IHE SERVICES | Building trust in eHealth interoperability

eHEALTH DIGITAL SERVICES INFRASTRUCTURE
NATIONAL CONTACT POINT IMPLEMENTATION AND TEST PLATFORM SERVICES

Security and Privacy Interoperability Specification

Author	Cédric EOCHE-DUVAL - Charles PARISOT
Contract Reference	Test Harness Support Service – HSE9100-LOT-2
Date	17/12/2018
Version	1.1
Status	Final
Reference	HSE9100-LOT2-IS-SECURITY_PRIVACY-1.1.docx

Document Lifecycle

Version	Date	Author	Update
0.1	27/07/2018	A-G BERGE	Creation
0.2	3/8/2018	Ch. PARISOT	Update
0.3	27/08/2018	C. EOCHE-DUVAL	Review and apply new template
0.4	05/08/2018	C. EOCHE-DUVAL	Add reference to IHE XUA profiles
0.5	02/10/2018	C. EOCHE-DUVAL	Additions after F2F meeting
0.6	14/11/2018	A-G BERGE	Assign OIDs after HSE gets its proper Root OID. Add refere to the SeR profile.
1.0	17/12/2018	A-G BERGE	Clean up
1.1	05/02/2019	H. RAMANANTSALAMA	Correction after Eamon's review

Approval

Name	Responsibility	Signature
Eamon Coyne		
Karen Wynne		

Distribution list

Name	Date	Contact	Purpose*
Eamon Coyne			V
Caitriona Wray			V
Peter Connolly			V

* A: for action / V: for Approval / C: for comments/ I: for information

Reference documents

This section gathers the documents which are referenced in this document. In the body of this document, any reference to an external document is formatted using [KEYWORD] from the first column.

Keyword	Name and reference
[ITERM]	*General Terminology Interoperability Specification* HSE9100-LOT2-IS-TERMINOLOGY
[DOC_SHARING]	*Document Sharing Interoperability Specification HSE9100-LOT2-IS-DOC_SHARING*
[UC_ANALYSIS]	ePrescription and Patient Summary use cases analysis HSE9100-LOT-2-2_DELIVERABLE-1A

Table of content

1 Preface

Ireland as a European country is becoming involved in the eHDSI(eHealth Digital Services Infrastructure) project led by the European Commission under the CEF (Connecting European Facilities) program and will participate to the deployment in the wave 3 (2020). To prepare the deployment of the NCPeH (National Contact Point for eHealth) in Ireland, the HSE (Health Service Executive) procured in 2018 the support services that will facilitate the implementation of the NCPeH and its connection to central Irish services. The first step of the project is to define the needed use cases to support and to design the architecture for connecting the Irish NCPeH. These tasks will be followed by the design of the architecture within Ireland, the corresponding Interoperability Specifications, the testing strategy including test plans and the implementation of Gazelle test platform that includes test cases, test tools and test data.

1.1 Context

Directive 2011/24/EU provides rules for facilitating access to safe and high quality cross border healthcare and promotes cooperation on healthcare between member states. The aims of implementing the Irish NCPeH exchange of Patient Summaries and ePrescription are in line with the principles of cross-border care. The NCPeH and cross border exchange implementations are all key building blocks that will interact with the national data dictionary (single source of trust for clinical data definitions across the enterprise) and the Patient Summary and ePrescribing documents and associated metadata will be stored there as minimum data sets.

The main goals are to design the platform based on the needs that will be developed in the first steps of the project that includes

- Use Cases for ePrescription and Patient Summary
- Corresponding Interoperability specifications and architecture orchestration
- Validated version of IHE Gazelle. The test harness will provide to the authority the ability to test prospective vendors and products against the above interoperability specifications.

1.2 Glossary

IHE profile: provides a common language for purchasers and vendors to discuss the integration needs of healthcare sites and the integration capabilities of healthcare IT products. A Profile is a guideline for implementation of a specific process, by providing precise definitions of how standards can be implemented to meet specific clinical needs. [eHealth Interoperability Conformity Assessment Scheme for Europe (EURO-CAS)]

Interoperability use case: description of a specific use of HIT(Health Information Technology) that includes depiction of both humans (business actors) and systems (technical actors), scope, workflows of tasks performed by healthcare professionals and associated data flows. It should be written in natural language and may include several scenarios. One or more use cases are derived from one business case [IHE taskforce]

Realisation scenario: description of human activities (business actors), systems (technical actors) roles (i.e., IHE actors) and transactions related to a set of technical use cases that

support the interoperability infrastructure for use cases (implementable infrastructure). [IHE taskforce]

1.3 Document purpose

An Interoperability Specification provides a detailed set of requirements (including references to specific profiles and standards) that enable health information exchange in an e-health deployment (national, regional, cross-border, intra institution) for a specific topic.

