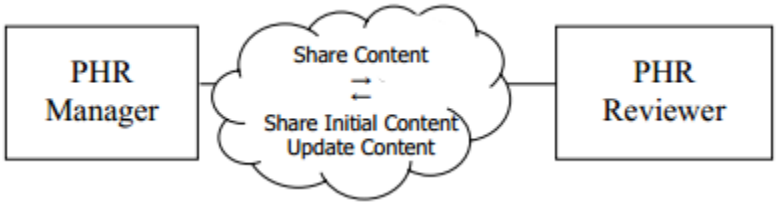
3.1.1.5 IHE-XDR – Cross enterprise Document Reliable Interchange

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	Cross-Enterprise Document Reliable Interchange (XDR) provides document interchange using a reliable messaging system. This permits direct document interchange between EHRs, PHRs, and other healthcare IT systems in the absence of a document sharing infrastructure such as XDS Registry and Repositories. XDR supports the reuse of the Provider and Register Set transaction with Web-Services as transport. Transfer is direct from source to recipient, no repository or registry actors are involved. XDR is document format agnostic, supporting the same document content as XDS and XDM. Document content is described in XDS Document Content Profiles. Examples are XDS-MS, XD-LAB, XPHR, and XDS-SD. XDR defines no new metadata or message formats. It leverages XDS metadata with emphasis on patient identification, document identification, description, and relationships. 		

Dependencies	• ebMS OASIS/ebXML Messaging Services Specifications v3.0 • ebRIM OASIS/ebXML Registry Information Model v3.0 • ebRS OASIS/ebXML Registry Services Specifications v3.0
Example of Use Case	Referral of patient from primary to secondary care using push technology

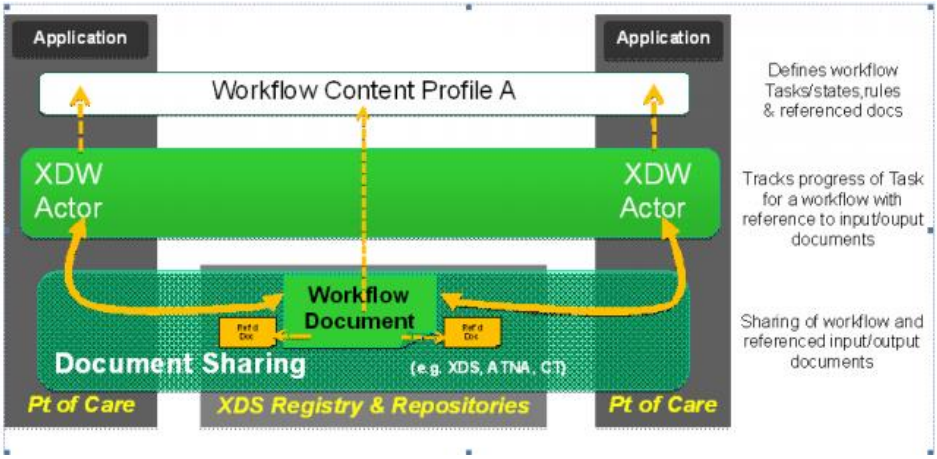
3.1.1.6 IHE-XPHR – Exchange of Personal Health Record

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Exchange of Personal Health Record Content (XPHR) integration profile describes the content and format of summary information extracted from a PHR system used by a patient for import into healthcare provider information systems, and vice versa. The purpose of this profile is to support interoperability between PHR systems used by patients and the information systems used by healthcare providers. This profile does not address all the data exchange requirements of PHR systems. A PHR system may leverage other IHE Integration and Content Profiles for interoperability in addition to the XPHR Content Profile. For example, a PHR Systems may implement XDS-MS to import medical summaries produced by EHR systems, XDS-I to import imaging information, XDS-Lab to import laboratory reports, et cetera. Upon seeing a healthcare provider for the first time, patients are requested to provide a great deal of information, including, their address, telephone numbers, birth date, sex, marital status, emergency contacts, insurance information, a medical and family history, and current medications and allergies. This information is also reviewed and updated on subsequent visits. This information is usually obtained by having the patient fill out one or more forms, whose contents are then manually transferred in to the information systems used by the healthcare provider. Automating this process will reduce transcription errors during the transfer of information, speed up the registration and check-in processes for patients, and also makes it possible for patients to have more participation in the management of their health information. Providers also need to participate in helping patients to manage their healthcare information; however, providers should not be solely responsible for updating the patient's health record, since they often are only participating in a portion of the patient's overall health activities. While PHR systems will allow patients to manage their healthcare information, and EHR and other information systems allow healthcare providers to manage the electronic records they maintain for their patients, but these two systems, operating separately, are not sufficient to allow patients and providers to collaborate in the care of the patient. What is needed is a way to integrate the activities of patients using a PHR system and healthcare providers using an EHR or other information system to provide for collaborative care between the patient and their provider. The XPHR		

	profile is intended to provide a mechanism for patients to supply the information most often requested by their healthcare providers, and to allow those same providers to assist patients in keeping their personal healthcare information up to date. It achieves this by allowing patients to provide a summary of their PHR information to providers, and gives providers a mechanism to suggest updates to the patient's PHR upon completion of a healthcare encounter. 
Dependencies	
Example of Use Case	Patient Summary sharing

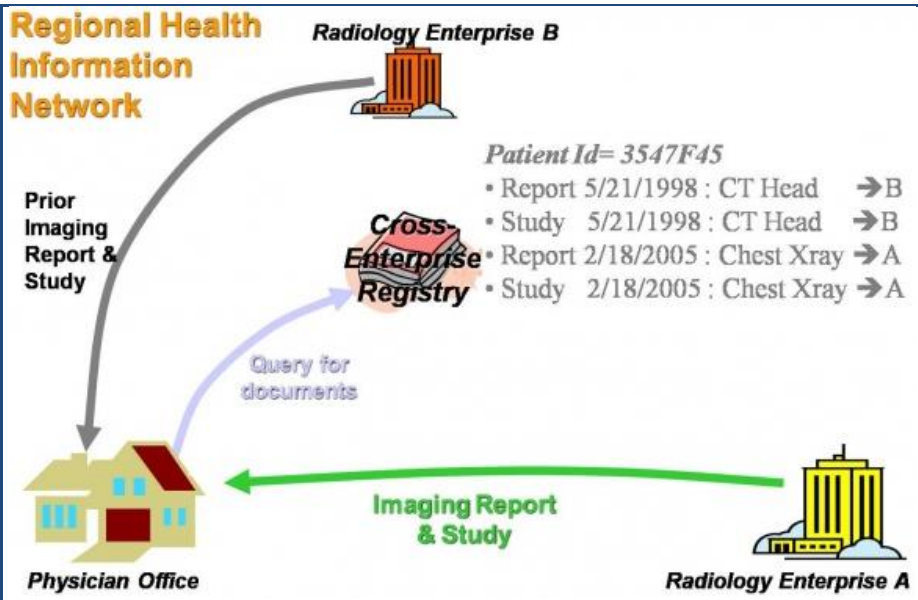
3.1.1.7 IHE-XDW – Cross Enterprise Document Workflow

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Cross-Enterprise Document Workflow (XDW) Profile enables participants in a multiorganisational environment to manage and track the tasks related to patient-centric workflows as the systems hosting workflow management applications coordinate their activities for the health professionals and patients they support. XDW builds upon the sharing of health documents provided by other IHE profiles such as XDS, adding the means to associate documents conveying clinical facts to a patient-specific workflow. XDW provides a common interoperability infrastructure upon which a wide range of specific workflow definitions may be supported. It is designed to support the complexity of health services delivery with flexibility to adapt as workflows evolve. This profile defines an instrument, called a “Workflow Document”, to manage and track a shared workflow. It records the creation of tasks and maintains a historical record of tasks as they move through the associated workflow. The Workflow Document also maintains the references to health information input and output associated with each task. Such shared workflow status information allows the various participating systems to coordinate their actions by: • being aware of the history of a workflow for a patient; • obtaining and reading the workflow’s incomplete tasks; • updating this shared document as the workflow tasks are performed according to a referenced Workflow Definition.		

	XDW provides to offer a common, workflow-independent interoperability infrastructure that: • provides a platform upon which a wide range of specific workflows can be defined with minimal specification and application implementation efforts on the workflow definition (e.g., Medical Referrals Workflow, Prescriptions Workflow, Home Care Workflow); • benefits many clinical and non-clinical domains by avoiding different competing approaches to workflow management; • increases the consistency of workflow interoperability, and enables the development of interoperable workflow management applications where workflow-specific customisation is minimised; • facilitates the integration of multi-organisational workflows with the variety of existing workflow management systems used within the participating organisations; • offers the necessary flexibility to support a large variety of different healthcare workflows by not being overly constrained; • executed in loosely connected, distributed environments, where centralised workflow management systems are not desired, or in many instances, possible. The XDW Workflow Architecture following illustration shows how the sharing of XDW Documents between "edge" applications using Document Sharing infrastructure supports the management of Workflow according to Workflow Definitions established between participating applications. 
Dependencies	
Example of Use Case	Referral
Comments	It is expected that BPEL and/or BPMN will be useful standards to support workflow definitions..

3.1.1.8 IHE-XDS-I – Cross Enterprise Document Sharing for Imaging

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	XDS-I provides a solution for publishing, finding and retrieving imaging documents across a group of affiliated enterprises. Affiliated Enterprises such as radiology departments, private physicians, clinics, long term care, and acute care centers can contribute and access imaging documents of interest. Imaging documents include: • Imaging studies (images, measurements, results from analysis packages, presentation states); • Diagnostic reports for imaging studies; • Key Image selections associated with the report content for their diagnostic significance. An Imaging Document Source that wants to share a set of images and/ or imaging information objects such as a presentation state constructs a DICOM manifest that references the DICOM instances that are to be published. The manifest along with metadata is submitted to the Document Repository. The metadata describes the information that is shared. Besides information about the patient and information required by the XDS profile, the Imaging Document Source provides metadata information that is image specific such as the type of imaging procedure, the modality and the anatomic region. Images and/ or imaging information objects that are made available are not transferred to the Document Repository. Instead, the Imaging Document Source is required to make them available to be retrieved. An Imaging Document Consumer that is interested in retrieving previously published imaging information, queries the registry (i.e. find all CT of the Head of patient John Doe for the last 2 years) and retrieves the manifest of interest. The Imaging Document Consumer decodes the manifest to extract the identifiers that uniquely identifies the available imaging information. The Imaging Document Consumer retrieves the images and/ or imaging information objects from the Imaging Document Source. An Imaging Document Source that wants to share an imaging report constructs a document that is shared either in a PDF and /or CDA (containing only text) format. The report is submitted to the Document Repository. A Document Consumer (any Document Consumer and not only Imaging Document Consumer) that is interested in retrieving previously published imaging report, queries the registry and retrieves the report from the Document Repository.		

	
Dependencies	
Example of Use Case	Cross-enterprise Medical Board Review in a cross border scope.

3.1.1.9 IHE-XDS - Cross Enterprise Document Sharing

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	Cross-Enterprise Document Sharing (XDS) is focused on providing a standards-based specification for managing the sharing of documents between any healthcare enterprise, ranging from a private physician office to a clinic to an acute care in-patient facility and personal health record systems. This is managed through federated document repositories and a document registry to create a longitudinal record of information about a patient within a given clinical affinity domain. These are distinct entities with separate responsibilities: • A Document Repository is responsible for storing documents in a transparent, secure, reliable and persistent manner and responding to document retrieval requests. • A Document Registry is responsible for storing information about those documents so that the documents of interest for the care of a patient may be easily found, selected and retrieved irrespective of the repository where they are actually stored. • Documents are provided by one or more Document Sources • They are then accessed by one or more Document Consumers The profile assumes that the enterprises belong to one or more XDS Affinity Domains. An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work		

	together using a common set of policies and share a common infrastructure.
	
	Examples of XDS Affinity Domains include:
	
	• Community of Care supported by a regional health information organisation in order to serve all patients in a given region.
	• Nationwide EHR
	• Specialised or Disease-oriented Care
	  ○ Cardiology Specialists and an Acute Cardiology Center
	  ○ Oncology network
	  ○ Diabetes network
	• Federation of enterprises
	  ○ A regional federation made up of several local hospitals and healthcare providers
	• Government sponsored facilities (e.g., VA or Military)
	• Insurance Provider Supported Communities
	
	The concept of a document in XDS is not limited to textual information. As XDS is document content neutral, any type of clinical information without regard to content and representation is supported. This makes the XDS IHE Integration Profile equally able to handle documents containing simple text, formatted text (e.g., HL7 CDA Release 1), images (e.g., DICOM) or structured and vocabulary coded clinical information (e.g., CDA Release 2, CCR, CEN ENV 13606, DICOM SR). In order to ensure the necessary interoperability between the document sources and the document consumers, the XDS Affinity Domain must adopt policies concerning document format, structure and content.

Dependencies	
Example of Use Case	e-Prescription and e-Dispensing on a cross-border scale in the epSOS Project. As described in the Use Case 1 about e-Prescription and e-Dispensing in the uses cases from Antilope.

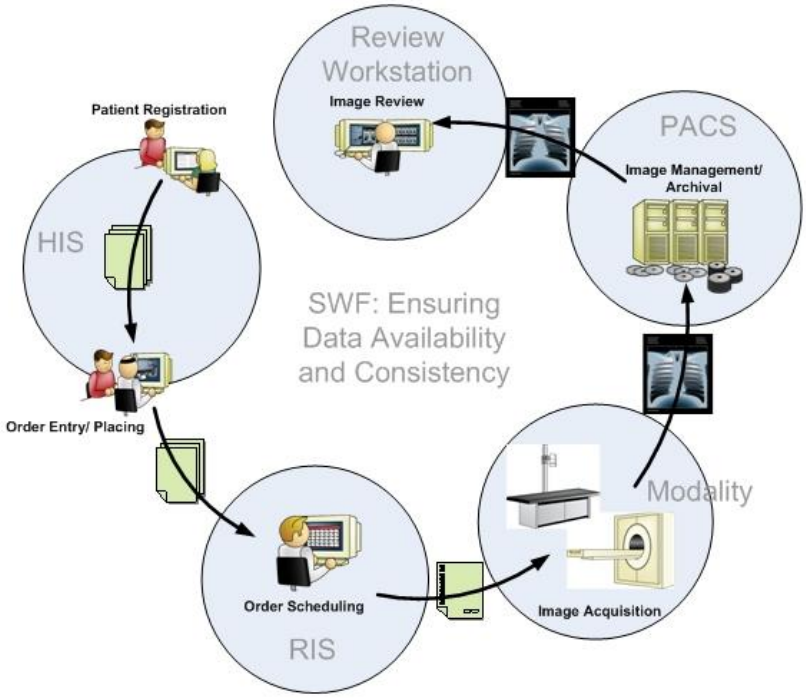
3.1.1.10 IHE-XD-LAB – Sharing Laboratory Reports

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	This Content Integration Profile describes a clinical laboratory report as an electronic document to be published towards a document sharing resource such as an Electronic Health Record (EHR) or a Personal Health Record (PHR) shared by a community of care providers, using one of the document sharing profiles defined in ITI-TF. Such an electronic document contains the set of releasable results produced by a clinical laboratory in fulfilment of one or more test Orders for a patient.		

	The report is both human-readable and importable in the consumer systems so as to consolidate their patient medical records. Provides an electronic format for the laboratory report, to make this report: • human-readable: displayed on screen or printed out, with a proper and clear layout and presentation. • machine-readable: Each observation displayed in the report is also represented in the document as a set of structured and coded data that can be imported in the database of any consumer of the document. This double capacity is achieved by leverageing the Clinical Document Architecture Release 2 standard from HL7.
Dependencies	CDA v2
Example of Use Case	The XD-LAB Integration Profile covers six major use cases: • At discharge time, a hospital physician publishing a summary laboratory report with the most significant results obtained during the patient stay. • The bio-medical scientist of a private laboratory publishes a report for a patient into the regional Patient Health Record. • An ambulatory physician shares a laboratory report obtained from a laboratory. • A private or public laboratory publishes automatically all its reports in a shared document repository. • A healthcare institution produces a cumulative report of all laboratory tests performed for the patient during the encounter. • A public health laboratory shares its reports into a regional repository.
Comments	The scope of this profile covers all laboratory specialties except anatomic pathology.

3.1.1.11 IHE-SWF – Scheduled Workflow

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	Establishes a seamless flow of information that supports efficient patient care workflow in a typical imaging encounter. It specifies transactions that maintain the consistency of patient information from registration through ordering, scheduling, imaging acquisition, storage and viewing. This consistency is also the foundation for subsequent workflow steps, such as reporting.		



- Establishes the continuity and integrity of basic departmental imaging data by profiling specific usage of HL7 messaging across multiple systems including: Patient registration (ADT), Order Placing (CPOE) and Order SCheduling (RIS) systems.
- Bridges the gap between HL7-based systems (like RIS) and DICOM-based systems (like acquisition modalities and PACS) within the radiology department by specifying the semantic mappings between messages.
- Maintains the consistency of patient demographic and ordering information across multiple systems by making that information available to image acquisition modalities via the DICOM Modality Worklist (MWL) Service.
- Ensures that acquired images are not inadvertently lost by specifying that the DICOM Storage Commitment Service is used to transfer the custodianship of images from the modality to the PACS.
- Ensures that the statuses of acquisition workflow steps are known throughout the department by specifying the use of the DICOM Modality Performed Procedure Step (MPPS) Service to convey that status from the modality to the RIS and the PACS.

Dependencies	DICOM, HL7
Example of Use Case	Imaging encounter

3.1.1.12 IHE-SVS – Sharing Value Sets

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Sharing Value Sets (SVS) profile provides a means through which healthcare systems producing clinical or administrative data, such as diagnostic imaging equipment, laboratory reporting systems, primary care physician office EMR systems, or national healthcare record systems, can receive a common, uniform nomenclature managed centrally. SVS provides a means through which healthcare systems producing clinical or administrative data, such as diagnostic imaging equipment, laboratory reporting systems, primary care physician office EMR systems, or national healthcare record systems, can receive a common, uniform nomenclature managed centrally. Shared nomenclatures are essential to achieving semantic interoperability. A single Value Set Repository can be accessed by many Value Set Consumers, establishing a domain of consistent and uniform set of nomenclatures. It supports automated loading of Value Sets by Value Set Consumers, reducing the burden of manual configuration. This profile describes two Transactions for retrieving Value Sets from a Value Set Repository by a Value Set Consumer. • A single value set can be retrieved based on an OID value. This is aimed at meeting the needs of systems that are pre-configured to use specific value sets. These systems are often medical devices with strictly controlled functions that should not be modified without careful review. This transaction does not include metadata content, and provides just the value set concept list as uniquely identified in the request. • Multiple value sets can be retrieved based on metadata about the value sets. This is aimed at meeting the needs of systems and users that will be dynamically selecting value sets, deciding which value sets should be used, and creating new value sets based on the contents of existing value sets. This transaction supports much richer selection criteria and provides metadata descriptions as well as the contents (expanded lists of coded values) of all the value sets that meet those criteria. Both transactions provide access to centrally managed value sets that have been assigned metadata, including group identification. The ability to identify groups of value sets is essential to achieving semantic interoperability and development of modular structures of electronic health records (EHR). Group identification can be used to identify, for example, all the value sets needed for a given purpose like filling in a particular kind of report.		

Dependencies	• HL7 Version 3 Standard: XML Implementation Technology Specifications - Data Types, R1 • IETF RFC 2616: Hypertext Transfer Protocol - HTTP 1.1 • IEEE Std 1003.2 IEEE Standard for Information Technology - Portable Operating System Interface (POSIX®) - Part 2: Shell and Utilities - Amendment 1: Batch Environment -Description
Example of Use Case	Request and results distribution workflow for laboratory within a hospital

3.1.1.13 IHE-RID – Retrieve information for display

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Retrieve Information for Display (RID) Integration Profile provides simple and rapid read-only access to patient-centric clinical information that is located outside the user's current application but is important for better patient care (for example, access to lab reports from radiology department). It supports access to existing persistent documents in well-known presentation formats such as CDA (Level 1), PDF, JPEG, etc. It also supports access to specific key patient-centric information such as allergies, current medications, summary of reports, etc. for presentation to a clinician. It complements workflows with access from within the users' on-screen workspace or application to a broad range of information. Offers the capability to leverage industry standards that address both the structure and content of documents that may be returned by information sources. Where this profile references HL7 Clinical Documentation Architecture (CDA), it limits itself to the approved CDA Level 1. Furthermore, it only uses a subset of CDA Level 1 that facilitates making information available for display.		
Dependencies	• IETF RFC1738 (URL) • XML • WSDL • XHTML		
Example of Use Case	Cross-enterprise workflow for laboratory requesting and results viewing		

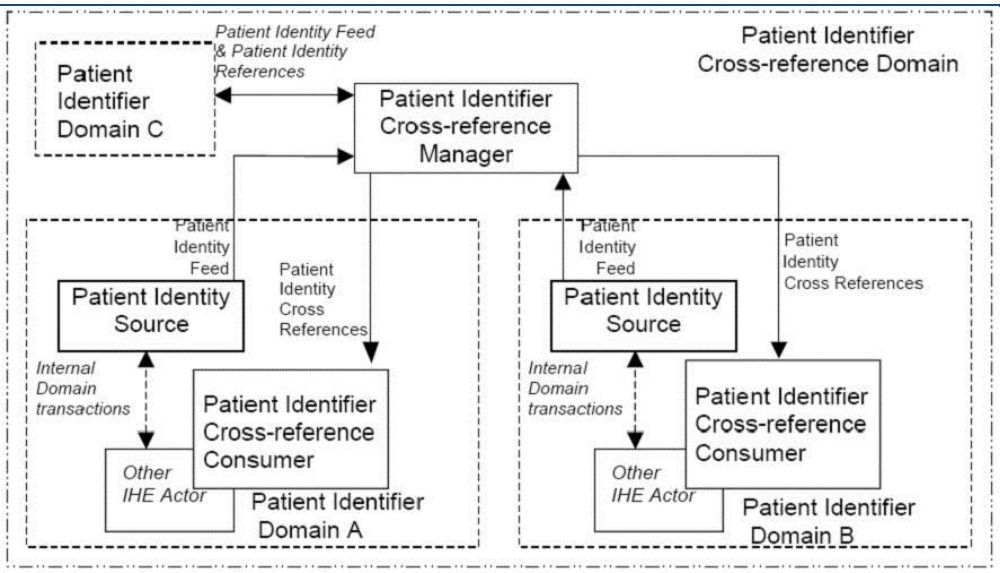
3.1.1.14 IHE-PRE – Pharmacy Prescription Document

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial

Description	The Pharmacy Prescription Document Profile (PRE) describes the content and format of a prescription document generated during the process in which a health care professional (in most cases, but not necessarily always, a medical specialist or a general practitioner) decides that the patient needs medication. A prescription is an entity that can be seen as an order to anyone entitled to dispense (prepare and hand out) medication to the patient. Documents created according to this profile are intended to be used in the context of the "Community Prescription and Dispense" Integration Profile (CMPD). The Community Pharmacy Prescription and Dispense workflow starts with the creation of a prescription in case the health care professional decides that the patient needs medication. A prescription document is issued by one ordering healthcare professional for one patient, in the context of zero or one administrative encounter (between the patient and the ordering physician and/or the healthcare institution). A prescription may contain one or more Prescription Items (lines on a paper prescription). Each line relates to one medication. A prescription is the outcome of a clinical decision. This profile defines the content and format of such a prescription document.
Dependencies	
Example of Use Case	Placing a prescription

3.1.1.15 IHE-PIX – Patient Identifier Cross Referencing

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Patient Identifier Cross Referencing (PIX) Integration Profile supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains by: • Transmitting patient identity information from an identity source to the Patient Identifier Cross-reference Manager. • Providing the ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via an update notification.		



The Patient Identifier Cross Referencing (PIX) Integration Profile supports two domains:

- A Patient Identifier Domain is defined as a single system or a set of interconnected systems that all share a common identification scheme (an identifier and an assignment process to a patient) and issuing authority for patient identifiers.
- The Patient Identifier Cross-reference Domain embodies the following assumptions about agreement within the group of individual Identifier Domains:
  - They have agreed to a set of policies that describe how patient identities will be cross-referenced across participating domains;
  - They have agreed to a set of processes for administering these policies;
  - They have agreed to an administration authority for managing these processes and policies.

All these assumptions are critical to the successful implementation of this profile.

Dependencies	This integration profile imposes minimal constraints on the participating Patient Identifier Domains and centralises most of the operational constraints for the overall Patient Identification Cross-reference Domain in the Patient Identifier Cross-reference Manager Actor.
Example of Use Case	Request and results sharing workflow for laboratory on a National/regional scale

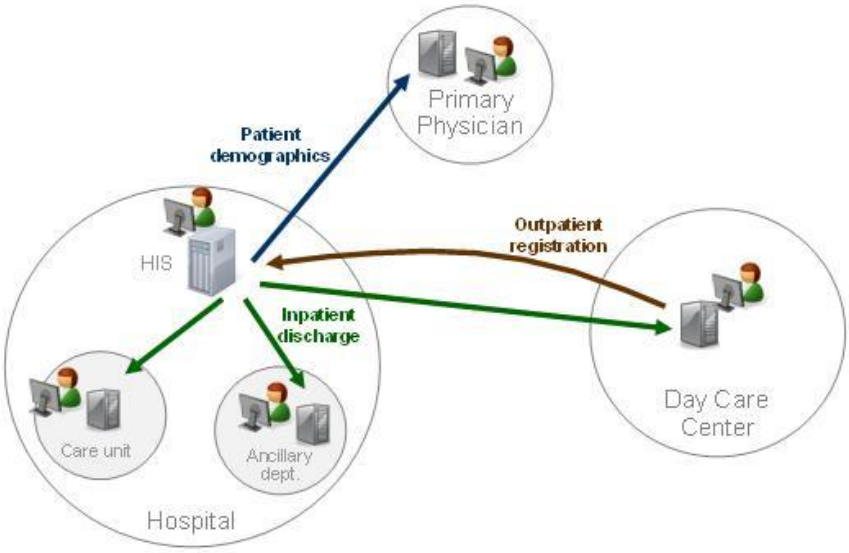
3.1.1.16 IHE-PDQ – Patient Demographics Query

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	

Description	The Patient Demographics Query (PDQ) Integration Profile lets applications query a central patient information server and retrieve a patient's demographic and visit information. Allows a Patient Demographics Supplier actor to receive a Patient Demographics Query or Patient Demographics and Visit Query request from the Patient Demographics Consumer actor, and returns demographics (and, where appropriate, visit) information. When the Patient Demographics Supplier Actor is grouped with actors in other IHE profiles that perform patient information reconciliation activities (e.g., Radiology PIR), the PDQ Supplier Actor may use the updated information to respond to PDQ Queries. In addition, the Patient Demographics Query Profile may play an integral workflow role in conjunction with other IHE Profiles.
Dependencies	HL7v2.5
Example of Use Case	Request and results distribution workflow for laboratory within a hospital

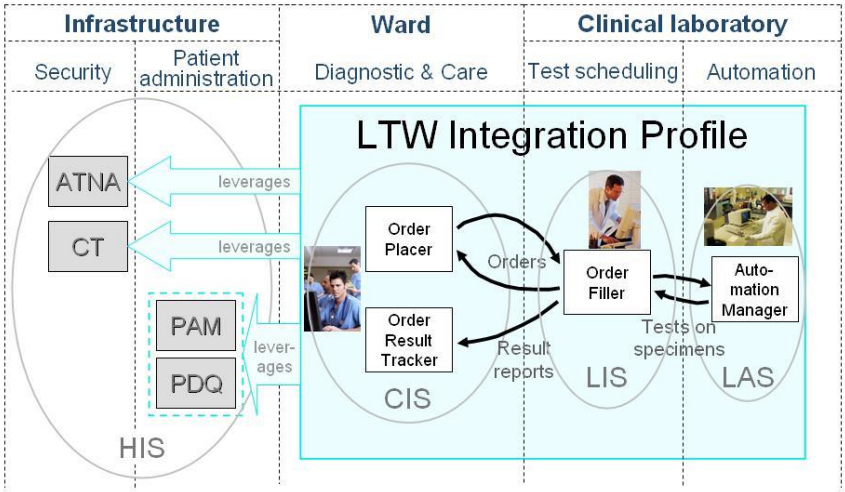
3.1.1.17 IHE-PAM – Patient Administration Management

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The PAM profile specifies two transactions to fulfil two great missions among applications cooperating in healthcare: • Patient Identity Feed: Maintain consistency of patient demographics (i.e. patient identification, full identity and persons related to the patient) across applications operating in acute care settings as well as in the ambulatory environment. • Patient Encounter Management: Coordinate the exchange of patient account, encounter and location information within and between acute care settings. These two transactions provide sets of event-triggered messages, notifying the creation and update of patient administrative data. Each transaction involves a pair of (Supplier, Consumer) Actors. Transaction Patient Identity Feed operates in a centralised manner (one Supplier application providing a number of Consumers). Transaction Patient Encounter Management can work in centralised mode as well as in peer to peer mode (Several applications cooperating as peers, each one playing alternatively Supplier and Consumer roles). Transaction Patient Encounter Management can be self-contained in a sense that the Patient Encounter Supplier sends both patient encounter information and patient identity and demographics information (in the context of the encounter data) to the Patient Encounter Consumer. In addition, this transaction also allows the Patient Encounter Supplier to send messages to the Patient Encounter Consumer for patient identity maintenance in the encounter context,		

	including patient update and identity merge. 
Dependencies	HL7
Example of Use Case	1. Patient Identity Management Use Case 2. Patient Encounter Management Use Case

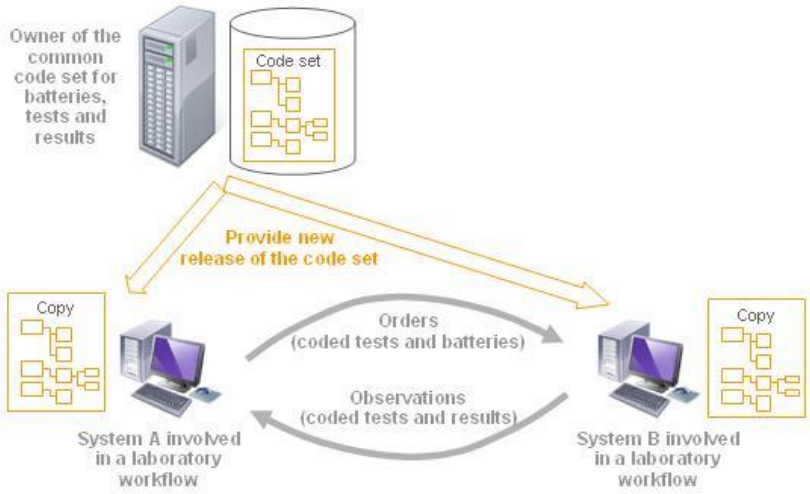
3.1.1.18 IHE-LTW – Laboratory Testing Workflow

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The Laboratory Testing Workflow Profile covers the workflow related to tests performed on in vitro specimens by a clinical laboratory inside a healthcare institution, for both existing and pending orders, related to identified patients and unidentified or misidentified patients. It maintains the consistency of patient and order information from registration through ordering, scheduling, pre-analytical processing, testing, technical and clinical validation, to results reporting and usage of laboratory observations and comments by the care providers.		

	
Dependencies	• HL7 v2.5 • Patient Administration Management (PAM) and/or Patient Demographics Query (PDQ) provide accurate patient demographics used by LTW. • Audit Trail and Node Authentication (ATNA) to audit creation and access to patient data during LTW. • Consistent Time (CT) to ensure timestamps in LTW data and audit messages are accurate.
Example of Use Case	1. Order placed with specimens collected and identified by the orderer 2. Order placed with specimens collected by a third party, then identified and labeled by the laboratory information system 3. Order generated by the laboratory and notified to the ordering system to obtain an order number.

3.1.1.19 IHE-LCSD – Laboratory Code Sets Distribution

Adoption Level		**Maturity**	
Standard Organisation		**Version**	
Description	A set of common codes is generally used by multiple application systems in a laboratory workflow environment. These common codes need to be synchronised across the various applications at a given site. In many implementations, one application system will be the owner (the "master") of the code set. The responsibility for managing a code set may also be distributed among different systems. This profile provides a way for the master of a code set (battery, test and observation codes) to send the code set to other applications.		

	 The LCSD Integration Profile defines a single Transaction called LAB-51. This transaction is based on HL7 release 2.5 or 2.5.1 messaging standard, namely the "master file notification" messages "MFN": • LAB-51 Laboratory Code Set Management. This transaction provides the set of MFN messages that enable to replace wholly the current version of a code set with a new version: • MFN^M08: Tests producing numeric results. In addition, this message can carry the units of measure, the range of decimal precision and the reference range. • MFN^M09: Tests producing categorical observations. In addition, this message can carry the list of valid answers (coded or textual) for each test. It also carries the preferred coding system used. • MFN^M11: Tests producing calculated observations. In addition, this message can carry the derivation rule, which will produce the observations. • MFN^M10: Batteries or panels. This message carries the batteries, their characteristics and the list of tests they are composed of.
Dependencies	HL7 v2.5
Example of Use Case	The system owning a laboratory code set

3.1.1.20 IHE-DIS – Pharmacy Dispense Document

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Pharmacy Dispense Document Profile (DIS) describes the content and format of a dispense document generated during the process in which a health care professional (in most cases, but not necessarily always, a pharmacist) hands out a medication to a patient. Documents created according to this profile are intended to be used in the		

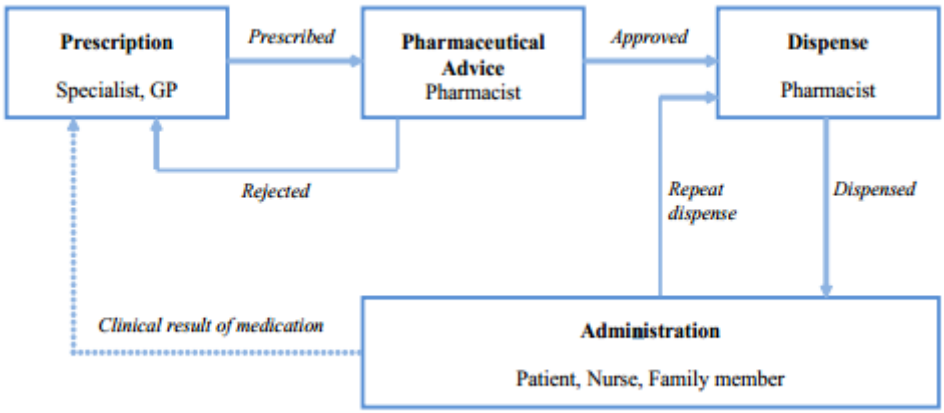
	context of the “Community Prescription and Dispense” Integration Profile (CMPD).
Dependencies	HL7 v3 Content Modules
Example of Use Case	Dispensing a prescribed item

3.1.1.21 IHE-DEC – Device Enterprise Communication

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	This profile addresses the need for consistent communication of PCD (Patient Care Device) data to the enterprise. Recipients of enterprise PCD data include, but are not limited to, Clinical Decision Support applications, Clinical Data Repositories (CDRs), Electronic Medical Record applications (EMRs), and Electronic Health Records (EHRs). Examples of patient care devices included in this profile include, but are not limited to, vital signs monitors, point of care blood analysers, infusion pumps, point of care glucometers, anesthesia systems, ventilators, and dialysis systems. The Device Enterprise Communication profile provides an optional "Publish/Subscribe" mechanism for applications to negotiate which PCD messages are communicated to a given application based on negotiated predicates. Publish and subscribe refers to the ability of one system, the publisher, to offer a data stream that can be sent to recipient systems upon subscription. This profile also provides an option to address the binding of the patient identification with the data from a PCD. Patient care device data includes periodic physiologic data (heart rate, invasive blood pressure, respiration rate, etc.), aperiodic physiologic data (non-invasive blood pressure, patient weight, cardiac output, etc.), CLIA waived (or equivalent international waiver) point-of-care laboratory tests (i.e. home blood glucose, etc.), and continuous data (ECG and invasive blood pressure waveforms). It must include patient identity data and may include contextual data such as caregiver identification, and patient care device configuration information. The Device Enterprise Communication (DEC) profile addresses the need for consistent communication of periodic, aperiodic, and CLIA waived patient care device data to the enterprise. Enterprise recipients of patient care device data include, but are not limited to, Clinical Decision Support applications, Clinical Data Repositories (CDRs), Electronic Medical Record (EMRs) applications, and Electronic Health Records (EHRs). The following examples describe which actors typical systems might be expected to support. This is not intended to define requirements, but rather to provide illustrative examples.		