When covering the requirements related to the realization of an interoperability use case, the corresponding interoperability specification is called a Core Interoperability Specification. A (Core) Interoperability Specification (IS) is targeted to be the sole entry point for the technology developers, the compliance assessment testing, and the purchaser of IT systems in term of technical requirements that will ensure interoperability.

When covering a subset of the interoperability requirements for one or more use cases, the corresponding interoperability specification is called a Supporting Interoperability Specification. Indeed, it is intended to be referenced by one of more Core Interoperability Specifications

The present document is a Supporting Interoperability Specification for the security and privacy topic.

1.4 How to read this document

This document contains three normative sections(2, 3, and 4), as well as informative appendices for the reader convenience. The document is structured as follows:

- **Section 2**: Conformance to the Irish constraints for security and privacy :
- **Section 3**: Irish eHealth constraints for Security and Privacy
- **Section 4**: Lists referenced documents, as well as the international standards which underpin the Interoperability Specification.
- **Appendix A**: Providesa sample consent document
- **Appendix B :** Access Control Decision Matrix

Reviewers note:

Yellow highlighted text requires confirmation/verification/alignment with Irish policies.

Pink highlighted text will be completed by the editor in the next version

1.5 References

From this supporting Interoperability Specification, a number of supporting Interoperability Specifications are referenced:

- General Terminology Interoperability Specification [ITERM]
- Document Sharing Interoperability Specification [DOCSHARING]

The above Interoperability Specifications include precise references to internationally adopted profiles and standards as well as Irish specific constraints.

Implementations are required to conform to the requirements within one or more (Core) Interoperability Specification; some of these requirements include referenced Supporting Interoperability Specifications (such as the present document), and the standards and profiles they specify.

1.6 Description

This Interoperability Specification describes the security and privacy aspects for a wide range of technical interface requirements. It is intended to be referenced by Core Interoperability Specifications (e.g. Patient Summary Sharing or ePrescription Sharing).

1.7 Document convention

Interoperability Specifications contain numbered requirements that follow this format:

[ABCD-###] where ABCD is a three or four letter acronym unique to that Interoperability Specification for convenient purposes, and ### is the unique number for that requirement within the Interoperability Specification.

These numbered requirements are the elements of the Interoperability Specification that the system conforms to. In other words, in order to implement a system that fully supports the Use Case and Interoperability Specification, the system shall be able to demonstrate that it conforms to every numbered requirement for the system actors to which it is claiming conformance.

Please note that all numbered requirements are numbered uniquely, however numbered requirements are not always sequential.

1.7.1 Requirements language

Throughout this document the following conventions[1] are used to specify requirement levels:

- **SHALL:** the definition is an absolute requirement of the specification.
- **SHALL NOT:** the definition is an absolute prohibition of the specification.
- **SHOULD:** there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.
- **MAY** or **OPTIONAL**: means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

1.8 Methodology

[1] Definitions based upon IETF RFC 2119

This Interoperability Specification has been developed with input from various Irish stakeholders collected during several months through workshops and teleconferences.Stakeholders included Physicians from many different disciplines and Irish IT specialists.

The development of a Core Interoperability Specification relies on the high-level requirements set by the associated Use Case. These high-level requirements are not restated in this specification and readers may consider reviewing the related Use Case document.

1.8.1 Introduction of the use case driven approach

This methodology[2] has the objective to:

- Define Use cases and their prioritization to answer the eHealth strategy objectives of nation/region;
- From use cases to design the interoperability specifications and infrastructure based on IHE profiles;
- To define the testing strategy and identify test plan and test methods (test cases, test tools and test data);
- To support Project teams to procure products or solutions for their eHealth Project (Telemedicine, national/regional EHR, replacement of product in hospitals, …);

The methodology is based on experiences and good practices in other countries or regions. It is further described in [UC_ANALYSIS], section 4.