	• A general purpose observation reporting gateway which combines the Device Observation Reporter and the Device Observation Filter. • A clinical decision support application which combines the Device Observation Consumer and Device Observation Filter. • A patient care device which bundles the Device Observation Reporter and the Device Observation Filter.
Dependencies	
Example of Use Case	All use cases that require data from a medical device

3.1.1.22 IHE-CMPD – Community Medication Prescription and Dispense

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Community Medication Prescription and Dispense Integration Profile (CMPD) describe the process of prescription, validation and dispense of medication in the community domain. In general, the medication business process consists of four distinct processes, which have to be connected through interactions that transfer information and/or guide the workflow. The following figure shows this flow:  In the Community Pharmacy domain, the process of “administration of medication” can usually not be governed by IT based systems so just the processes “Prescription”, “Pharmaceutical Advice” and “Dispense” are covered by the Community Pharmacy Prescription and Dispense Profile only. The CMPD Profile is intended to be used in the context of the Pharmacy Content Profiles: • Pharmacy Prescription Supplement (PRE) • Pharmacy Pharmaceutical Advice Supplement (PADV) • Pharmacy Dispense Supplement (DIS)		

	• Pharmacy Medication List (PML) These Content Profiles are based on the Patient Care Coordination (PCC) Technical Framework and define the semantic of the payload transported by the CMPD Profile
Dependencies	• IHE-XDS • IHE-ATNA • IHE-CT • IHE-XDW • IHE-PCC
Example of Use Case	Administration of medication in the Community Pharmacy

3.1.1.23 IHE- PADV Pharmacy Pharmaceutical Advice Supplement

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Pharmacy Pharmaceutical Advice Document Profile (PADV) describes the content and format of a pharmaceutical advice document generated during the process in which a health care professional (in most cases, but not necessarily always, a pharmacist) validates a Prescription. Item of a prescription against pharmaceutical knowledge and regulations. The validation can be with regard to conflicts with other Prescription Items or current medication of the patient or other reasons which affect the further processing of the Prescription Item (may be dispensed, dispensed with change, etc.). The Community Pharmacy Prescription and Dispense workflow includes the stage of validation of a prescription by a health care professional, usually different from the prescriber, possibly also supported by expert systems. A Pharmaceutical Advice document is the outcome of the validation or review of one Prescription- or Dispense Item. It contains the overall result of the validation or review which affects the further processing as well as additional information such as Intolerances, Contraindications and Allergies (ICAs) and all other information which was discovered during validation. A Pharmaceutical Advice document is also used to manage Prescription- or Dispense Items (e.g., change, cancel, etc.) as well as to document Medication Interaction Checking Issues and their resolutions. This profile defines the content and format of such a Pharmaceutical Advice document`.		
Dependencies	• HL7 v3 NE 2009 (It's not a standard, a Normative Edition (NE) is a publication of the HL7 v3 standard documentation which contains the latest normative versions of all domains) • CDA v2 • CCD		

	• XMLXSL • LOINC • IHE-PCC (It is not a standard, IHE Patient Care Coordination (PCC) domain was established in July 2005 to deal with integration issues that cross providers, patient problems or time. It deals with general clinical care aspects such as document exchange, order processing, and coordination with other specialty domains. PCC also addresses workflows that are common to multiple specialty areas and the integration needs of specialty areas that do not have a separate domain within IHE.)
Example of Use Case	• Validating a prescribed item • Reviewing and manage a dispensed item (stopping) • Reviewing and manage a dispensed item (changing) • Reviewing and manage a dispensed item (suspend/reactivate)

3.1.1.24 IHE-PML Pharmacy Medication List

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Draft for Public Comment
Description	The Pharmacy Medication List Profile (PML) describes the content and format of a Medication List document generated during a process in which a health care professional (physician, pharmacist, nurse, etc.) requests this information (e.g., to support its prescribing).Documents created according to this profile are intended to be used in the context of the “Community Prescription and Dispense” Integration Profile. A Medication List document is the documentation of the performed determination of the Medication list. It contains a set of Prescription- and/or Dispense Items (and their related Pharmaceutical Advice Items) representing the Medication information of the patient at a certain point of time and according to business rules specified out of scope of this profile.		
Dependencies	• HL7 v3 NE 2009 (It’s not a standard, a Normative Edition (NE) is a publication of the HL7 v3 standard documentation which contains the latest normative versions of all domains) • CDA v2 • CCD • XMLXSL		
Example of Use Case	Request Medication List		

3.1.1.25 IHE XCPD Cross-Community Patient Discovery

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Cross-Community Patient Discovery (XCPD) profile supports the means to locate communities which hold patient relevant health data and the translation of patient identifiers across communities holding the same patient's data. A community is defined as a group of facilities/enterprises that have agreed to work together using a common set of policies for the purpose of sharing health information within the community via an established mechanism. Facilities/enterprises may host any type of healthcare application such as EHR, PHR, etc. A community is identifiable by a globally unique id called the homeCommunityId. Membership of a facility/enterprise in one community does not preclude it from being a member in another community. Such communities may be XDS Affinity Domains which define document sharing using the XDS profile or any other communities, no matter what their internal sharing structure.		
Dependencies	• IHE-ATNA • IHE-CT		
Example of Use Case	• Share patient information in a federate EHR		

3.1.1.26 IHE-XCF Cross Community Fetch

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The Cross-Community Fetch (XCF) profile defines a single transaction for accessing medical data between gateways that facilitate multiple dimensions of communication (trust, semantics, encoding, legislation, authority, etc.). XCF is related to the Cross-Community Access (XCA) profile. When only a few dynamically created documents are needed from the other community, a single transaction may reduce implementation difficulty when transcoding and translation of the documents is desirable. XCF simplifies the implementation of stateless Responding Gateways, at the expense of possibly more complex Initiating Gateway deployment. The XCF Profile prerequisites are: • the document properties to be communicated are known in advance, • the result data sets can be characterised in advance, • the documents are feasible to be returned in a single response, • no further selection and/or manual interaction is needed in the communication		

	process, • preconditions, such as purpose of use, legitimate data, and environment, are agreed upon in advance and are documented in a community or framework agreement, • it may not be assumed in every case that the same query with the same query parameters will return the same document version with the same document id.
Dependencies	• ebRIM OASIS/ebXML Registry Information Model v3.0 • ebRS OASIS/ebXML Registry Services Specifications v3.0
Example of Use Case	
Comments	Ideally, only one document will satisfy the Fetch (e.g., only the most current instance of a patient summary is provided by the Responding Gateway). If the set of documents returned is too large, an error code is returned by the Responding Gateway. If these prerequisites cannot be met then XCA can not be used.

3.1.1.27 IHE XUA

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	Cross-Enterprise User Assertion Profile (XUA) - provides a means to communicate claims about the identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross-enterprise transactions there is a need to identify the requesting principal in a way that enables the receiver to make access decisions and generate the proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the users, as well as others that may have chosen to use a third party to perform the authentication. The XUA profile carries a readable and verifiable claim of the user identity, authentication method, and as needed their roles, purpose of use, and consent.		
Dependencies	• HL7 V3		
Example of Use Case	• User Authentication • HL7 Export/Import • HL7 Query • DICOM Export/Import • DICOM Query • Etc…		
Comments	It is important to cover the extension of this profile called IHE-XUA++		

3.1.1.28 IHE DSG - Document Digital Signature

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	Electronic documents are being increasingly relied upon in healthcare. Signatures have been a part of the electronic documentation process in health care and have traditionally been indicators of accountability. Reliable exchange of data between disparate systems requires a standard that implements non-repudiation to prevent document creators from denying authorship and rejecting responsibility. Other IHE clinical domains are encouraged to utilise the digital signature document described in this profile to sign their clinical and administrative documents and use their defined message transfer or use of XDS. For example, Patient Care Coordination could create a patient care workflow that relies on signature or the sharing of patient consent documents. The infrastructure to do the signing, verification, and identity management exists and is not defined in this profile. The specific Private Key Infrastructure (PKI) is not identified by this profile. Whichever infrastructure is selected shall adhere to ISO TS-17090 standards for PKI in healthcare. The scope of this supplement profile is currently limited to by-reference signatures, where the signature is a reference to the whole document. This document content profile can be used by domains wanting to implement e-referral and e-prescription using signatures by-reference in XDS. Other forms of signatures such as embedded signatures and partial XML signatures are out of scope for this profile. Eg: DICOM, PDF, Digitally signed report. An XDS Repository is not responsible to validate any signature documents it stores. Only Document Sources and Document Consumer Actors are responsible to produce and process document content.		
Dependencies	• IHE-XDS		
Example of Use Case	• Electronic documents exchange		

3.1.1.29 ISO 27799

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	:2008
Description	ISO 27799 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard. ISO 27799 specifies a set of detailed controls for managing health information security		

	and provides health information security best practice guidelines. By implementing this International Standard, healthcare 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. ISO 27799 applies to health information in all its aspects; whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.
Dependencies	ISO 27002:2013
Example of Use Case	Any transmission of health data between devices

3.1.1.30 IHE-XDM - Cross Enterprise Document Media Interchange

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	This Integration Profile, referred to as XDM (for Cross-Enterprise Document Media Interchange), complements the existing XDS Integration Profile by providing for the use of XDS defined formats and metadata in a simpler environment: • Transfer of documents and related metadata over CD-R and USB memory devices • Transfer of documents and related metadata over email using a ZIP attachment It focuses on providing a standards-based specification for managing the interchange of documents that healthcare enterprises (anywhere from a private physician to a clinic to an acute care in-patient facility) have decided to explicitly exchange documents using media between the patient and the patient's care providers, or between care providers. This enables better interoperability between Electronic Health Records (EHRs) and Personal Health Records (PHRs), as a natural complement to the IHE ITI XDS Integration Profile (for cross-enterprise document sharing).		
Dependencies			
Example of Use Case			

3.1.1.31 IHE-XPID - Change Management

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	Trial
Description	The XAD-PID Change Management (XPID) profile provides a means by which a XDS Document Registry can be notified of external changes to XDS Affinity Domain Patient IDs (XAD-PIDs) links so that it can affect these changes, as appropriate, in its database. This profile addresses only the linking of patient identifiers. Linking of patient identifiers supports an environment where multiple patient identifier domains are being used and translation among those patient identifiers is needed to enable patient identification across patient identifier domains. Patient identifiers across patient identifier domains can be linked, reflecting that the same patient is identified by all linked identifiers, and can be unlinked, reflecting that it was later found that the identifiers previously linked are not referring to the same patient.		

Dependencies	
Example of Use Case	

3.1.2 Architectural

This section covers the standards that define the architecture from a IT perspective that have to be defined to support the health business processes in a uniform and standard way.

3.1.2.1 ISO 17090-3:2008			
Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2008
Description	ISO 17090-3:2008 gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements. ISO 17090-3:2008 also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare. The healthcare industry is faced with the challenge of reducing costs by moving from paper-based processes to automated electronic processes. New models of healthcare delivery are emphasising the need for patient information to be shared among a growing number of specialist healthcare providers and across traditional organisational boundaries. Healthcare information concerning individual citizens is commonly interchanged by means of electronic mail, remote database access, electronic data interchange and other applications. The Internet provides a highly cost-effective and accessible means of interchanging information, but it is also an insecure vehicle that demands additional measures be taken to maintain the privacy and confidentiality of information. Threats to the security of health information through unauthorised access (either inadvertent or deliberate) are increasing. It is essential to have available to the healthcare system reliable information security services that minimise the risk of unauthorised access. How does the healthcare industry provide appropriate protection for the data conveyed across the Internet in a practical, cost-effective way? Public key infrastructure (PKI) and digital certificate technology seek to address this challenge. The proper deployment of digital certificates requires a blend of technology, policy and administrative processes that enable the exchange of sensitive data in an unsecured environment by the use of “public key cryptography” to protect information in transit and “certificates” to confirm the identity of a person or entity. In healthcare environments, this technology uses authentication, encipherment and digital signatures to facilitate confidential access to, and movement of, individual health records to meet both clinical and administrative needs. The services offered by the deployment of digital certificates (including encipherment, information integrity and digital signatures) are able to address many of these security issues. This is especially the case if digital		

	certificates are used in conjunction with an accredited information security standard. Many individual organisations around the world have started to use digital certificates for this purpose. Interoperability of digital certificate technology and supporting policies, procedures and practices is of fundamental importance if information is to be exchanged between organisations and between jurisdictions in support of healthcare applications (for example between a hospital and a community physician working with the same patient). Achieving interoperability between different digital certificate implementations requires the establishment of a framework of trust, under which parties responsible for protecting an individual's information rights may rely on the policies and practices and, by extension, the validity of digital certificates issued by other established authorities. Many countries are deploying digital certificates to support secure communications within their national boundaries. Inconsistencies will arise in policies and procedures between the certification authorities (CAs) and the registration authorities (RAs) of different countries if standards development activity is restricted to within national boundaries. Digital certificate technology is still evolving in certain aspects that are not specific to healthcare. Important standardisation efforts and, in some cases, supporting legislation are ongoing. On the other hand, healthcare providers in many countries are already using or planning to use digital certificates. ISO 17090 seeks to address the need for guidance of these rapid international developments. ISO 17090 describes the common technical, operational and policy requirements that need to be addressed to enable digital certificates to be used in protecting the exchange of healthcare information within a single domain, between domains and across jurisdictional boundaries. Its purpose is to create a platform for global interoperability. It specifically supports digital certificate-enabled communication across borders, but could also provide guidance for the national or regional deployment of digital certificates in healthcare. The Internet is increasingly used as the vehicle of choice to support the movement of healthcare data between healthcare organisations and is the only realistic choice for cross-border communication in this sector.
Dependencies	
Example of Use Case	All communications to exchange information

3.1.2.2 SAML v2 - Security Assertion Markup Language

Adoption Level		**Maturity**	

Standard Organisation	OASIS	**Version**	2.0
Description	Security Assertion Markup Language 2.0 (SAML 2.0) is a version of the SAML standard for exchanging authentication and authorisation data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, that is, an identity provider, and a SAML consumer, that is, a service provider. SAML 2.0 enables web-based authentication and authorisation scenarios including cross-domain single sign-on (SSO), which helps reduce the administrative overhead of distributing multiple authentication tokens to the user. SAML 2.0 was ratified as an OASIS Standard in March 2005, replacing SAML 1.1. The critical aspects of SAML 2.0 are covered in detail in the official documents SAMLConform, SAMLCore, SAMLBind and SAMLProf. Some 30 individuals from more than two dozen companies and organisations were involved in the creation of SAML 2.0. In particular, and of special note, Liberty Alliance donated its Identity Federation Framework (ID-FF) specification to OASIS, which became the basis of the SAML 2.0 specification. Thus SAML 2.0 represents the convergence of SAML 1.1, Liberty ID-FF 1.2, and Shibboleth 1.3.		
Dependencies	Digital Certificates		
Example of Use Case	Applies to all use cases that involves or requires a relationship between two or more entities		

3.1.2.3 WS-I Basic Profile

Adoption Level		**Maturity**	
Standard Organisation	WS-I	**Version**	2.0
Description	The WS-I Basic Profile (official abbreviation is BP), a specification from the Web Services Interoperability industry consortium (WS-I), provides interoperability guidance for core Web Services specifications such as SOAP, WSDL, and UDDI. The profile uses Web Services Description Language (WSDL) to enable the description of services as sets of endpoints operating on messages. To understand the importance of WSI-BP, note that it defines a much narrower set of valid services than the full WSDL or SOAP schema. Many common platforms support WSI-BP but do not support services outside of it. Compare the WSDL 1.1 specification to the subset permitted in WSI-BP. Also note that WSI-BP generally narrows the SOAP specification. There is a notable exception where WSI expands on the SOAP standard, and that is in adding xml:lang attribute on fault elements.		
Dependencies	SOAP 1.2		

Example of Use Case	All uses cases that require retrieve or insert information in other entity

3.1.2.4 WS-Addressing

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	
Description	Web Services Addressing (WS-Addressing) defines two interoperable constructs that convey information that is typically provided by transport protocols and messaging systems. These constructs normalise this underlying information into a uniform format that can be processed independently of transport or application. The two constructs are endpoint references and message information headers. A Web service endpoint is a (referenceable) entity, processor, or resource where Web service messages can be targeted. Endpoint references convey the information needed to identify/reference a Web service endpoint, and may be used in several different ways: endpoint references are suitable for conveying the information needed to access a Web service endpoint, but are also used to provide addresses for individual messages sent to and from Web services. To deal with this last usage case this specification defines a family of message information headers that allows uniform addressing of messages independent of underlying transport. These message information headers convey end-to-end message characteristics including addressing for source and destination endpoints as well as message identity. Both of these constructs are designed to be extensible and re-usable so that other specifications can build on and leverage endpoint references and message information headers.		
Dependencies			
Example of Use Case			

3.1.2.5 WS-I Basic security

Adoption Level		**Maturity**	
Standard Organisation	WS-I	**Version**	1.1
Description	The Profile was developed according to a set of principles that, together, form the philosophy of the Basic Security Profile 1.1, as it relates to bringing about interoperability. This section documents these guidelines. No guarantee of interoperability Although it is impossible to completely guarantee the interoperability of a particular		

service, the Basic Security Profile 1.1 attempts to increase interoperability by addressing the most common problems that implementation experience has revealed to date.

Focus profiling effort

The focus of the Basic Security Profile 1.1 is the specifications that are explicitly defined as in-scope for the Basic Security Profile 1.1. Other specifications are profiled to the minimal extent necessary to allow meaningful profiling of the scoped specifications. This allows an in-depth profile of the scoped specifications with reduced constraining of other specifications.

Application semantics

Although communication of application semantics can be facilitated by the technologies that comprise the Basic Security Profile 1.1, assuring the common understanding of those semantics is not addressed by it.

Testability

When possible, the Basic Security Profile 1.1 makes statements that are testable. However, such testability is not required. Preferably, testing is achieved in a non-intrusive manner (e.g., examining artifacts "on the wire"). Note: Due to the nature of cryptographic security, non-intrusive testing may not be possible.

Strength of requirements

The Profile makes strong requirements wherever feasible; if there are legitimate cases where such a requirement cannot be met, conditional are used. Optional and conditional requirements introduce ambiguity and mismatches between implementations.

Restriction vs. relaxation

When amplifying the requirements of referenced specifications (including the Basic Profile 1.0), the Basic Security Profile 1.1 may restrict them, but does not relax them.

Multiple mechanisms

If a referenced specification allows multiple mechanisms to be used interchangeably to achieve the same goal, the Basic Security Profile 1.1 selects those that are well-understood, widely implemented and useful. Extraneous or underspecified mechanisms and extensions introduce complexity and therefore reduce interoperability.