[2] Bourquard,Karima and Berler, Alexander. Use case driven approach for a pragmatic implementation of interoperability in eHealth. IGI Global Journal

2 Conformance to the Irish constraints for security and privacy

Systems **SHALL** NOT claim conformance to this Interoperability Specification. Systems **SHALL** claim conformance to the requirements defined in the Core Interoperability Specifications thatreference this document. The Core Interoperability Specifications deliver a user-relevant set of requirements corresponding to an Interoperability Use Case.

3 Irish eHealth constraints for Security and Privacy

This section specifies Irish extensions and constraints related to a series of specific areas of Security and Privacy and the relevant underlying IHE profile. All details of these IHE Profiles are specified in IHE ITI TF-1 (See Section 4, Table 4-2, for more information on where to find these profiles).

3.1 Requirements for maintaining consistent time

3.1.1 Requirements for a Time Server

*[S&P-001]*The ***Irish eHealth Infrastructure*** Time Server Actor **SHALL** implement the IHE CT Time Server Actor

> *Note: The IHE CT Profile requires the Time Server Actor to support both the SNTP and the NTP protocol options.*

3.1.2 Requirements for a Time Client

*[S&P-002]*The Core Interoperability Specification defined Actor **SHALL** implement the IHE CT Time Client technical actor.

> Note: The IHE CT Profile requires the Time Client Actor to support either the SNTP or the NTP protocol option with 1 second accuracy.

3.2 Requirements for Secured Node Communication

3.2.1 Requirements for Authentication for a Secure Node Actor or a Secured Application Actor

[S&P-003] The Machines/Hosts connected to the Irish eHealth Infrastructure shall be Identified and Authenticated. As a result, each one shall be assigned by the Irish eHealth Infrastructure a specific digital certificate that shall be securely loaded into the secured certificate store of that Machine/Host and used for TLS mutual authentication. The Irish eHealth Infrastructure will also provide them a public key for the Identification and Authentication of an Irish eHealth Infrastructure Secure Node to connect to.

*[S&P-004]*An Irish eHealth Infrastructure Trust Model **SHALL** be supported by every Secure Node Actor.

*[S&P-007]*The CA Trust Model approach**SHALL** be used: Node Certificates **SHALL** be issued under the *Irish Health Information Exchange Policy* to nodes under the authority of a designated *National Center for Digital Certificates*) that creates a dedicated branch (Root CA for eHealth).

Note: The Irish Health Information Exchange Policy is under definition by the Department of Health. Irish Health Information Exchange Policy is used as a "place holder". These requirements are consistent with the intended direction and will be used until such policy is issued.

Note: These node certificates include the identity of the issuing CA proven by a signature of that CA. It is proposed that the CA supports both the CRL (with http transport) and OCSP revocation checking protocols.

[S&P-005] Secured Node Actors **SHALL** perform certificate validation including expiration and revocation supporting either CRL (with http transport) and/or OCSP as identified in the certificate content. Revocation checking **SHOULD NOT** be performed for every transaction but**SHALL** be performed at least every 6 hours.

3.2.2 Requirements for Channel Security for a Secure Node Actor or a Secured Application Actor

[S&P-006] The Machines/Hosts connected to ***Irish eHealth Infrastructure*****SHALL** use encryption for the exchange of information to and from the***Irish eHealth Infrastructure***.

*[S&P-007]*The TLS version 1.2 is strongly recommended, but TLS versions 1.0 and 1.1 are allowed.

*[S&P-008]*The TLS encryption on these Machines/Hosts **SHALL** support the following cipher algorithms:

- TLS_DHE_RSA_WITH AES_128_CBC_SHA
- TLS_DHE_RSA_WITH AES_256_CBC_SHA.

Note: stronger algorithms may be implemented and become activated through TLS negotiation.

3.3 Requirementsfor Audit Trail

The *Irish Health Information Exchange Policies*establish that requirements for audit trail depend on the type of systems:

- ***HIE (Health Information Exchange) Nodes*** are defined as nodes connected to the***Irish eHealth Infrastructure*** Systems.Applicationson these HIE Nodes are required to perform internal audit logging of policy-specified information audit events (and their attributes) as typically required by Core Interoperability Specification(s). For ***HIE Nodes***, no electronic exchange of the audit events information with the***Irish eHealth Infrastructure*** systems is required.