Future compatibility

When possible, the Basic Security Profile 1.1 aligns its requirements with in-progress revisions to the specifications it references. This aids implementers by enabling a graceful transition, and assures that WS-I does not 'fork' from these efforts. When the Basic Security Profile 1.1 cannot address an issue in a specification it references, this

	information is communicated to the appropriate body to assure its consideration. Compatibility with deployed services Backwards compatibility with deployed Web services is not a goal for the Basic Security Profile 1.1, but due consideration is given to it; the Profile does not introduce a change to the requirements of a referenced specification unless doing so addresses specific interoperability issues. Focus on interoperability Although there are potentially a number of inconsistencies and design flaws in the referenced specifications, the Basic Security Profile 1.1 only addresses those that affect interoperability. Conformance targets Where possible, the Basic Security Profile 1.1 places requirements on artifacts (e.g., WSDL descriptions, SOAP messages) rather than the producing or consuming software's behaviors or roles. Artifacts are concrete, making them easier to verify and therefore making conformance easier to understand and less error-prone. Lower-layer interoperability The Profile speaks to interoperability at the web-services layer only; it assumes that interoperability of lower-layer protocols (e.g. TCP, HTTP) and technologies (e.g. encryption and signature algorithms) is adequate and well-understood. WS-I does not attempt to assure the interoperability of these protocols and technologies as a whole. This assures that WS-I's expertise in and focus on Web Services standards is used effectively. Do no harm Interoperability of security technologies does not in and of itself ensure security, and the act of combining new technologies and protocols is especially susceptible to security threats. The profile takes steps to avoid introducing new security threats. Best Practices It is not the intent of the Basic Security Profile 1.1 to define security best practices. However, when multiple options exist, it may uses known security weaknesses as a means of reducing choice and thus enhancing interoperability. The Basic Security Profile 1.1 will offer non-normative security considerations where the authors deem appropriate; however, these are by no means exhaustive and should not be perceived as a sanctioning of a security best practice. Selected Errata Inclusion The Basic Security Profile 1.1 restates selected requirements from the WS-Security Errata rather than including the entire Errata by reference, preferring interoperability

	over strict conformance.
Dependencies	• SOAP 1.2 • SAML v2
Example of Use Case	All use cases that require web services as way to interoperate between the systems involved

3.1.2.6 WS-TRUST V1.3

Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	1.3
Description	WS-Trust is a WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange. The WS-Trust specification was authored by representatives of a number of companies, and was approved by OASIS as a standard in March 2007. Using the extensions defined in WS-Trust, applications can engage in secure communication designed to work within the Web services framework		
Dependencies			
Example of Use Case			

3.1.2.7 WSDL 1.1

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	1.1
Description	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate. A WSDL document defines services as collections of network endpoints, or ports. In WSDL, the abstract definition of endpoints and messages is separated from their		

	concrete network deployment or data format bindings. This allows the reuse of abstract definitions: messages, which are abstract descriptions of the data being exchanged, and port types which are abstract collections of operations. The concrete protocol and data format specification for a particular port type constitutes a reusable binding. A port is defined by associating a network address with a reusable binding, and a collection of ports define a service. Hence, a WSDL document uses the following elements in the definition of network services: • Types– a container for data type definitions using some type system (such as XSD). • Message– an abstract, typed definition of the data being communicated. • Operation– an abstract description of an action supported by the service. • Port Type–an abstract set of operations supported by one or more endpoints. • Binding– a concrete protocol and data format specification for a particular port type. • Port– a single endpoint defined as a combination of a binding and a network address. • Service– a collection of related endpoints. In addition, WSDL defines a common binding mechanism. This is used to attach a specific protocol or data format or structure to an abstract message, operation, or endpoint. It allows the reuse of abstract definitions. In addition to the core service definition framework, this specification introduces specific binding extensions for the following protocols and message formats: • SOAP 1.1 • HTTP GET / POST • MIME
Dependencies	HTTP 1.1
Example of Use Case	All use cases that require web services as way to interoperate between the systems involved

3.1.2.8 HTTP 1.1

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	1.1
Description	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. A feature of HTTP is the typing and negotiation of data		

	representation, allowing systems to be built independently of the data being transferred. HTTP has been in use by the World-Wide Web global information initiative since 1990. This specification defines the protocol referred to as "HTTP/1.1", and is an update to RFC 2068. HTTP has been in use by the World-Wide Web global information initiative since 1990. The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet. HTTP/1.0, as defined by RFC 1945, improved the protocol by allowing messages to be in the format of MIME-like messages, containing metainformation about the data transferred and modifiers on the request/response semantics. However, HTTP/1.0 does not sufficiently take into consideration the effects of hierarchical proxies, caching, the need for persistent connections, or virtual hosts. In addition, the proliferation of incompletely-implemented applications calling themselves "HTTP/1.0" has necessitated a protocol version change in order for two communicating applications to determine each other's true capabilities. This specification defines the protocol referred to as "HTTP/1.1". This protocol includes more stringent requirements than HTTP/1.0 in order to ensure reliable implementation of its features. Practical information systems require more functionality than simple retrieval, including search, front-end update, and annotation. HTTP allows an open-ended set of methods and headers that indicate the purpose of a request. It builds on the discipline of reference provided by the Uniform Resource Identifier (URI), as a location (URL) or name (URN), for indicating the resource to which a method is to be applied. Messages are passed in a format similar to that used by Internet mail as defined by the Multipurpose Internet Mail Extensions (MIME). HTTP is also used as a generic protocol for communication between user agents and proxies/gateways to other Internet systems, including those supported by the SMTP, NNTP, FTP, Gopher, and WAIS protocols. In this way, HTTP allows basic hypermedia access to resources available from diverse applications.
Dependencies	TCP/IP
Example of Use Case	

3.1.2.9 SOAP 1.2

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	1.2
Description	SOAP Version 1.2 (SOAP) is a lightweight protocol intended for exchanging structured information in a decentralised, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation		

	specific semantics. Two major design goals for SOAP are simplicity and extensibility. SOAP attempts to meet these goals by omitting, from the messaging framework, features that are often found in distributed systems. Such features include but are not limited to "reliability", "security", "correlation", "routing", and "Message Exchange Patterns" (MEPs). While it is anticipated that many features will be defined, this specification provides specifics only for two MEPs. Other features are left to be defined as extensions by other specifications. The SOAP Version 1.2 specification defines the SOAP messaging framework consisting of: • The SOAP processing model defining the rules for processing a SOAP message • The SOAP Extensibility model defining the concepts of SOAP features and SOAP modules • The SOAP underlying protocol binding framework describing the rules for defining a binding to an underlying protocol that can be used for exchanging SOAP messages between SOAP nodes • The SOAP message construct defining the structure of a SOAP message
Dependencies	HTTP 1.1
Example of Use Case	

3.1.2.10 UDDI 3

Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	3.0.2
Description	Web services are meaningful only if potential users may find information sufficient to permit their execution. The focus of Universal Description Discovery & Integration (UDDI) is the definition of a set of services supporting the description and discovery of: • Businesses, organisations, and other Web services providers • The Web services they make available • The technical interfaces which may be used to access those services. Based on a common set of industry standards, including HTTP, XML, XML Schema, and SOAP, UDDI provides an interoperable, foundational infrastructure for a Web services-based software environment for both publicly available services and services only exposed internally within an organisation. UDDI was written in August 2000, at a time when the authors had a vision of a world in		

	which consumers of web services would be linked up with providers through a public or private dynamic brokerage system. In this vision, anyone needing a service, such as credit card authentication, would go to their service broker and select a service supporting the desired SOAP (or other) service interface, and meeting other criteria. In such a world, the publicly operated UDDI node or broker would be critical for everyone. For the consumer, public or open brokers would only return services listed for public discovery by others, while for a service producer, getting a good placement in the brokerage—by relying on metadata of authoritative index categories—would be critical for effective placement.
Dependencies	• HTTP 1.1 • SOAP 1.2 • XML
Example of Use Case	

3.1.2.11 IEEE 1003.2 POSIX Shell Standard

Adoption Level		**Maturity**	
Standard Organisation	IEEE	**Version**	1003.2
Description	There have been many attempts to standardise UNIX. Hardware companies' monolithic attempts at market domination, fragile industry coalitions, marketing failures, and other such efforts are the stuff of history-and the stuff of frustration. Only one standardisation effort has not been tied to commercial interests: the Portable Operating System Interface, known as POSIX. This effort started in 1981 with the /usr/group (now UniForum) Standards Committee, which produced the /usr/group Standard three years later. The list of contributors grew to include the Institute of Electrical and Electronic Engineers (IEEE) and the International Organisation for Standardisation (ISO). The first POSIX standard was published in 1988. This one, called IEEE P1003.1, covers low-level issues at the system call level. IEEE P1003.2, covering the shell, utility programs, and user interface issues, was ratified in September 1992 after a six-year effort. The POSIX standards were never meant to be rigid and absolute. Instead, the standards are designed to be flexible enough to allow for both coexistence of similar available software, so that existing code isn't in danger of obsolescence, and the addition of new features, so that vendors have the incentive to innovate. In other words, they are supposed to be the kind of third-party standards that vendors might actually be interested in following. POSIX 1003.2 itself consists of two parts. The first, 1003.2, addresses shell script		

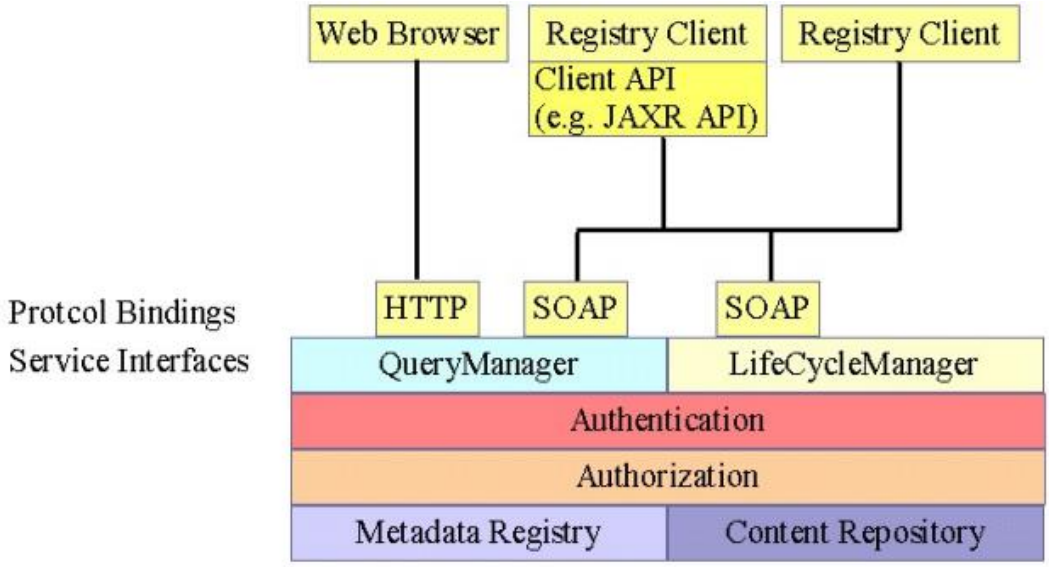
	portability; it defines the shell and the standard utilities. The second, 1003.2a, called the User Portability Extensions (UPE), defines standards of interactive shell use and interactive utilities like the vi editor. The committee members had two motivating factors to weigh when they designed the 1003.2 shell standard. On the one hand, the design had to accomodate, as much as possible, existing shell code written under various Bourne-derived shells (the Version 7, System V, BSD, and Korn shells). These shells are different in several extremely subtle ways, most of which have to do with the ways certain syntactic elements interact with each other.
Dependencies	
Example of Use Case	

3.1.2.12 ebMS OASIS/ebXML Messaging Services Specifications v3.0

Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	3.0
Description	This specification describes a communication-protocol neutral method for exchanging electronic business messages. It defines specific enveloping constructs supporting reliable, secure delivery of business information. Furthermore, the specification defines a flexible enveloping technique, permitting messages to contain payloads of any format type. This versatility ensures that legacy electronic business systems employing traditional syntaxes (i.e. UN/EDIFACT, ASC X12, or HL7) can leverage the advantages of the ebXML infrastructure along with users of emerging technologies. The prime objective of the ebXML Messaging Service (ebMS) is to facilitate the exchange of electronic business messages within an XML framework that leverages common Internet standards, without making any assumption on the integration and consumption model these messages will follow on the back-end. These messages may be consumed in different ways that are out of scope of this specification: they may bind to a legacy application, to a service, be queued, enter a message workflow process, be expected by an already-running business process, be batched for delayed processing, be routed over an Enterprise Service Bus before reaching their consumer application, or be dispatched based on header data or payload data, etc. It is becoming critical for broad adoption among all partners – large or small - of a supply-chain, to handle differences in message flow capacity, intermittent connectivity, lack of static IP addresses or firewall restrictions. Such new capabilities played an important role in the motivation that led to ebMS 3.0, along with the need to integrate and profile the emerging SOAP-based QoS-supporting standards. The message header profiling that provided, in ebMS 2.0, a standard business-level header, has also been extended to better address the diversity of back-end binding models, as well as the		

	emerging trend in business activity monitoring, the eBusiness side of which a message handler should be able to support. The ebXML messaging framework is not a restrictive one: business messages, identified as the 'payloads' of ebXML messages, are not limited to XML documents. Traditional EDI formats may also be transported by ebMS. These payloads can take any digital form–XML, ASC X12, HL7, AIAG E5, database tables, binary image files, etc. Multiple payloads, possibly of different MIME types, can be transported in a single ebMS message. An objective of ebXML Messaging protocol is to be capable of being carried over any available transfer protocol. This version of the specification provides bindings to HTTP and SMTP, but other protocols to which SOAP may bind can also be used. The choice of an XML framework rather reflects confidence in a growing XML-based Web infrastructure and development tools infrastructure, the components of which can be leveraged and reused by developers. The ebXML infrastructure is composed of several independent, but related, components. Some references and bindings to other ebXML specifications in this document should be interpreted as aids to integration, rather than as a requirement to integrate or to use in combination. For example, ebMS may refer to the [ebCPPA] specification, rather than require its use. The ebMS relies on a concept of "Agreement", the concrete representation of which (e.g. CPA or other configuration information) is left for implementers to decide. The ebMS defines messaging functions, protocol and envelope intended to operate over SOAP (SOAP 1.1 or SOAP 1.2, and SOAP with Attachments). Binding to lower transport layers such as HTTP and SMTP relies on standard SOAP bindings when these exist, and ebMS only specifies some complement to these, as required. This version of ebMS leverages established SOAP-based specifications that handle quality of service in the domains of reliability and security. The ebMS specification defines how these are composed in the ebMS context. The design of this composition takes into account the reuse of existing implementations of these standards, not just the reuse of these standards themselves. The concept for an ebMS implementation is of an ebXML Messaging Service Handler (MSH), that is abstractly defined as implementing the specified messaging functions. Any interface to the MSH is out of scope of this specification. Although it is clearly helpful in many cases to define a standard API, such an interface should not exclude other ways applications may want to interact with an MSH. Such an interface definition should rather belong to an implementation guideline companion document. An implementation of this specification could be delivered as a wholly independent software component or as an embedded component of a larger system.
Dependencies	SOAP 1.2
Example of Use Case	

3.1.2.13 ebRS OASIS/ebXML Registry Services Specifications v3.0

Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	3.0
Description	An ebXML Registry is an information system that securely manages any content type and the standardised metadata that describes it. The ebXML Registry provides a set of services that enable sharing of content and metadata between organisational entities in a federated environment. An ebXML Registry may be deployed within an application server, a web server or some other service container. The registry MAY be available to clients as a public, semi-public or private web site. This document defines the services provided by an ebXML Registry and the protocols used by clients of the registry to interact with these services.  *Figure 1: Simplified View of ebXML Registry Architecture*		
Dependencies	• HTTP 1.1 • SOAP 1.2		
Example of Use Case	Electronic Medical Records Repository		

3.1.2.14 XML

Adoption Level		**Maturity**	

Standard Organisation	W3C	**Version**	1.0
Description	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalised Markup Language [ISO 8879]. By construction, XML documents are conforming SGML documents. XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure. [Definition: A software module called an XML processor is used to read XML documents and provide access to their content and structure.] [Definition: It is assumed that an XML processor is doing its work on behalf of another module, called the application.] This specification describes the required behavior of an XML processor in terms of how it must read XML data and the information it must provide to the application.		
Dependencies			
Example of Use Case			

3.1.2.15 XML XSL

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	
Description	XSL is a language for expressing style sheets. An XSL style sheet is, like CSS, a file that describes how to display an XML document of a given type. XSL shares the functionality and is compatible with CSS2 (although it uses a different syntax). It also adds: • A transformation language for XML documents: XSLT. Originally intended to perform complex styling operations, like the generation of tables of contents and indexes, it is now used as a general purpose XML processing language. XSLT is thus widely used for purposes other than XSL, like generating HTML web pages from XML data. • Advanced styling features, expressed by an XML document type which defines a set of elements called Formatting Objects, and attributes (in part borrowed from CSS2 properties and adding more complex ones) Styling requires a source XML documents, containing the information that the style sheet will display and the style sheet itself which describes how to display a document of a given type.		

Dependencies	• XML
Example of Use Case	

3.1.2.16 XML Schema

Adoption Level		**Maturity**	
Standard Organisation	W3C	**Version**	1.1
Description	The purpose of XML Schema Definition Language: Structures is to define the nature of XSD schemas and their component parts, provide an inventory of XML markup constructs with which to represent schemas, and define the application of schemas to XML documents. The purpose of an XSD schema is to define and describe a class of XML documents by using schema components to constrain and document the meaning, usage and relationships of their constituent parts: datatypes, elements and their content and attributes and their values. Schemas can also provide for the specification of additional document information, such as normalisation and defaulting of attribute and element values. Schemas have facilities for self-documentation. Thus, XML Schema Definition Language: Structures can be used to define, describe and catalogue XML vocabularies for classes of XML documents. Any application that consumes well-formed XML can use the formalism defined here to express syntactic, structural and value constraints applicable to its document instances. The XSD formalism allows a useful level of constraint checking to be described and implemented for a wide spectrum of XML applications. However, the language defined by this specification does not attempt to provide all the facilities that might be needed by applications. Some applications will require constraint capabilities not expressible in this language, and so will need to perform their own additional validations.		
Dependencies	XML		
Example of Use Case			

3.1.2.17 ANSI X12

Adoption Level		**Maturity**	
Standard Organisation	ANSI	**Version**	
Description	EDI ANSI X12 stands for Electronic Data Interchange, American National Standards		

	Institute X12. The EDI ANSI X12 standard was developed to govern the use of EDI to exchange information electronically between businesses. The EDI ANSI X12 standard is most prevalent in the United States and has counterparts used in other parts of the world, like the UN/EDIFACT standard that is the equivalent of EDI ANSI X12 outside the US. EDI X12 standard covers number of requirements for data structure, separators, control numbers, etc. However many big trading partners impose they own even more strict rules and requirements. It can be everything: specific data format requirements for some elements, requirement to contain specific segments (segments that are not mandatory in EDI X12 standard being made mandatory).
Dependencies	
Example of Use Case	

3.1.2.18 UN/EDIFACT - ISO 9735

Adoption Level		**Maturity**	
Standard Organisation	United Nations, ANSI, ISO	**Version**	
Description	UN/EDIFACT (the United Nations rules for Elec-tronic Data Interchange for Administration, Commerce and Transport) comprise a set of internationally agreed standards, directories, and guidelines for the electronic interchange of structured data, between independent computerised information systems. The EDIFACT standard provides: • a set of syntax rules to structure data • an interactive exchange protocol (I-EDI) • standard messages which allow multi-country and multi-industry exchange EDIFACT has a hierarchical structure where the top level is referred to as an interchange, and lower levels contain multiple messages which consist of segments, which in turn consist of composites. The final iteration is an element which is derived from the United Nations Trade Data Element Directory (UNTDED); these are normalised throughout the EDIFACT standard.		
Dependencies			
Example of Use Case			

3.1.2.19 IEEE 11073 'Personal Health Devices'

Adoption Level		**Maturity**	
Standard Organisation	IEEE	**Version**	
Description	IEEE 11073 standards are designed to help healthcare product vendors and integrators create interoperable devices and systems for disease management, health and fitness and independent living that can help save lives and improve quality of life for people worldwide. The growing IEEE 11073 family of standards is intended to enable interoperable communication for traditional medical devices, as well as personal health devices, and convey far-ranging potential benefits, such as reducing clinical decision-making from days to minutes, reducing gaps and errors across the spectrum of healthcare delivery and helping to expand the potential market for the medical devices themselves. The 12 most important standards: • IEEE 11073-10101™ "Health informatics—Point-of-care medical device communication—Part 10101: Nomenclature" • IEEE 11073-10201™ “Health informatics—Point-of-care medical device communication—Domain information model” • IEEE 11073- 20101™ “Health informatics—Point-of-care medical device communication—Application profile—Base standard” • IEEE 11073-20601™ “Health informatics—Personal health device communication—Part 20601: Application profile—Optimised exchange protocol” • IEEE 11073-20601a-2010™ “Health informatics—Personal health device communication—Part 20601: Application profile—Optimised exchange protocol” • IEEE 11073-10408™ “Health informatics—Personal health device communication—Part 10408: Device specialisation—Thermometer” • IEEE 11073-10415™ “Health informatics—Personal health device communication—Part 10415: Device specialisation—Weighing scale” • IEEE 11073-10404™ “Health informatics—Personal health device communication—Part 10404: Device specialisation—Pulse oximeter” • IEEE 11073-10421-2010™ “Health informatics—Personal health device communication Part 10421: Device specialisation—Peak expiratory flow monitor (peak flow)” • IEEE 11073-10406-2011™ “Health informatics—Personal health device communication Part 10406: Device specialisation—Basic electrocardiograph (ECG) (1- to 3-lead ECG)” • IEEE 11073-10407™ “IEEE ISO/IEEE Health informatics—Personal health device communication—Part 10407: Device specialisation—Blood pressure monitor” • IEEE 11073-10417™ “IEEE ISO/IEEE Health informatics—Personal health device communication—Part 10417: Device specialisation—Glucose meter”		

Dependencies	
Example of Use Case	

3.1.2.20 ISO/TR 16056

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	X:2004
Description	Addresses the interoperability of telehealth systems and networks. Specifically: • Standards for real---time telehealth systems: The document describes the technical standards related to real---time telehealth applications, including audio, video, and data conferencing capabilities. It also identifies gaps, overlaps and inconsistencies in the standards, and provides some guidance about how they need to evolve. • Interoperability issues in telehealth applications: The document examines interoperability aspects of real---time multimedia conferencing standards and telehealth products, and identifies areas of concern from the interoperability perspective that need to be resolved. • Requirements for interoperable telehealth systems and networks: The document defines interoperability requirements at different levels of interaction between telehealth systems and provides some guidelines on how interoperability can be achieved. • Framework for interoperable architectures: The document identifies interoperable building blocks for telehealth solutions and interactions between these building blocks, and explores the possibility of standardisation of these building blocks.		
Dependencies			
Example of Use Case			

3.1.2.21 MLLP

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	
Description	The purpose of the MLLP Protocol (Minimum Lower Layer Protocol) is to provide both a minimalistic Open Systems Interconnection (OSI)-session layer framing protocol as well as a minimalistic reliable transport protocol. If security is an issue, additional protocols or technologies will have to be layered on top of MLLP to achieve these goals. These transport specifications are not to be confused with the content of transmission infrastructure. Transmission infrastructure describes the information model, messages and interactions related to the assembly of an HL7 Version 3 composite message. The		

	transport specifications address moving the message payload (the HL7 Version 3 composite message and/or HL7 Version 2 composite message) from sender to receiver. These transports are all capable of moving HL7 Version 3 composite messages and may also support moving HL7 Version 2 and Clinical Document Architecture (CDA®) composite messages.
Dependencies	
Example of Use Case	

3.2 Syntactical Standards

Syntax refers to the structure of a communication; it can be thought of as equivalent to spelling and grammar rules. The HL7 Version 2.x messaging standard is an example of a standard for syntactic interoperability. Syntactical standards are particularly important because they define how information is packaged and communicated from one party to another. Such standards set the language, structure and data types required for seamless integration from one system to another.

3.2.1 Document Syntax

These indicate the types of information that may be included in documents and where information can be found in documents. Like CCR (Continuity of Care Record – an ASTM standard) provides a standard data set for electronic referral among healthcare professionals that includes patient identification information, encounter and treatment records, medications, allergies, and recommendations for the healthcare plan.

3.2.1.1 ASTM CCD

Adoption Level		**Maturity**	
Standard Organisation	ASTM	**Version**	
Description	The HL7/ASTM Continuity of Care Document (CCD) is an implementation guide for sharing Continuity of Care Record (CCR) patient summary data using the HL7 Clinical Document Architecture (CDA). CCD establishes a rich set of templates representing the typical sections of a summary record and expresses these templates as constraints on CDA. These same templates—for vital signs, family history, plan of care, and so on—can then be reused in other CDA document types, establishing interoperability across a wide range of clinical use cases. The CCD is the basis for interoperability in the US Health Information Technology Standards Panel (HITSP) and Integrating the Healthcare Enterprise (IHE) use cases. The CCD is a joint effort of HL7 and ASTM to foster interoperability of clinical data to allow physicians to send electronic medical information to other providers without loss of meaning, which will ultimately improve patient care. It passed balloting in February 2007 and is endorsed by the Healthcare Information Technology Standards Panel (HITSP) as the harmonised format for the exchange of clinical information including patient demographics, medications and allergies. The CCD is a CDA implementation of ASTM's Continuity of Care Record (CCR). It is intended as an alternate implementation to the one specified in ASTM ADJE2369 for those institutions or organisations committed to implementation of the HL7 Clinical Document Architecture. The CCD represents a complete implementation of CCR, combining the best of HL7 technologies with the richness of CCR's clinical data representation, and does not disrupt the existing data flows in payer, provider, or pharmacy organisations. The CCD is an XML-based standard that specifies the structure and encoding of a patient summary clinincal document. It provides a "snapshot in time," constraining a summary of the pertinent clinical, demographic, and administrative data for a specific patient. From its inception, CDA has supported the ability to represent professional society recommendations,		

	national clinical practice guidelines, standardised data sets, etc.
Dependencies	• ATSM CCR • HL7 CDA
Example of Use Case	• Integrating the Healthcare Enterprise Patient Care Coordination Profiles • Integrating the Healthcare Enterprise XDS Medical Summary for Referral and Discharge.

3.2.1.2 ASTM CCR

Adoption Level		**Maturity**	
Standard Organisation	ASTM	**Version**	
Description	The Continuity of Care Record (CCR) is a core data set of the most relevant administrative, demographic, and clinical information facts about a patient's healthcare, covering one or more healthcare encounters. It provides a means for one healthcare practitioner, system, or setting to aggregate all of the pertinent data about a patient and forward it to another practitioner, system, or setting to support the continuity of care. The primary use case for the CCR is to provide a snapshot in time containing the pertinent clinical, demographic, and administrative data for a specific patient. To ensure interchangeability of electronic CCRs, this specification specifies XML coding that is required when the CCR is created in a structured electronic format. Conditions of security and privacy for a CCR instance must be established in a way that allows only properly authenticated and authorised access to the CCR document instance or its elements. The CCR consists of three core components: the CCR Header, the CCR Body, and the CCR Footer.		
Dependencies			
Example of Use Case	• Get a snapshot in time containing the pertinent clinical, demographic, and administrative data for a specific patient		

3.2.2 Messaging Syntax

These allow for consistent data flow among systems and organisations, specifying format, data elements and structure. Common standards include HL7 for administrative and clinical care data, DICOM for radiological images.

3.2.2.1 HL7 v2.x

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	2.x
Description	HL7's Version 2.x (V2) messaging standard is the workhorse of electronic data exchange in the clinical domain and arguably the most widely implemented standard for healthcare in the world. This messaging standard allows the exchange of clinical data between systems. It is designed to support a central patient care system as well as a more distributed environment where data resides in departmental systems. The first commercial use of HL7 V2.x was version 2.1 in 1991. The current version of HL7 2.x is 2.7 that was published in 2011. HL7 v2.x has allowed for the interoperability between electronic Patient Administration Systems (PAS), Electronic Practice Management (EPM) systems, Laboratory Information Systems (LIS), Scheduling, Dietary, Pharmacy, Billing, Radiology patient monitoring devices as well.		
Dependencies			
Example of Use Case			

3.2.2.2 HL7 v3

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	3.0
Description	The Health Level Seven Version 3 (V3—a suite of specifications based on HL7's Reference Information Model (RIM)—provides a single source that allows implementers of V3 specifications to work with the full set of messages, data types, and terminologies needed to build a complete implementation. The Version 3 represents a new approach to clinical information exchange based on a model driven methodology that produces messages and electronic documents expressed in XML syntax. The V3 specification is built around subject domains that provide storyboard descriptions, trigger events, interaction designs, domain object models derived from the RIM, hierarchical message descriptors (HMDs) and a prose description of each element.		
Dependencies	HL7 v3 RIM		

Example of Use Case	

3.2.2.3 DICOM

Adoption Level		**Maturity**	
Standard Organisation	NEMA	**Version**	
Description	DICOM — Digital Imaging and Communications in Medicine — is the international standard for medical images and related information (ISO 12052). It defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use. DICOM is implemented in almost every radiology, cardiology imaging, and radiotherapy device (X-ray, CT, MRI, ultrasound, etc.), and increasingly in devices in other medical domains such as ophthalmology and dentistry. With tens of thousands of imaging devices in use, DICOM is one of the most widely deployed healthcare messaging standards in the world. There are literally billions of DICOM images currently in use for clinical care. Since its first publication in 1993, DICOM has revolutionised the practice of radiology, allowing the replacement of X-ray film with a fully digital workflow. Much as the Internet has become the platform for new consumer information applications, DICOM has enabled advanced medical imaging applications that have “changed the face of clinical medicine”. From the emergency department, to cardiac stress testing, to breast cancer detection, DICOM is the standard that makes medical imaging work — for doctors and for patients.		
Dependencies			
Example of Use Case			

3.2.3 Data Model Standards

Define the standards that establish a data structure for data exchange and the data model building blocks for other standards.

3.2.3.1 HL7 v3 RIM			
Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	3.0
Description	The HL7 Reference Information Model (RIM) is a critical component of the HL7 V3 family of standards. It is the root of all information models and structures developed as part of the V3 development process. The Reference Information Model (RIM) is the combined consensus view of information from the perspective of the HL7 working group and the HL7 affiliates. The RIM is the ultimate source from which all HL7 Version 3 standards draw their information-related content. The RIM, along with Data Types and Vocabularies are the foundation for all information modelling within HL7. The constrained models derived from these serve as documents, data for services, and messages. As such, they are a "part" of every HL7 Version 3 standard and have the same "customers" as do the standards defined from them. The RIM is a static model of health and healthcare information as viewed within the scope of HL7 standards development activities. The RIM is essential to HL7's ongoing mission of increasing precision of data. The RIM became an ANSI-approved standard in late 2003 and was published as an International Organisation for Standardisation (ISO) standard in September 2006.		
Dependencies			
Example of Use Case			

3.2.3.1 ebRIM OASIS/ebXML Registry Information Model v3.0			
Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	3.0
Description	An ebXML Registry is an information system that securely manages any content type and the standardised metadata that describes it. The ebXML Registry provides a set of services that enable sharing of content and		

	metadata between organisational entities in a federated environment. It defines the types of metadata and content that can be stored in an ebXML Registry. A separate standard, ebXML Registry: Services and Protocols [ebRS], defines the services provided by an ebXML Registry and the protocols used by clients of the registry to interact with these services. An ebXML Registry is capable of storing any type of electronic content such as XML documents, text documents, images, sound and video. Instances of such content are referred to as a RepositorytItems. RepositorytItems are stored in a content repository provided by the ebXML Registry. In addition to the RepositoryItems, an ebXML Registry is also capable of storing standardised metadata that MAY be used to further describe RepositoryItems. Instances of such metadata are referred to as a RegistryObjects (or one of its sub-types, as described later in this document). RegistryObjects are stored in the registry provided by the ebXML Registry. To illustrate these concepts consider this familiar metaphor: • An ebXML Registry is like a local library. • The repository is like the bookshelves in the library. • The repository items in the repository are like book on the bookshelves. The repository items can contain any type of electronic content just like the books in the bookshelves can contain any type of information. • The registry is like the card catalog. It is organised for finding things quickly. • A Registry object is like a card in the card catalog. All Registry Objects conform to a standard just like the cards in the card catalog conform to a standard. • Every repository item MUST have a RegistryObject that describes it, just like every book must have a card in the card catalog. To summarise, ebXML Registry stores any type of content as RepositoryItems in a repository and stores standardised metadata describing the content as RegistryObjects in a registry.
Dependencies	
Example of Use Case	

3.2.3.2 HSSP CTS2

Adoption Level		**Maturity**	
Standard Organisation	HSSP / OMG	**Version**	
Description	The goal of the Common Terminology Services 2 (CTS 2) specification stack is to provide a standardised interface for the usage and management of terminologies. Terminologies provide the atomic building blocks of shared semantics, concepts. In a shared semantics environment, CTS2 provides a modular, common and universally deployable set of behaviours which can be used to deal with a set of terminologies chosen by the users of the service in their deployment environment. The service will contribute to interoperability by supporting an easy access to the foundational elements of shared semantics. It will also foster the authoring of high-quality terminologies via its authoring profile. This goal is realised via the expansion of the original functionality outlined in HL7's Common Terminology Service (CTS) Specification. CTS 2 defines the functional requirements of a set of service interfaces to allow the representation, access, and maintenance of terminology content either locally, or across a federation of terminology service nodes. The CTS 2 specification strives to expand on the original functionality outlined in HL7's Common Terminology Service specification, specifically looking to: 1. Establish the minimal common structural model for terminology behaviour independent from any specific terminology implementation or interchange model, and how it is related to metadata (information about data) and data (the information itself) 2. Integrate into CTS 2 the functional coverage outlined in the existing CTS specification. 3. Specify both an information and functional model that addresses the relationships and use of terminology, e.g. how value sets are built and queried, and how terminological information is validated. 4. Specify the interactions between terminology providers and consumers – how terminology users can submit unambiguous requests for corrections and extensions and how revisions to content are identified, distributed and integrated into running systems. 5. Specify how mapping between compatible terminologies and data models is defined, exchanged and revised. 6. Specify how logic-based terminologies can be queried about subsumption and inferred relationships. 7. Engage broad community participation to describe the dimensions of use and purpose for vocabularies and value sets. This aim will attempt to harmonise these efforts in terms of models, use cases, and requirements for creating a functional model for CTS 2.		

Dependencies	
Example of Use Case	

3.2.3.3 GS1 Healthcare

Adoption Level		**Maturity**	
Standard Organisation	GS1	**Version**	
Description	GS1 standards provide a much wider framework for supply chain visibility. The current architecture of GS1 standards is as follows: • Identify: Standards for the identification of items, locations, shipments, assets, etc.. and associated data • Capture: Standards for encoding and capturing data in physical data carriers such as barcodes and RFID tags • Share: Standards for sharing data between parties GS1 identification standards do not provide identification of country of origin for a given product. Member companies may manufacture products anywhere in the world.		
Dependencies			
Example of Use Case			
Comments	This version is a specific version focused in Healthcare based on the same standards from GS1 for the retail sector. Widely used.		

3.2.3.4 OID

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	
Description	An object identifier or OID is an identifier used to name an object. Structurally, an OID consists of a node in a hierarchically-assigned namespace, formally defined using the ITU-T's ASN.1 standard, X.690. Successive numbers of the nodes, starting at the root of the tree, identify each node in the tree. Designers set up new nodes by registering them under the node's registration authority.		
Dependencies			

Example of Use Case	

3.2.3.5 FHIR

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	
Description	Fast Healthcare Interoperability Resources (FHIR, pronounced "Fire") defines a set of "Resources" that represent granular clinical concepts. The resources can be managed in isolation, or aggregated into complex documents. Technically, FHIR is designed for the web; the resources are based on simple XML or JSON structures, with an http-based RESTful protocol where each resource has predictable URL. Where possible, open internet standards are used for data representation.		
Dependencies	HL7 V3		
Example of Use Case			

3.2.3.6 CEN/ISO EN 13606

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	
Description	The CEN/ISO EN13606 is a European norm from the European Committee for Standardization (CEN) also approved as an international ISO standard. It is designed to achieve semantic interoperability in the electronic health record communication. The overall goal of the CEN/ISO 13606 standard is to define rigorous and stable information architecture for communicating part or all of the electronic health record (EHR) of a single subject of care (patient) between EHR systems, or between EHR systems and a centralized EHR data repository. It may also be used for EHR communication between an EHR system or repository and clinical applications or middleware components (such as decision support components) that need to access or provide EHR data, or as the representation of EHR data within a distributed (federated) record system. To achieve this objective, CEN/ISO 13606 follows an innovative Dual Model architecture. The Dual Model architecture defines a clear separation between information and knowledge. The former is structured through a Reference Model that contains the basic entities for representing any information of the EHR. The latter is based on archetypes, which are formal definitions of clinical concepts, such as discharge report, glucose measurement or family history, in the form of structured and constrained combinations of the entities of a Reference Model. It provides a semantic		

	meaning to a Reference Model structure. The interaction of the Reference Model (to store data) and the Archetype Model (to semantically describe those data structures) provides an unseen capability of evolution to the information systems. Knowledge (archetypes) will change in the future, but data will remain untouched.
Dependencies	
Example of Use Case	

3.2.3.7 OpenEHR Clinical Models

Adoption Level		**Maturity**	
Standard Organisation	OpenEHR	**Version**	
Description	The foundations of openEHR are the clinical models, consisting of archetypes and templates. These models require terminology and finally the models need to support automated clinical process, offering the clinician users decision support and suggesting quality care options in the form of computerised clinical pathways. Models of clinical information exist in every computer system that is used in health care. While doctors, nurses and other health professionals share many clinical concepts and can communicate very effectively about these concepts, computers have not had a standard means of representing clinical information. openEHR offers this capability and in doing so provides a platform for health care computing. If we do not have such a platform then the benefits of computing in health care will be very slow coming and require absolutely massive investment. • Archetypes: Archetypes are the fundamental shareable specifications of clinical information to provide quality health care, and have been formally accepted as a European standard in 2007 (CEN 13606 Part II). Each archetype represents a whole, discrete specification which is as inclusive as possible, always in terms of the openEHR reference model. The reference model itself guarantees that the key attributes for information in health records (such as who, when and where) are already taken care of and do not need to be addressed in each archetype. • Templates: Templates are a further means of building clinical models; these are composed of one or more archetypes and add further constraints required for the use of those archetypes in a particular setting. Thus, archetypes for blood pressure, weight and blood sugar may be used when recording an annual review of a diabetic person or in an antenatal visit by a pregnant woman. That is to say, templates will be created that are specific to 'diabetic review' and 'antenatal visit'.		