Note: IHE ATNA may be used within the organization acting as an HIE Node, but this is not required.

- ***Irish eHealth Infrastructure***Systems are defined as systems to which ***HIE Nodes*** are connected.Applicationson these eHealth Infrastructure systems are required to perform audit logging of policy-specified event information in a manner for which electronic exchange of the audit events information is centralized on a***Irish eHealth Infrastructure*** Audit Record Repository using IHE ATNA Profile based interoperability. This provides the ***Irish eHealth Infrastructure*** Security and Privacy officer a single access to all audit events collected by all ***Irish eHealth Infrastructure*** Systems.

Note: The rationale for this approach is to ensure that any security or privacy investigation may be easily analyzed by designating the HIE Nodes that are likely involved. The security and privacy officer responsible for an HIE Node will need to use its internal audit trail repository to further pursue the investigation as necessary. The policy requires full cooperation of the HIE Node security and privacy officers with the Irish eHealth Infrastructure Security and Privacy Officer.

3.3.1 Requirements for Audit Trail Source Actor for Irish eHealth Infrastructure Systems

[S&P-010] An Audit Trail **SHALL** be recorded according to the Audit Events defined for the transactions supported by those systems and the IHE ATNA Profile.

*[S&P-011]*Audit Events **SHALL** be sent using the Syslog TCP Transport over TLS (RFC 5425, See ATNA Profile section 3.20.4.1.2.1.1 Transmission of Syslog Messages over TLS).

Note: In ATNA Profile, Transmission of Syslog messages over TLS (RFC5425) with the Syslog Protocol (RFC5424) formalizes sending Syslog messages over a streaming protocol protectable by TLS. RFC5425 states that this MUST be TLS version 1.2.

3.3.2 Requirements for Audit Trail Source Actor for HIE Nodes

*[S&P-012]**HIE Nodes*** connected to the ***Irish eHealth Infrastructure*** Systems **SHALL** ensure the recording of the security relevant audit events (See IHE ITI TF-2a Section 3.20.6 Trigger Events and Message semantics and other specific profile or standards defined audit events) in a persistent store. The data elements recorded for these audits events **SHALL** comply only with the data elements definitions from the IHE ATNA Profile and more specifically IHE ITI TF-2a Section 3.20.7 Audit Message Formats (they **MAY NOT** support the IHE ATNA specific encoding and transport.

[S&P-013] - This persistent store **SHALL** support security and privacy inquiries (see Irish Health Information Exchange Policies) such as:

- list all users that accessed or modified a specified subject of care information over a period of time)
- list of all subjects of care that were accessed by a given user or system over a period of time
- list of all breakglass events
- list all access events where the user is not listed as a provider in any patient record
- list events that request information that is marked as sensitive

Note: The Irish Health Information Exchange Policy is under definition by the Department of Health. Irish Health Information Exchange Policy is used as a "place holder". These requirements are consistent with the intended direction and will be used until such policy is issued.

3.4 Requirements for USER Assertion

User SAML Assertionsare used to communicate identity claims about an authenticated principal (user, application, system, etc.) in the services requested by systems connected to the Irish eHealth Infrastructure using one of the Core Interoperability Specifications. Those

assertions are carryingthe identification of the user with a number of attributes.These attributes enable the receiver to make access decisions and create proper audit trail entries.

3.4.1 Requirements for an X-Service User Actor

[S&P-027] Nodes that need to be grouped with an X-Service User **SHALL** fulfill requirements of the IHE XUA X-Service User actor and transaction ITI-40 requirements.

X-Service User**SHALL** support the following attributes:

- *[S&P-021]*Subject Role. The value **SHALL** be one of the values of Individual Provider Specialty Value Set (OID= 1.2.372.980010.3.4) specified in the General Terminology Interoperability Specification.
- *[S&P-022]*Purpose of Use (including breakglass).The value **SHALL** be one of the values of the Purpose of Use Value Set.The value set (OID=1.2.372.980010.3.5)is specified in the General Terminology Interoperability Specification.
- *[S&P-026]* A local text field containing the reason for the breakglass**SHALL** be captured and recorded in the local audit trail.

Note: This recorded reason for the breakglass need not be transmitted in the User Assertion when ensuing communication occurs with the **Irish eHealth Infrastructure**.