Dependencies	
Example of Use Case	
Comments	**This is a proprietary standard as it does not have a CEN/ISO EN imprimatur.**

3.2.3.8 HL7 v3 Data Types

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	3
Description	The HL7 V3 Data Types specification is one of the more stable and robust parts of the HL7 V3 standard. For anyone tasked with implementing and supporting HL7 V3 messaging, or CDA Release 2 document creation or processing, it will be quite useful to have a single common reusable implementation of the HL7 V3 data types. The abstract implementation describes the relationships among the various data types. The HL7 V3 data types have rich semantics and this result in a quite complicated schema, and also in a complex object-oriented implementation. Every data element has a data type. Data types define the meaning (semantics) of data values that can be assigned to a data element. Meaningful exchange of data requires that we know the definition of values so exchanged. This is true for complex "values" such as business messages as well as for simpler values such as character strings or integer numbers. According to ISO 11404, a data type is "a set of distinct values, characterized by properties of those values and by operations on those values." A data type has intension and extension. Intentionally, the data type defines the properties exposed by every data value of that type. Extensionally, data types have a set of data values that are of that type (the type's "value set"). Semantic properties of data types are what ISO 11404 calls "properties of those values and [...] operations on those values." A semantic property of a data type is referred to by a name and has a value for each data value. The value of a data value's property must itself be a value defined by a data type - no data value exists that would not be defined by a data type. Data types are thus the basic building blocks used to construct any higher order meaning: messages, computerized patient record documents, or business objects and their transactions. Data type values stand for themselves, the value is all that counts, neither identity nor state or changing of state is defined for a data value.		
Dependencies			

Example of Use Case	

3.2.3.9 ISO 21090 Harmonized data types for information interchange

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2011
Description	It provides a set of datatype definitions for representing and exchanging basic concepts that are commonly encountered in healthcare environments in support of information exchange in the healthcare environment. It specifies a collection of healthcare-related datatypes suitable for use in a number of health-related information environments. It declares the semantics of these datatypes using the terminology, notations and datatypes defined in ISO/IEC 11404, thus extending the set of datatypes defined in that standard. It provides UML definitions of the same datatypes using the terminology, notation and types defined in Unified Modelling Language (UML) version 2.0; It specifies an XML (Extensible Mark-up Language) based representation of the datatypes. It can offer a practical and useful contribution to the internal design of health information systems, but is primarily intended to be used when defining external interfaces or messages to support communication between them.		
Dependencies			
Example of Use Case			

3.2.3.10 ISO/IEC 11404 General-Purpose Datatypes

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2007
Description	SO/IEC 11404:2007 specifies the nomenclature and shared semantics for a collection of datatypes commonly occurring in programming languages and software interfaces, referred to as the General-Purpose Datatypes (GPD). It specifies both primitive datatypes, in the sense of being defined ab initio without reference to other datatypes, and non-primitive datatypes, in the sense of being wholly or partly defined in terms of other datatypes. The specification of datatypes in ISO/IEC 11404:2007 is "general-purpose" in the sense that the datatypes specified are classes of datatype of which the		

	actual datatypes used in programming languages and other entities requiring the concept "datatype" are particular instances. These datatypes are general in nature; thus, they serve a wide variety of information processing applications.
Dependencies	
Example of Use Case	

3.2.3.11 ISO/TS 22220 Health informatics -- Identification of subjects of health care

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2011
Description	ISO/TS 22220:2011 indicates the data elements and structure suited to accurate and procedurally appropriate and sensitive identification of individuals in health care in a face-to-face setting supported by computer technology, or through interactions between computer systems. It provides guidelines for improving the positive identification of subjects of care within and between health care organizations. ISO/TS 22220:2011 defines demographic and other identifying data elements suited to capturing subject of care identification in health care settings, and the wide variety of manual and computer enhanced procedures used for this process. It provides guidance on the application of these procedures in the manual and the computer environment and makes recommendations about the nature and form of health care identifiers, the management organization to oversee subject of care identification and computer support to be provided for the identification process.		
Dependencies			
Example of Use Case			

3.3 Semantic Standards

Semantics hold the meaning of a communication, the equivalent of a dictionary or thesaurus. Terminologies such as SNOMED and LOINC and content "payload" standards such as the HL7 Clinical Document Architecture (CDA) when communicating coded structured data are examples of semantic standards.

Semantic interoperability is the way in which, once data has been collected, information can be meaningfully interpreted and incorporated into the receiving system. In order to achieve this type of interoperability for any aspect of the healthcare record, it needs to use the same vocabulary. It is necessary to design vocabulary control strategies so that the clinical information stored in health information systems can be shared, either for administrative purposes or in making clinical decisions (perhaps incorporating the use of automated decision---support tools) in ways that maximise the quality and safety of patient care. Without semantic interoperability, data can be interchanged but there is no certainty that they can be used or understood by the person receiving them. Coded structured data is also needed to accurately collect and analyse population data for public health research and reporting.

3.3.1 Terminologies / Classifications

These vocabularies provide specific codes for clinical concepts such as diseases, problem lists, allergies, medications, and diagnoses, any of which could have variants in the paper record or transcription. Examples of terminology standards are LOINC for lab results, SNOMED for clinical terms, and ICD for medical diagnosis.

3.3.1.1 **Terminologies**

3.3.1.1.1 SNOMED CT			
Adoption Level		**Maturity**	
Standard Organisation	IHTSDO	**Version**	
Description	SNOMED CT is a comprehensive and precise clinical health terminology, owned and distributed around the world by The International Health Terminology Standards Development Organisation (IHTSDO). • Is a resource with comprehensive, scientifically validated clinical content. • Enables consistent, processable representation of clinical content in electronic health records. • Is mapped to other international standards. • Is already used in more than fifty countries. When implemented in software applications, SNOMED CT can be used to represent clinically relevant information consistently, reliably and comprehensively as an integral part of producing electronic health information. SNOMED CT supports the development of comprehensive high-quality clinical content in health records. It provides a standardised way to represent clinical phrases captured by the clinician and enables automatic interpretation of these. SNOMED CT is a clinically validated, semantically rich, controlled vocabulary that facilitates evolutionary growth in expressivity to meet emerging requirements. SNOMED CT based clinical information benefits individual		

	patients and clinicians as well as populations and it supports evidence based care.
Dependencies	
Example of Use Case	

3.3.1.1.2 LOINC

Adoption Level		**Maturity**	
Standard Organisation	Regenstrief	**Version**	
Description	The LOINC effort is housed in the Regenstrief Institute, an internationally respected non-profit medical research organisation associated with Indiana University. LOINC was initiated in 1994 by the Regenstrief Institute and developed by Regenstrief and the LOINC committee as a response to the demand for electronic movement of clinical data from laboratories that produce the data to hospitals, physician's offices, and payers who use the data for clinical care and management purposes. The purpose of the LOINC database is to facilitate the exchange and pooling of results for clinical care, outcomes management, and research. Currently, most laboratories and clinical services use HL7 to send their results electronically from their reporting systems to their care systems. However, the tests in these messages are identified by means of their internal, idiosyncratic code values. Thus, the care system cannot fully "understand" and properly file the results they receive unless they either adopt the producer's laboratory codes (which is impossible if they receive results from multiple sources), or invest in the work to map each result producer's code system to their internal code system. LOINC codes are universal identifiers for laboratory and other clinical observations that solve this problem. The scope of the LOINC effort includes laboratory and other clinical observations. The laboratory portion of the LOINC database contains the usual categories of chemistry, hematology, serology, microbiology (including parasitology and virology), toxicology; as well as categories for drugs and the cell counts, antibiotic susceptibilities, and more. The clinical portion of the LOINC database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments (e.g. Glasgow Coma Score, PHQ-9 depression scale, CMS-required patient assessment instruments), and other clinical observations.		
Dependencies			
Example of Use Case			

3.3.1.1.3 ISO/TS 14265			
Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	
Description	ISO/TS 14265:2011 defines a set of high-level categories of purposes for which personal health information can be processed. This is in order to provide a framework for classifying the various specific purposes that can be defined and used by individual policy domains (e.g. healthcare organisations, regional health authorities, jurisdictions, countries) as an aid to the consistent management of information in the delivery of health care services and for the communication of electronic health records across organisational and jurisdictional boundaries. The scope of application of ISO/TS 14265:2011 is limited to Personal Health Information as defined in ISO 27799, information about an identifiable person that relates to the physical or mental health of the individual, or to provision of health services to the individual.		
Dependencies	ISO 27799		
Example of Use Case			

3.3.1.1.4 ISO/TS 21298			
Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	
Description	ISO/TS 21298:2008 defines a model for expressing functional and structural roles and populates it with a basic set of roles for international use in health applications. Roles are generally assigned to entities that are actors. This will focus on roles of persons (e.g. the roles of health professionals) and their roles in the context of the provision of care (e.g. subject of care). Roles addressed in ISO/TS 21298:2008 are not restricted to privilege management purposes, though privilege management and access control is one of the applications of this Technical Specification. ISO/TS 21298:2008 does not address specifications related to permissions. This Technical Specification treats the role and the permission as separate constructs. Further details regarding the relationship with permissions, policy and access control are provided in ISO/TS 22600-1.		
Dependencies			

Example of Use Case	

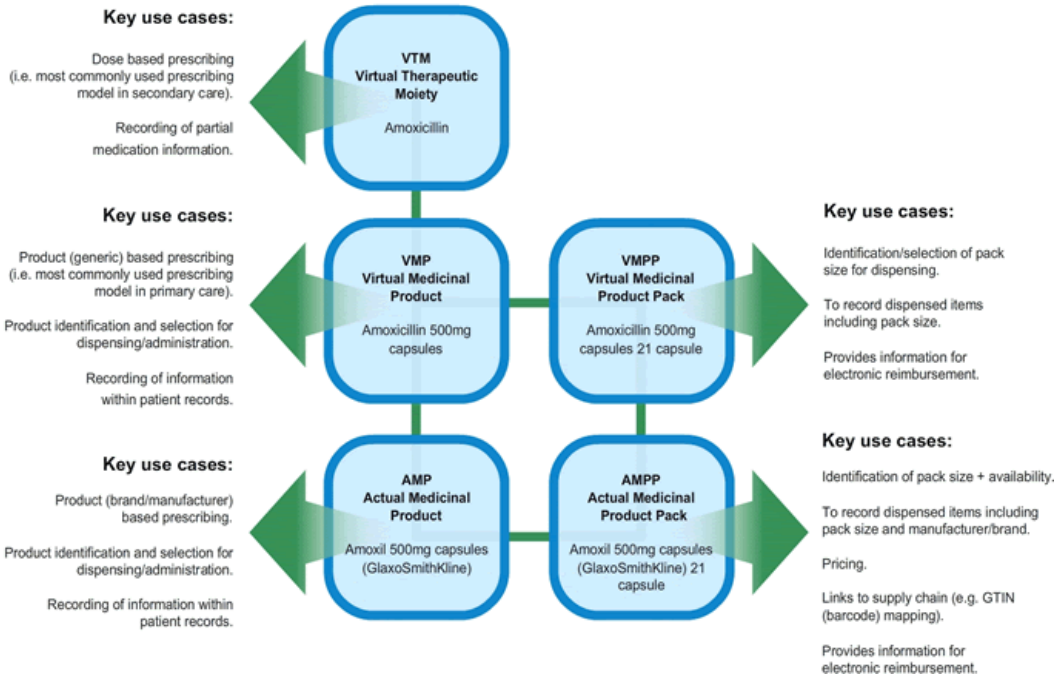
3.3.1.1.5 ASTM E1986 - 09(2013)

Adoption Level		**Maturity**	
Standard Organisation	ASTM	**Version**	
Description	ASTM E1986: Standard Guide for Information Access Privileges to Health Information covers the process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organisational data in the healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.		
Dependencies			
Example of Use Case			

3.3.1.1.6 PCD-RTM – Rosseta Terminology Mapping

Adoption Level		**Maturity**	
Standard Organisation	IHE	**Version**	
Description	The primary purpose of the Rosetta Terminology Mapping (RTM) profile is to harmonise the use of existing ISO/IEEE 11073-10101 nomenclature terms by systems compliant with IHE PCD profiles. The RTM profile also specifies the correct units-of-measure and enumerated values permitted for each numeric parameter to facilitate safe and interoperable communication between devices and systems. The Rosetta Table also is designed to serve as a temporary repository that can be used to define new nomenclature terms that are currently not present in the ISO/IEEE 11073-10101 nomenclature. This could also serve as a framework for adding and reconciling new terms to support the IEEE 11073 'Personal Health Devices' initiative.		
Dependencies			
Example of Use Case			

3.3.1.1.7 Dm+d

Adoption Level		**Maturity**	
Standard Organisation	NHS	**Version**	
Description	dm+d is a NHS dictionary containing unique identifiers (codes) and associated textual descriptions for representing medicines and medical devices in information systems and electronic communications. It has been developed for use throughout the NHS as a means of uniquely identifying the specific medicines and medical devices used in the diagnosis or treatment of patients. dm+d has five basic components. Each component (represented as a box in the picture below) describes a product at different levels of granularity to support various use cases and this makes up the dm+d model. **dm+d data model** 
Dependencies			
Example of Use Case	Prescription, Reimbursement		

3.3.1.1.8 SNOMED CT UK Drug Extension

Adoption Level		**Maturity**	
Standard Organisation	NHS	**Version**	
Description	At its simplest SNOMED CT is a three table terminology (Concepts, Descriptions and Relationships) designed to comply with all the principles of good terminology practice; at its simplest dm+d is a nine table dictionary designed to support the business processes of the NHS and comply with good vocabulary practice wherever possible. Translating components of dm+d into SNOMED CT format to produce content for the SNOMED CT UK Drug Extension involves representing these nine tables in the three table SNOMED CT format. Conversion of dm+d information to form part of the SNOMED CT Drug Extension means addition of the following to the original data: • Fully Specified Name (to follow SNOMED CT naming convention) and UK preferred term for each concept • A valid SNOMED CT Description Id for each description (e.g. FSN, PreferredTerm etc) associated with a dm+d concept • Relationships to SNOMED CT International Release. Each dm+d concept will have a SNOMED CT defined relationship either to an appropriate supertype concept in the SNOMED CT International Release or to another dm+d concept that is itself linked (directly or indirectly) to a SNOMED CT International Release concept. • Inherited defining relationships (where appropriate) • Specific defining relationships. Relationships to other SNOMED CT International Release defined concepts. • Historical relationships.		
Dependencies			
Example of Use Case	Prescription		

3.3.1.2 Classifications

3.3.1.2.1 ICPC-2

Adoption Level		**Maturity**	
Standard Organisation	WONCA International Classification Committee	**Version**	
Description	The International Classification of Primary Care (ICPC) is a classification method for primary care encounters. It allows for the classification of the patient's reason for encounter (RFE), the problems/diagnosis managed, primary or general health care interventions, and the ordering of the data of the primary care session in an episode of care structure. It was developed by the WONCA International Classification Committee (WICC), and was first published in 1987 by Oxford University Press (OUP). A revision and inclusion of criteria and definitions was published in 1998. The second revision was accepted within the World Health Organisation's (WHO) Family of International Classifications. The classification was developed in a context of increasing demand for quality information on primary care as part of growing worldwide attention to global primary health care objectives, including the WHO's target of "health for all".		
Dependencies			
Example of Use Case			

3.3.1.2.2 ICD-10

Adoption Level		**Maturity**	
Standard Organisation	World Health Organisation's	**Version**	10
Description	The International Classification of Diseases (ICD) is the standard diagnostic tool for epidemiology, health management and clinical purposes. This includes the analysis of the general health situation of population groups. It is used to monitor the incidence and prevalence of diseases and other health problems, proving a picture of the general health situation of countries and populations. ICD is used by physicians, nurses, other providers, researchers, health information managers and coders, health information technology workers, policy-makers, insurers and patient organisations to classify diseases and other health problems recorded on many types of health and vital records, including death certificates and health records. In addition to enabling the storage and retrieval of diagnostic information for clinical, epidemiological and quality purposes, these records also provide the basis for the compilation of national mortality and morbidity statistics by WHO Member States.		

	Finally, ICD is used for reimbursement and resource allocation decision-making by countries. All Member States use the ICD which has been translated into 43 languages. Most countries (117) use the system to report mortality data, a primary indicator of health status.
Dependencies	
Example of Use Case	

3.3.1.2.3 ICD-10-AM

Adoption Level		**Maturity**	
Standard Organisation	World Health Organisation's and customised by ACCD/NCCH	**Version**	10
Description	ICD-10-AM is the International Statistical Classification of Diseases and Related Health Problems, Tenth Revision, Australian Modification. It consists of a tabular list of diseases and accompanying index. ICD-10-AM was developed by the National Centre for Classification in Health and has been in use since 1998. It was developed with assistance from clinicians and clinical coders to ensure that the classification is current and appropriate for Australian clinical practice. ICD-10-AM is a derived version of the World Health Organisation (WHO) ICD-10. It uses an alphanumeric coding scheme for diseases and external causes of injury. It is structured by body system and aetiology, and comprises three, four and five character categories. ICD-10-AM is updated on a regular basis, with the regular updates of ICD-10 being included as part of the updating process.		
Dependencies			
Example of Use Case			

3.3.1.2.4 OPCS-4

Adoption Level		**Maturity**	
Standard Organisation	NHS Connecting for Health	**Version**	
Description	OPCS-4 is the fourth revision of the classification devised for translating or classifying all operations and surgical procedures that may be carried out on a patient during an episode of health care." NHS Connecting for Health has responsibility for OPCS-4 codes.		

Dependencies	
Example of Use Case	

3.3.1.2.5 MEDDEV

Adoption Level		**Maturity**	
Standard Organisation	Europa Public Health	**Version**	2.4 Classification 2.1 Guidelines
Description	MEDDEV is a set of guidelines relating to questions of application of EU Directives on medical devices. They are not legally binding. Only the European Court of Justice can give an authoritative interpretation of Community Law. Contains guidance for the application of the classification rules for medical devices as set out in Annex IX of Directive 93/42/EEC1, as amended. It is for the national Competent Authorities and national Courts to take legally binding decisions on a case-by-case basis.		
Dependencies	MEDDEV Additional guidelines like the guideline for “Active Implantable and general medical devices”		
Example of Use Case			

3.3.1.2.6 RxNorm

Adoption Level		**Maturity**	
Standard Organisation	U.S. National Library or Medicine	**Version**	
Description	RxNorm provides normalised names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software, including those of First Databank, Micromedex, MediSpan, Gold Standard Drug Database, and Multum. By providing links between these vocabularies, RxNorm can mediate messages between systems not using the same software and vocabulary.		
Dependencies			
Example of Use Case			

3.3.2 Semantic Standards

3.3.2.1 HL7 Version 3 Clinical Document Architecture or CDA v2

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	2 -> 3 in development
Description	The HL7 Version 3 Clinical Document Architecture (CDA®) is a document markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients. It defines a clinical document as having the following six characteristics: 1) Persistence, 2) Stewardship, 3) Potential for authentication, 4) Context, 5) Wholeness 6) Human readability. CDA is an XML-based, electronic standard used for clinical document exchange. CDA conforms to the HL7 V3 Implementation Technology Specification (ITS), is based on the HL7 Reference Information Model (RIM), and uses HL7 V3 data types. It was known earlier as the Patient Record Architecture (PRA). CDA is a flexible standard and is unique in that it can be read by the human eye or processed by a machine. This is due to its use of XML language, which also allows the standard to be broken into two different parts. A mandatory free-form portion enables human interpretation of the document, while an optional structured part enables electronic processing (like with an EMR system). Text, images and even multimedia can be included in the document. A CDA can contain any type of clinical content -- typical CDA documents would be a Discharge Summary, Imaging Report, Admission & Physical, Pathology Report and more. The most popular use is for inter-enterprise information exchange. A CDA document could be, for example, any of the following: discharge summary, referral, clinical summary, history/physical examination, diagnostic report, prescription, or public health report. In short, any document that might have a signature is a viable document for CDA.		
Dependencies	HL7 v3 data types		
Example of Use Case	Referral, Discharge between many others		

3.3.2.2 OASIS-XSPA

Adoption Level		**Maturity**	
Standard Organisation	OASIS	**Version**	
Description	The XSPA profile of WS-Trust provides cross-enterprise authorisation of entities within and between healthcare information technology (IT) systems by providing common semantics and vocabularies for interoperable coarse and fine-grained access control.		
Dependencies			
Example of Use Case			

3.3.2.3 BPMN

Adoption Level		**Maturity**	
Standard Organisation	OMG	**Version**	2.0
Description	A standard Business Process Model and Notation (BPMN) will provide businesses with the capability of understanding their internal business procedures in a graphical notation and will give organisations the ability to communicate these procedures in a standard manner. Furthermore, the graphical notation will facilitate the understanding of the performance collaborations and business transactions between the organisations. This will ensure that businesses will understand themselves and participants in their business and will enable organisations to adjust to new internal and B2B business circumstances quickly.		
Dependencies			
Example of Use Case	Operational workflow		

3.4 Security Standards

Security and privacy application standards determine the way business rules are implemented and how users interact with software systems. These standards will help to keep patient medical information secure in an electronic environment. They will also help to assure that this information will only be used by authorised personnel for official purposes

3.4.1.1.1 VPN - IPSec (RFC 4301)			
Adoption Level		**Maturity**	
Standard Organisation	IETF	**Version**	
Description	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer.		
Dependencies			
Example of Use Case			

3.4.1.1.2 TLS (RFC 5246)			
Adoption Level		**Maturity**	
Standard Organisation	IETF	**Version**	1.2
Description	The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP [TCP]),		

	is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties: • The connection is private. Symmetric cryptography is used for data encryption (e.g., AES [AES], RC4 [SCH], etc.). The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption. • The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA-1, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters. The TLS Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the TLS Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties: • The peer's identity can be authenticated using asymmetric or public key, cryptography (e.g., RSA [RSA], DSA [DSS], etc.). This authentication can be made optional, but is generally required for at least one of the peers. • The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection. • The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication. One advantage of TLS is that it is application protocol independent. Higher-level protocols can layer on top of the TLS protocol transparently. The TLS standard, however, does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left to the judgment of the designers and implementors of protocols that run on top of TLS.
Dependencies	
Example of Use Case	

3.4.1.1.3 ITU-T X.509 / ISO/IEC 9594-8

Adoption Level		**Maturity**	
Standard Organisation	ITU-T / ISO	**Version**	
Description	Recommendation ITU-T X.509 | ISO/IEC 9594-8 defines frameworks for public-key certificates and attribute certificates. The public-key certificate framework is the base specification for public-key certificates, for the different components going into a public-key infrastructure (PKI) for validation procedures and for public-key certificate revocation, etc. The attribute certificate framework is the base specification for attribute certificates and the different components going into the Privilege Management Infrastructure (PMI). These frameworks may be used by standards bodies to profile their application to PKIs and PMIs.		
Dependencies			
Example of Use Case			

3.4.1.1.4 ETSI TS 103 231

Adoption Level		**Maturity**	
Standard Organisation	ETSI	**Version**	3.2
Description	The purpose of a Trust-service Status List (TSL), and hence of this standard, is to provide a harmonised way in which assessment schemes having an oversight role with regards to trust services and their providers (trust service providers - TSPs) can publish information about the services and TSPs which they currently oversee, or indeed (through the provision of historical information) have overseen. An assessment scheme operator may also use the TSL to only refer to other assessment schemes, in which case the services of these assessment scheme operators are considered as a specific type of trust service. The present standard is based upon the reasoning that it will enhance the confidence of parties relying on certificates or other services related to electronic signatures if they had access to information that would allow them to know whether a given TSP was operating under the approval of any recognised scheme at the time of providing their services and of any dependent transaction that took place. The assurance provided by information available within a TSL is intended to serve as a secondary source of trust, rather than a primary source of trust which might be derived by parsing a certificate chain. The present standard is not intended to be a replacement for certificate chains and the assurance which may be obtained from parsing them to establish the validity of certificates (or other forms of trust service tokens) associated with providers of trust		

	services of any kind. The information should be available for a wide range of services and schemes, including the use of Qualified Certificates. The importance of this information is especially significant for cross-domain and international transactions. This information should preferably be accessible using an on-line protocol, although accessibility both off-line and on-line should be possible. Entities having such an oversight role could be supervisory systems or voluntary approval schemes as defined in Directive 1999/93/EC [1] (see note), similar schemes established by other sovereign states or economies (e.g. certain government e-authentication frameworks), and those established by specific industry sectors or for international promotion of trust services. • *NOTE: This refers in particular to the Trusted Lists to be established, published and maintained by every European Union Member State and that consist in the Member State's "Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC". Those Trusted Lists (one single list per Member State) will comply with the present standard requirements while making use of the URIs and extensions described in annex L.*
Dependencies	
Example of Use Case	

3.4.1.1.5 S/MIME			
Adoption Level		**Maturity**	
Standard Organisation	IETF	**Version**	3
Description	S/MIME (Secure/Multipurpose Internet Mail Extensions), provides a method to send and receive secure MIME messages. Before using a public key to provide security services, the S/MIME agent must certify that the public key is valid. S/MIME agents MUST use PKIX certificates to validate public keys as described in the Internet X.509 Public Key Infrastructure (PKIX) Certificate and CRL Profile , S/MIME agents must meet the certificate processing.		
Dependencies	MIME		
Example of Use Case	Send medical information through email		

3.5 Business Standards

There is a set of standards which are related to general health information management, these have been defined as business standards. In order to support this need, some SDOs have defined standards specifically focused on the business viewpoint. Most of the standards below come from the ISO standards categorised as “Health informatics”.

3.5.1.1 ISO/TR 13054 Knowledge management of health information standards

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2012
Description	ISO/TR 13054:2012 describes a standards knowledge management (SKM) methodology and metadata to support the easy identification of the existence of a health informatics standard, its developmental status, and it's associated Standards Development Organization (SDO). In particular, it describes a knowledge-based navigation methodology to enable rapid appreciation of the contextual roles and purposes of a standard, including the relationship between one standard and others, particularly in the same standards domain. ISO/TR 13054:2012 also gives information about the design of tools to support knowledge management of health informatics standards.		
Dependencies			
Example of Use Case			

3.5.1.2 ISO/DIS 13940 Health informatics -- System of concepts to support continuity of care

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	Under development
Description	This standard is currently under development and will standardise the concepts used for systems providing continuity of care.		
Dependencies			
Example of Use Case			

3.5.1.3 ISO/TS 27527 Health informatics -- Provider identification

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2010
Description	ISO/TS 27527:2010 provides a framework for improving the positive identification of providers. Identification of "providers" encompasses individuals and organizations. ISO/TS 27527:2010 includes data elements needed for identification of individual providers (i.e. individuals) and data elements needed for the identification of organization providers (i.e. organizations). "Identification" in ISO/TS 27527:2010 refers		

	both to the process of being able to identify individuals and organizations, and the data elements required to support that identification manually and from a computer processing perspective. ISO/TS 27527:2010 can be applied to all providers of services, individuals and organizations. It details both data and processes for collection and application of identifying information for providers. It defines demographic and other identifying data elements suited to capture and use for the identification of providers in health care settings and provides guidance on their application.
Dependencies	
Example of Use Case	

3.5.1.4 ISO EN 12967 Health Informatics Service Architecture HISA

Adoption Level		**Maturity**	
Standard Organisation	ISO	**Version**	2009
Description	ISO 12967-1:2009 provides guidance for the description, planning and development of new systems, as well as for the integration of existing information systems, both within one enterprise and across different healthcare organizations, through an architecture integrating the common data and business logic into a specific architectural layer (i.e. the middleware), distinct from individual applications and accessible throughout the whole information system through services.		
Dependencies			
Example of Use Case			

3.5.1.5 HL7 EHR-System Functional Model

Adoption Level		**Maturity**	
Standard Organisation	HL7	**Version**	Release 2
Description	The HL7 EHR-S Functional Model defines a standardized model of the functions that may be present in EHR Systems. From the outset, a clear distinction between the EHR as a singular entity and systems that operate on the EHR. This includes “core” healthcare functionality, typically provided by healthcare-specific applications that manage electronic healthcare information. It also includes associated generic application-level capabilities that are typically provided by middleware or other		

	infrastructure components. Also includes interoperability and integration capabilities such as location discovery and such areas as cross application workflow. Interoperability is considered both from semantic (clear, consistent and persistent communication of meaning) and technical (format, syntax and physical connectivity) viewpoints. This standard makes no distinction regarding implementation - the EHR-S described in a Functional Profile may be a single system or a system of systems. This Functional Model is not: • a messaging specification • an implementation specification • a conformance specification • an EHR specification • a conformance or conformance testing metric • an exercise in creating a definition for an EHR or EHR-S
Dependencies	ISO/DIS 13940 Health informatics -- System of concepts to support continuity of care
Example of Use Case	EHR
Comments	The EHR-S Functional Model is not sufficient to provide a longitudinal health record; however, it will contribute to its development.

3.6 Accessibility Standards

Accessibility standards and guidelines provide guidance and direction to enable systems to be used by users with various forms of disability. These standards facilitate the use of assistive technologies to enable users to interact with IT systems.

3.6.1.1 Irish National IT Accessibility Guidelines

Adoption Level		**Maturity**	
Standard Organisation	Irish National Disability Authority	**Version**	
Description	The primary national guidelines are the Irish National Disability Authority guidelines. These provide guidelines for accessible products and services, including: • Descriptions of high level accessibility goals and the difficulties faced by users • Prioritised guidelines for each technology • Motivation and justification for each guideline • Guidance on design techniques and testing methods		

Dependencies	
Example of Use Case	
Comments	

3.6.1.2 Web Content Accessibility Guidelines

Adoption Level		**Maturity**	
Standard Organisation	World Wide Web Consortium (W3C)	**Version**	2.0
Description	The Web Content Accessibility Guidelines (WCAG) are produced by the World Wide Web Consortium (W3C). WCAG 2.0 is a stable, referenceable technical standard. It has 12 guidelines that are organized under 4 principles: perceivable, operable, understandable, and robust. For each guideline, there are testable success criteria, which are at three levels: A, AA, and AAA. Web Content Accessibility Guidelines (WCAG) is developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of proving a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.		
Dependencies			
Example of Use Case	All browser based access to HSE Systems		
Comments			

4 Policies and Procedures

This section describes the roles, policies and procedures that govern the use and maintenance of the standards catalogue. This section covers two main procedures:

- *Manage a procurement process*: How the application classification model and the associated standards catalogue are used to support the specification of systems in a procurement process.

- *Update the classification:* How to maintain the standards catalogue as health technology, standards and vendors change the Health IT landscape over time.

4.1 Standards Management Process Roles & Responsibilities

4.1.1 Standards Owner

The standards owner is the person or team that has responsibility for the maintenance, management, update and access control of this document. This role is central to identifying which standards are applicable to a new asset that is being procured and must support and align with the owner of the asset classification model to provide a uniform experience for the final user.

4.1.2 Subject Matter Expert

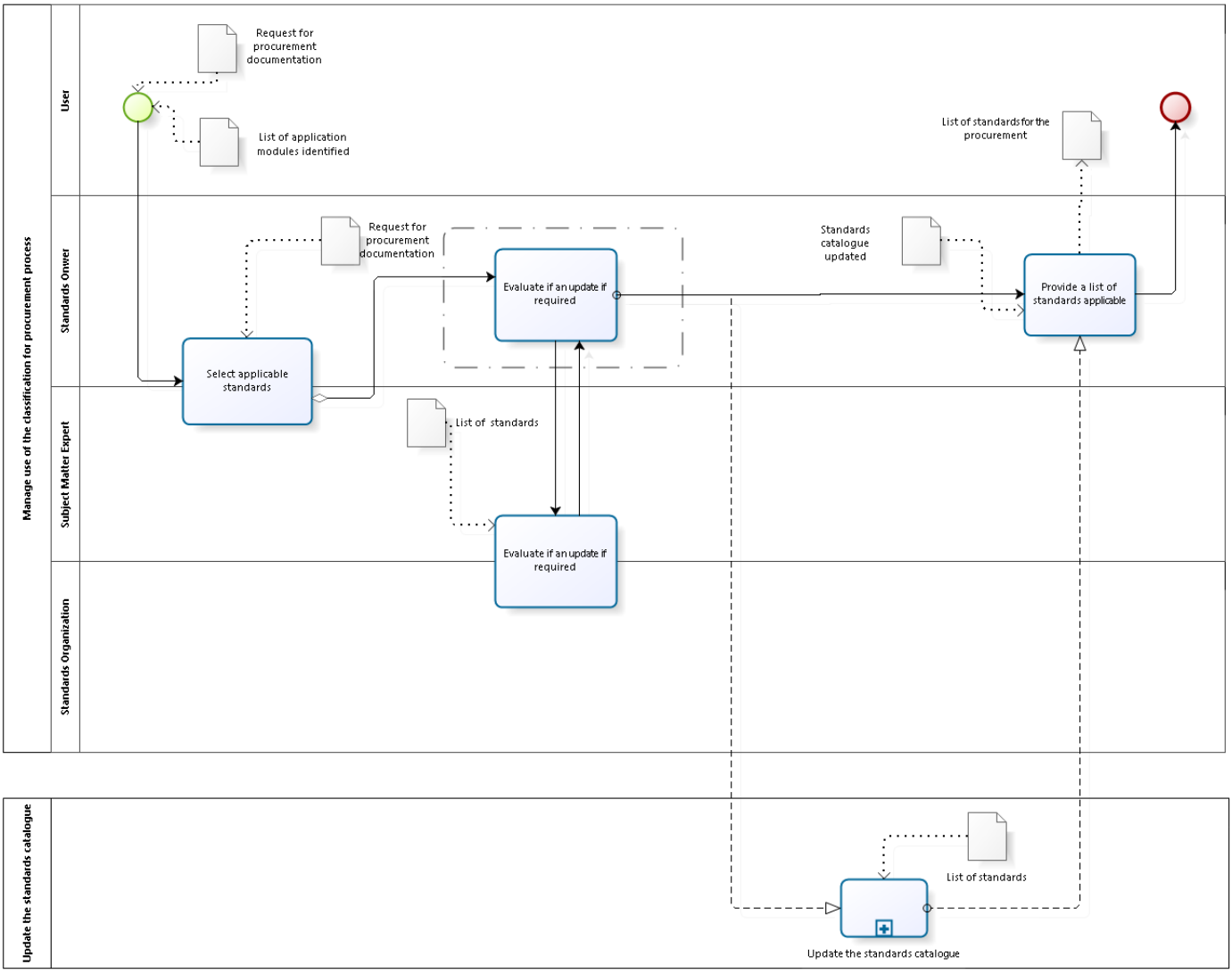
This role identifies the person(s) that have the knowledge of the detailed subject matter area and associated standards (e.g. HL7). It is their responsibility to provide authoritative knowledge and support regarding all decisions related to the assets within their subject area. Their duties do not include any management or maintenance of this document.

4.1.3 Standards Organisation

The relevant standards organisation will be consulted regarding which standards need to be included in the standards catalogue. Usually the changes promoted by this role are related to a national/European requirement or by changes in the applicable legislation.

4.2 Manage use of standards for a procurement process

This process involves the selection of the standards applicable to an assets or a business capability that need to be included in procurement requirements. The main purpose of this process is to establish a framework which will constrain procurements by a set of common standards (ensuring interoperability) and to define a uniform landscape for technical and application architecture.



A detailed description of the activities in the above diagram, along with inputs, outputs and roles involved are described in the following table:

Activity Name	Description	Roles involved
Select Applicable Standards • **Input:** Request for a procurement and list of application modules • **Output:** List of applicable standards	This process is triggered by a procurement need, however, the asset classification model process for managing procurement will have been applied before this process commences. In this step the standards owner identifies the standards applicable to the previously identified applications modules. This process produces a list of applicable standards.	• Standards Owner • Subject Matter Expert
Evaluate if an update is required • **Input:** List of applicable standards. • **Output:** No updated required *or* Request to update the standards	This list of applicable standards is reviewed by the relevant standards organisation (e.g. a representative of HIQA) and the SME (Subject Matter Expert). The standards owner will organise and facilitate this step and provide input where necessary. The SME and standards organisation will determine if an update process will be triggered. Usually the standard organisations will	• Standards Owner • Subject Matter Expert • Standards organisation

	determine if there are any new standards under which the organisation must be aligned.	
Update the standards catalogue • **Input:** Request to update the standards • **Output:** List of standards updated	If it was determined that an update to the standards catalogue is required, the process of update is executed. Once completed, a new list with the applicable standards replaces the previous standards catalogue list as the entry point for the next step. The standards owner manages and orchestrates the update process. For more information on this sub process please refer to section **Error! Reference source not found.** where it is escribed in detail.	• Standards Owner • Subject Matter Expert • Standards organisation
Provide a compressive list of standards • **Input:** List of updated standards *or* No updated is required • **Output:** Standards framework for procurement	With the list of standards from the step before, the standards owner will approve the final list and provide the appropriate detail to support the procurement. **The end of the process is this list of applicable standards**.	• Standards Owner

Use case – Applying the Standards Catalogue to support a new procurement

As result of a new procurement process to get a new EHR, a list of applications modules to be covered is identified as a result of applying the Asset Classification Model for a new procurement. This list works as the entry point for the procurement process around the Standards Catalogue and the following steps will occur:

1. *The standards owner reviews the application module list and drafts a list of relevant standards associated with those application modules.*
2. *The Standards Owner, SME and standard organisation review the draft standards list to identify any potential need for updates. A meeting to discuss the conclusions of each party is convened. Here it will be decided whether or not to trigger an update process to the standards catalogue.*

As a result of the above steps a final list of standards is produced and the Standards Owner will provide this list for use in the procurement process.

4.3 Update of the standards catalogue

The process of updating the standards catalogue includes the review of completely new standards, updated versions of current standards already listed in the catalogue and the removal of retired standards.