- *[S&P-023]* -Subject Id is the local login username
- *[S&P-024]* - Subject Organization Identifier

Note: this Organization Identifier is expected to be configured in the source system to be consistent with the Organization Identifier provided by the IrishService Directory service.

- *[S&P-025]*National Provider Identifier

Note: This Provider Identifier is expected to be the Irish issued Professional ID from the Irish Service Directory service.

Note: Those attributes are focused on a person authentication, we also need to consider System/Application authentication in an Assertion (in case of automatic triggering, batch…)

3.4.2 Requirements for an X-Service Provider Actor

[S&P-036] Nodes that need to be grouped with an X-Service Provider **SHALL** fulfill requirements of the IHE XUA X-Service Provider actor and ITI-40 transaction requirements.

*[S&P-030]*To enable the receiver to make access decisions and proper audit entries the following attributes shall be supported (See access control matrices in Appendix B – Access Control Decision Matrices).

- *[S&P-031]* Subject Role. The value SHALL be one of the values of the Individual Provider Role Value Set (OID= 1.2.372.980010.3.4) specified in the General Terminology Interoperability Specification.

- *[S&P-032]* Purpose of Use (including breakglass). The value **SHALL** be one of the values of the Purpose of Use Value Set specified in the General Terminology Interoperability Specification (OID = 1.2.372.980010.3.5).
- *[S&P-033]* Subject ID is the local login username
- *[S&P-034]* Subject Organization Identifier

Note: This Organization Identifier is expected to be configured in the source system to be consistent with the Organization Identifier provided by the Irish Healthcare Service when deployed.

- [S&P-035] - National Provider Identifier

Note: This Provider Identifier is expected to be the Irish issued Professional ID from the Irish Service Directory service.

3.5 Requirements for Confidentiality Level

3.5.1 Requirements for an Actor That Is the Source of Information

[S&P-040] A source of an information element (e.g. a document) **SHALL** place (e.g. document entry metadata) the appropriate confidentiality level given the privacy sensitivity of the information communicatedthrough the***Irish eHealth Infrastructure***. This requirement results in using the restricted confidentiality level per the *Irish Health Information Exchange Policy:* The Confidentiality Code values to be used are specified in the Confidentiality Code value set (OID=1.3.6.1.4.1.12559.11.10.1.3.1.42.31) from the General Terminology Interoperability Specification.

3.5.2 Requirements for an Actor that accesses of information

[S&P-041] A consumer of an information element (e.g. a document) **SHALL** process the Confidentiality Code to account for the privacy sensitivity of the information accessed from the Document Repository Actor. The confidentiality codes are specified by the Confidentiality Code Value Set (OID=1.3.6.1.4.1.12559.11.10.1.3.1.42.31) from the General Terminology Interoperability Specification. The control resulting from an information element (e.g. a document) with the restricted confidentiality level **SHALL** apply requirements from the Irish Health Information Exchange Policy (See access control matrices in Appendix B – Access Control Decision Matrices).

3.6 Requirements for Privacy Consent

3.6.1 Requirements for a Privacy Consent Creator Actor

The Privacy Consent Creator Actor is an IHE Technical Actor that is typically implemented in a point of service Use Case Actor or in a system part of the ***Irish eHealth Infrastructure*** such as a client portal system. It allows the patient to express preferences in term of privacy.

[S&P-042] A Privacy Consent Creator shall implement the IHE Basic Patient Privacy Consents Profile (BPPC). It results in the selection of one of the following policies:

- *[S&P-043]* Opt-Out Policy identified with an OID (1.2.372.980010.2.2) specified in Appendix A.

- *[S&P-044]* Opt-In Policy identified with an OID (1.2.372.980010.2.1)specified in Appendix A.

Note: This simple policy choice is based upon the current understanding that the Irish Health Information Exchange Policy allows that all "clients" of the Irish Health Infrastructure (e.g. patients/citizens) can be, by default, considered "opt-in" until they chose to "opt-out". At any point in time a client that previously opted-out may choose to revert its opt-out for an opt-in. If other privacy consent expressions are allowed, the above list would need to be extended with additional specific privacy policies.