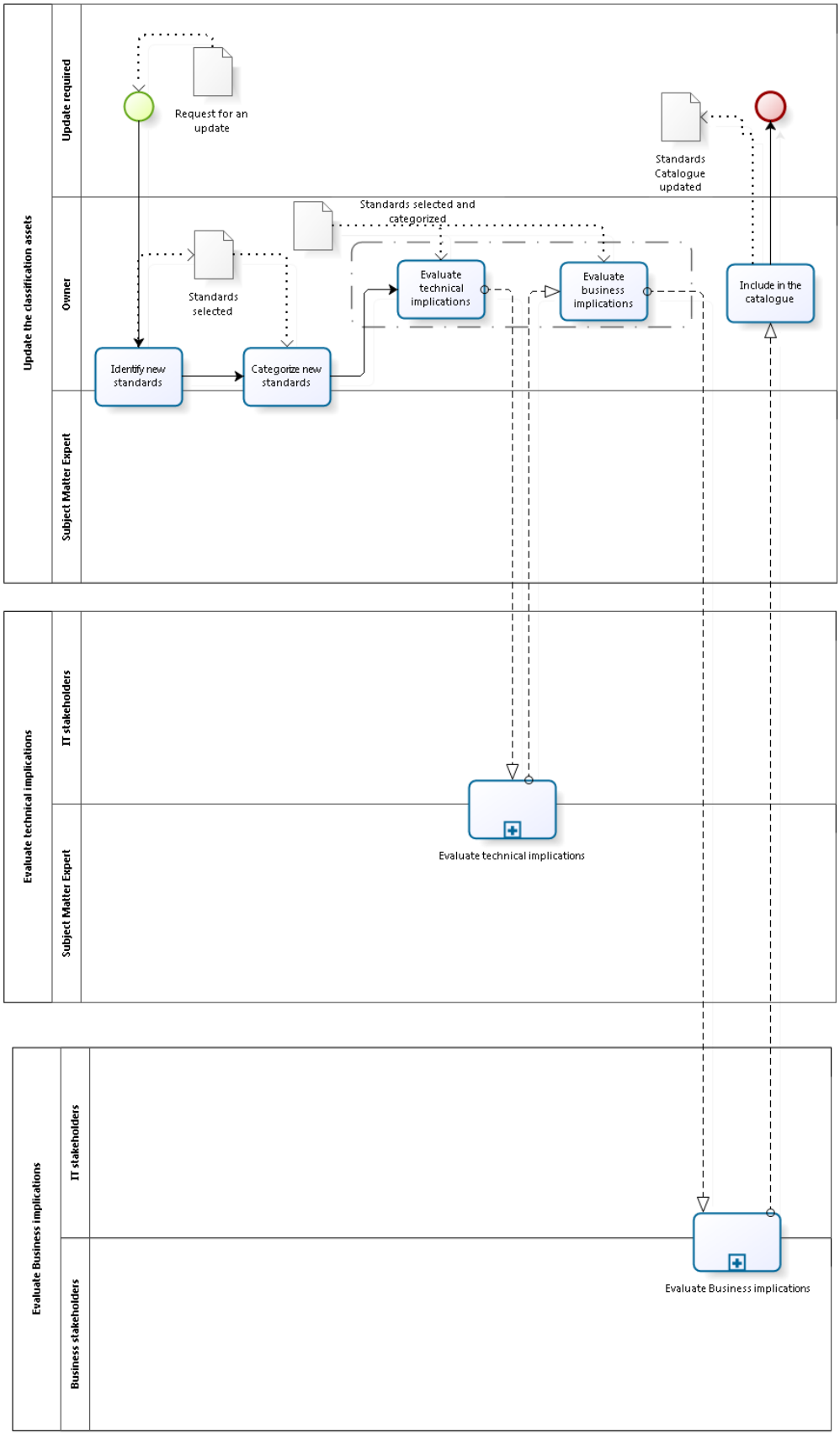
This process is triggered by a request for update as a result of the following two events:

- *Periodic update. In order to maintain the catalogue up to date, the catalogue must be updated two times per year. The aim of the process is to ensure the standards remain relevant, with an emphasis on the IHE profiles standards related to the European SDOs.*

- *Trigger from a procurement process. As result of applying the standards catalogue for a procurement process.*

An update of the standards catalogue usually requires time and analysis of the updates that have to be included. As such both IT and business stakeholders are involved in the update process, and any changes have to be considered from both points of view.
Once an update has been decided on, it is policy to notify the changes to all stakeholders:

- *Each time the catalogue is updated, the changes have to be published and all the known stakeholders must be notified.*



A detailed description of the activities in the above diagram, along with inputs, outputs and roles involved are described in the following table

Activity Name	Description	Roles involved
Identify new standards/new versions • **Input:** Request for update and application module list • **Output:** List of new standards to be considered ***or*** Current Catalogue	A request for update triggers this process. The standards owner, the standard organisation role and SME are responsible for evaluating the entire document and identifying: • New versions • Retired standards • New standards As a result of the evaluation, the standards owner could: • Conclude there is no need for an update; or • Produce a list of the changes to standards identified during this step	• Standards Owner • SME • Standard Organisation
Categorise new standards • **Input:** List of new standards to be considered • **Output:** List of categorise standards	During this step, the standards owner and the SME categorise the new standards to the asset classification model and also the standard categories (e.g.. semantic, syntactic etc.). As result of this step a list the categorised changes are provided as starting point to the next step.	• Standards Owner • SME
Evaluate technical implications • **Input:** List of categorise standards • **Output:** List of changes accepted ***or*** Current Asset Classification	This is a critical step whereby all stakeholders (from local director of IT to the CTO) evaluate the impact of the proposed changes to the standards catalogue (this requires a rigorous review process that covers cost, systems involved, possible outcomes of the changes etc.). The proposed changes can be totally or partially accepted, or all the changes are discarded so the catalogue remains in its current state. During this step the SME, stakeholders and the standards owner will act as the decision makers and refine the list of changes.	• Standards Owner • IT Stakeholders • SME
Evaluate business implications • **Input:** List of changes accepted • **Output:** List of changes accepted ***or*** Current Asset Classification	If it is decided that changes to the standards catalogue can be applied from a technical perspective, the process will continue to evaluate the business implications. The final decision on making the changes has to be taken between the IT stakeholders, the Business stakeholders, the SME and the standards owner. During this step the business stakeholders evaluate the impact of the proposed changes to the standards catalogue (this requires analysis of the business impact, organisational changes, costs, etc.). The proposed changes can be totally or partially accepted, or all the changes are discarded so the catalogue remains in its current state. During this step the SME, stakeholders and the standards owner will act as the decision makers and refine the list of changes.	• Standards Owner • IT Stakeholders • Business Stakeholders • SME
Include in the catalogue • **Input:** List of changes	If at least part of the proposed changes are accepted, the process continues to the final step where the	• Standards Owner

accepted • **Output:** Asset classification updated	standards owner updates the standards catalogue and notifies all stakeholders that a new version is available to be used. From that moment, all systems or business processes have to be modified according to the new version and any new procurement process will use it to define the procurement requirements.	

Use case – Applying the standards catalogue update process

As a consequence of an annual revision of the standards catalogue, HIQA acting as the standard organisation role has identified that a new version of the standard ICD. This has to be used in systems where the newer version (version 11) of the standard applies. This would follow the trend towards wide utilisation of the updated standard in other countries.

The SME categorise the standard under Semantic->Classifications. In a sequence of meetings with different IT stakeholders, the impact of the change from the current version 10 to version 11 is assessed.

They identify the technical impact and in a final meeting, the CTO concludes that the changes only represent an impact to the Terminology and Classification Central Server. As such it is decided to continue the process of including the update in the standards catalogue.

The process continues to the next step where the business stakeholders (with the support of the IT stakeholders, SME and the standards owner) analyse the business impact. After several meetings the CEO concludes that the changes are acceptable from a business point of view, mainly because the new version is backward compatible with the current version and only a couple of minor changes are required to adapt to the new version.

At the end the Standards Owner updates the catalogue and notifies all stakeholders of the availability of the new version.

5 Health Interoperability initiatives

This section covers the health sector interoperability initiatives around the world that are working on the definition and establishment of standards and specifications, as well as promoting eHealth.
This is not an exhaustive list; it only includes the key initiatives thought to be relevant at the time of writing.

5.1 From US

5.1.1 Commonwell health alliance

Commonwell health alliance is committed to supporting interoperability that requires robust privacy and security for all data exchanges through the Alliance services. As such, its services and specifications are designed with privacy as a key consideration.

Services and specifications adopted by CommonWell Health Alliance will strive to improve transparency to enable providers of care and patients to understand permitted uses, access and disclosure of protected health information and to facilitate the identity management in a manner that protects the privacy of the patient.

5.2 From UK

5.2.1 NHS Connecting for Health

NHS Connecting for Health (NHS CFH) is part of the Department of Health Informatics Directorate. Its role is to maintain and develop the NHS national IT infrastructure. This infrastructure includes a number of national services and a range of national applications. To enable a fluent and real interoperability, this initiative defines a set of internal initiatives described in the next subsections.

5.2.1.1 **The Interoperability Toolkit (ITK)**

The ITK is an attempt to try and fill the vacuum by providing a number of specifications and technologies which are consistent and applicable across a wide range of domains and localities.

The Interoperability Toolkit (ITK) is a set of common specifications, frameworks and implementation guides to support interoperability within local organisations and across local health and social care communities.

This initiative provides many benefits:

- Reductions in the NHS expenditure on 'local' system integration projects that are often bespoke ad-hoc integrations by standardising technology and interoperability specifications.
- Reduction in overlap or expenditure from vendors for similar integration across NHS organisations by adopting common standards across the NHS.
- Reduction in time to delivery by reducing the complexities of integration.
- Allows opening up the market to new entrants, niche suppliers and local teams by lowering the entry barrier for new entrants by defining the standard to develop against upfront.
- Allows benefits realised from interoperability to be replicated and scaled up

ITK uses open international standards and is aligned with HL7 and 'Integrating the Healthcare Enterprise' (IHE) and it provides an ITK Accreditation. This means that the system supplier can prove that a product has been developed to and tested against the ITK specifications.

This initiative is internal to NHS and used across UK, but it is not on an international standards track.

5.2.1.2 Spine Services

The Spine is a collection of national applications, services and directories that support the NHS in the exchange of information across national and local NHS systems. The Spine connects clinicians, patients and local service providers throughout England to essential national services, for example, the Electronic Prescription Service, Summary Care Record, Choose and Book and Demographics services.

The Spine provides the infrastructure that enables increased patient safety, improved quality of healthcare, greater clinical effectiveness and better administrative efficiency. It is used and supported 24 hours a day, 365 days a year and is highly resilient.

5.2.1.3 Messaging Implementation Manual

The Messaging Implementation Manual for the HL7v3 messages defined by CFH (NHS Connecting for Health). MIM provides a key enabler of the interoperability inside UK. Details the messaging interfaces for the HL7v3 messages intended for use on the Spine. These messaging specifications are provided as one part of the implementation information required to implement the defined messages.

5.3 From Europe

5.3.1 Antilope

Apart from being a Standards Organisation, Antilope is a European initiative for Health Interoperability and is fully aligned with epSOS.
Since 2013, key national and international organisations have been working together in the framework of the EU-funded Antilope project. They have selected and defined eHealth standards and specifications, created, validated and disseminated a common approach for testing and certification of eHealth solutions and services in Europe.

5.3.2 Expand

The EXPAND project is a Thematic Network funded through the European Competitiveness and Innovation Framework Programme and started on January 1st, 2014. It is intended to be concluded in December 2015.

The initial focus of EXPAND will be to secure the epSOS pilot services or similar services from other mature pilot projects, up to the launch of the Connecting Europe Facility (CEF) and foresee a proper handover to it. EXPAND will operate in the gap between piloting and deployment and aims to secure the sustainability and expandability of the epSOS pilot services.

5.3.3 epSOS

Established in 2008, the European Patient Smart Open Services (epSOS) project is intended to provide cross-border services that ensure safe, secure and efficient medical treatment for citizens when traveling across Europe. Two specific areas were identified: a shared patient summary for EU citizens and an e-prescription service (including e-dispensing). The project consists of 12 member states and 29 beneficiaries, including an industry consortium of more than 30 partners. It is a time-limited project aiming to provide pilot implementations of the use cases

6 Appendix A – Standards Matrix

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.1.1.1 IHE-CT (RFC1305) – Consistent Time			√										
3.1.1.2 IHE-ATNA – Audit Trail and Node Authentication			√										
3.1.1.3 IHE-XCA - Cross-Community Access			√										
3.1.1.4 IHE-BPPC – Basic Patient Privacy Consents			√										
3.1.1.5 IHE-XDR – Cross enterprise Document Reliable Interchange			√										
3.1.1.6 IHE-XPHR – Exchange of Personal Health Record			√										
3.1.1.7 IHE-XDW – Cross Enterprise Document Workflow			√										
3.1.1.8 IHE-XDS-I – Cross Enterprise Document Sharing for Imaging			√										
3.1.1.9 IHE-XDS - Cross Enterprise Document Sharing			√										
3.1.1.10 IHE-XD-LAB – Sharing Laboratory Reports			√										
3.1.1.11 IHE-SWF – Scheduled Workflow			√										
3.1.1.12 IHE-SVS – Sharing Value Sets			√										
3.1.1.13 IHE-RID – Retrieve information for display			√										
3.1.1.14 IHE-PRE – Pharmacy Prescription Document			√										
3.1.1.15 IHE-PIX – Patient Identifier Cross Referencing			√										
3.1.1.16 IHE-PDQ – Patient Demographics Query			√										
3.1.1.17 IHE-PAM – Patient Administration Management			√										
3.1.1.18 IHE-LTW – Laboratory Testing Workflow			√										

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.1.1.19 IHE-LCSD – Laboratory Code Sets Distribution			√										
3.1.1.20 IHE-DIS – Pharmacy Dispense Document			√										
3.1.1.21 IHE-DEC – Device Enterprise Communication			√										
3.1.1.22 IHE-CMPD – Community Medication Prescription and Dispense			√										
3.1.1.23 IHE- PADV Pharmacy Pharmaceutical Advice Supplement			√										
3.1.1.24 IHE-PML Pharmacy Medication List			√										
3.1.1.25 IHE XCPD Cross-Community Patient Discovery			√										
3.1.1.26 IHE-XCF Cross Community Fetch			√										
3.1.1.27 IHE XUA			√										
3.1.1.28 IHE DSG			√										
3.1.1.29 ISO 27799			√										
3.1.1.30 IHE-XDM Cross Enterprise Document Media Interchange			√										
3.1.1.31 IHE-XPID - Change Management			√										
3.1.2.1 ISO 17090-3:2008				√									
3.1.2.2 SAML v2 - Security Assertion Markup Language				√									
3.1.2.3 WS-I Basic Profile				√									
3.1.2.4 WS-Addressing				√									
3.1.2.5 WS-I Basic security				√									
3.1.2.6 WS-TRUST V1.3				√									

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.1.2.7 WSDL 1.1				√									
3.1.2.8 HTTP 1.1				√									
3.1.2.9 SOAP 1.2				√									
3.1.2.10 UDDI 3				√									
3.1.2.11 IEEE 1003.2 POSIX Shell Standard				√									
3.1.2.12 ebMS OASIS/ebXML Messaging Services Specifications v3.0				√									
3.1.2.13 ebRS OASIS/ebXML Registry Services Specifications v3.0				√									
3.1.2.14 XML				√									
3.1.2.15 XML XSL				√									
3.1.2.16 XML Schema				√									
3.1.2.17 ANSI X12				√									
3.1.2.18 UN/EDIFACT - ISO 9735				√									
3.1.2.19 IEEE 11073 ‘Personal Health Devices’				√									
3.1.2.20 ISO/TR 16056				√									
3.1.2.21 MLLP				√									
3.2.1.1 ASTM CCD					√								
3.2.1.2 ASTM CCR					√								
3.2.2.1 HL7 v2.x						√							

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.2.2.2 HL7 v3						√							
3.2.2.3 DICOM						√							
3.2.3.1 HL7 v3 RIM							√						
3.2.3.1 ebRIM OASIS/ebXML Registry Information Model v3.0							√						
3.2.3.2 HSSP CTS2							√						
3.2.3.3 GS1 Healthcare							√						
3.2.3.4 OID							√						
3.2.3.5 FHIR							√						
3.2.3.6 CEN/ISO EN 13606							√						
3.2.3.7 OpenEHR Clinical Models							√						
3.2.3.8 HL7 v3 Data Types							√						
3.2.3.9 ISO 21090 Harmonized data types for information interchange							√						
3.2.3.10 ISO/IEC 11404 General-Purpose Datatypes							√						
3.2.3.11 ISO/TS 22220 Health informatics -- Identification of subjects of health care							√						
3.3.1.1.1 SNOMED CT								√					
3.3.1.1.2 LOINC								√					
3.3.1.1.3 ISO/TS 14265								√					
3.3.1.1.4 ISO/TS 21298								√					

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.3.1.1.5 ASTM E1986 - 09(2013)								√					
3.3.1.1.6 PCD-RTM – Rosetta Terminology Mapping								√					
3.3.1.1.7 Dm+d								√					
3.3.1.1.8 SNOMED CT UK Drug extension								√					
3.3.1.2.1 ICPC-2									√				
3.3.1.2.2 ICD-10									√				
3.3.1.2.3 ICD-10-AM									√				
3.3.1.2.4 OPCS-4									√				
3.3.1.2.5 MEDDEV									√				
3.3.1.2.6 RxNorm									√				
3.3.2.1 HL7 Version 3 Clinical Document Architecture or CDA v2										√			
3.3.2.2 OASIS-XSPA										√			
3.3.2.3 BPMN										√			
3.4.1.1.1 VPN - IPSec (RFC 4301)											√		
3.4.1.1.2 TLS (RFC 5246)											√		
3.4.1.1.3 ITU-T X.509 / ISO/IEC 9594-8											√		
3.4.1.1.4 ETSI TS 103 231											√		
3.4.1.1.5 S/MIME											√		

Standards	Adoption	Maturity	IT Standards		Syntactical			Semantic			Security	Business	Accessibility
			Operational	Architectural	Document Syntax	Messaging Syntax	Data Model	Terminologies	Classifications	Semantic			
3.5.1.1 ISO/TR 13054 Knowledge management of health information standards												√	
3.5.1.2 ISO/DIS 13940 Health informatics -- System of concepts to support continuity of care												√	
3.5.1.3 ISO/TS 27527 Health informatics -- Provider identification												√	
3.5.1.4 ISO EN 12967 Health Informatics Service Architecture HISA												√	
3.5.1.5 HL7 EHR-System Functional Model												√	
3.6.1.1 Irish National IT Accessibility Guidelines													√
3.6.1.2 Web Content Accessibility Guidelines													√

7 Appendix B - References

Reference List

1. D1.4.1 - EED SERVICES including use cases for all services. Available online from: http://www.epsos.eu/uploads/tx_epsosfileshare/D1.4.1_use_case_description_v1_0_20120221_01.pdf. Accessed on: 25 December 2014

2. EPrescribing and Electronic Transfer of Prescriptions - Hiqa. Available online from: http://hiqa.ie/system/files/Intl-Review-ePrescribing.pdf. Accessed on: 25 December 2014

3. Antilope Refinement Uses Cases, available online from: http://www.antilope-project.eu/wp-content/uploads/2013/05/D1.1-Refinement-of-Antilope-Use-Cases-v1.0.pdf

4. DICOM: http://dicom.nema.org/

5. http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf

6. Interoperability Report. Available online from, Accessed on 25 December 2014. http://healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf.

7. HIQA: http://hiqa.ie/

8. ANTILOPE: http://www.antilope-project.eu/

9. NSAI: http://www.nsai.ie/

10. ISO: http://www.iso.org/iso/home.html

11. CEN: https://www.cen.eu/Pages/default.aspx

12. HL7: http://www.hl7.org/

13. OpenEHR: http://www.openehr.org/

14. Antilope overview. Accessed 25 December 2014: http://www.antilope-project.eu/wp-content/uploads/2013/05/D1.2a-Educational-material-presentation-v1_4.pdf

8 Glossary

8.1 Appendix: Terminology

Term	Definition
(Base) Standard	"As defined in European legislation (Article 1,paragraph 6, of Directive 98/34/EC), a standard is a technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory and which is one of the following: - International standard: a standard adopted by an international standardisation organisation and made available to the public. - European standard: a standard adopted by a European standardisation body and made available to the public - national standard: a standard adopted by a national standardisation body and made available to the public."
Interoperability	The ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.
Interoperability Governance	"Interoperability governance covers the ownership, definition, development, maintenance, monitoring, promoting and implementing of interoperability frameworks in the context of multiple organisations working together to provide services. It is a high-level function providing leadership, organisational structures and processes to ensure that the interoperability frameworks sustain and extend the organisations' strategies and objectives."

Service Level Agreement	"A formalised agreement between two cooperating entities; typically, a service provider and a user. Expressed in the form of a written, negotiated contract. Typically, such agreements define specific metrics (Key Performance Indicators— KPIs) for measuring the performance of the service provider (which in total define the 'service level'), and document binding commitments defined as the attainment of specific targets for certain KPIs, plus associated actions such as corrective measures."

8.2 Appendix: Acronyms

Acronym	Definition
ED	Emergency Department
CDR	Clinical Data Repository
CDS	Clinical Decision Support
HIE	Health Information Exchange
CPOES	Computerised Practitioner Order Entry Systems
BPM	Business process management
ESB	Enterprise Service Bus
SOA	Service Oriented Architecture
ETL	Extract Transform Load
PAS	Patient Administration System
PACS	Picture archiving and communication system
RIS	Radiology information system