[S&P-065] - The Privacy Consent Creator **SHALL** support the creation of shared BPPC Consent Document. The following XDS Metadata attributes**SHALL**be included:

- *[S&P-066]*eventCodeList**SHALL** contain the OID of the selected policy. (See Section 5.1.2.1.1.2 XDSDocumentEntry.eventCodeList from IHE ITI TF-3)
- *[S&P-067]* Title **SHALL**contain the display name of the "Privacy Policy Acknowledgement Document".
- *[S&P-068]*documentClass**SHALL** contain the coded value "PATIENT" as defined in the XDS classCodevalue set (OID = "1.3.6.1.4.1.19376.1.2.6.1").
- *[S&P-069]*typeCode**SHALL** contain the LOINC code "57016-8" (Privacy Policy Acknowledgement Document) with a codeSystem OID: 2.16.840.1.113883.6.1.
- *[S&P-070]*mimeType**SHALL** contain "text/xml".
- *[S&P-071]*formatCode**SHALL** contain "urn:ihe:iti:bppc-sd:2007"(BPPC with scanned part).

All other XDS Metadata Attributes shall contain values as specified in the Document Sharing Interoperability Specification

  - *[S&P-072]*Confidentiality Code: **SHALL**contain the value "N" of the value set OID=1.3.6.1.4.1.12559.11.10.1.3.1.42.31 from the General Terminology Interoperability Specification.
  - *[S&P-073]*HealthcareFacilitytype**SHALL**be taken from value set Organization Provider Type (OID = 1.2.372.980010.3.2)
  - *[S&P-074]*PracticeSettingCode**SHALL**be taken from value set Organization Specialty (OID = 1.2.372.980010.3.3)

- *[S&P-075]* All other XDS Metadata Attributes with corresponding data elements in the Consent document **SHALL** be consistent with these values in the Consent document.

[S&P-048] The expression of the acknowledgement of any of the above policies **SHALL** be represented by a Privacy Consent Document as specified by IHE BPPC profile with the appropriate service event in the CDA Header and a Body as an enclosed PDF (e.g. with a wet signature).

[S&P-049] Any update to the expression of this consent (opt-out or opt-in after opt-out) **SHALL** result in the Privacy Content Creator to replace the associated Privacy

Consent Document as specified by IHE Basic Patient Privacy Consent (BPPC) Profile.

3.6.2 Requirements for a Document Repository and Document Registry Actor to enforce access control

*[S&P-050]*Document Repository Actor shall act as an Authorization Decisions Verifier actor for the IHE Secure Retrieve (SeR) profile.

*[S&P-051]*Document Registry Actor shall act as an Authorization Decisions Manager actor for the IHE Secure Retrieve (SeR) profile.

Note: Document Repository and Document Registry might choose to implement an ad Hoc interface with functionalities and purposes equivalent to the SeR profile.

Note: When using the SeR profile, Document Repository and Document Registry shall agree in advance of the attributes to be used in the Authorization Decision Query transaction.

Document Registry Actor **SHALL**take access control decisions based on following policies:

- *[S&P-052]* Default Opt-In Policy. The access control matrix specified in Appendix B table B-1 shall be enforced.
- *[S&P-053]* Opt-Out Policy. The access control matrix specified in Appendix B table B-2 shall be enforced.

Note: *Changing from policy Opt-In to policy Opt-Out results in switching the enforcement from Appendix B table B-1 to table B-2.*

4 Referenced Documents and Standards

The following documents and standards were referenced during the development of this Interoperability Specification.

TABLE 4-1 INTERNAL REFERENCES

DOCUMENT OR STANDARD	DESCRIPTION
General Terminology Interoperability Specification	Specifies the terminology concepts and associated coded value sets for common data elements used throughout Irish eHealth Interoperability Specifications. For example, common metadata data elements used within the content related Irish interoperability specifications.
Irish Health Information Exchange Policies	Contains the policies and supporting definitions that support the security and privacy aspects of the Irish Health Information Exchange. The Irish Health Information Exchange Policies apply to all individuals and organizations that have access to the health records access through the Irish eHealth Infrastructure, including those connected to the Irish eHealth Infrastructure, their Business Associates, as well as any subcontractors of Business Associates. These policies apply to all information provided to or retrieved from the Irish eHealth Infrastructure.

TABLE 4-2 EXTERNAL REFERENCES

DOCUMENT OR STANDARD	DESCRIPTION
ASTM International(ASTM) #E1986 09(2013) Standard Guide for Information Access Privileges to Health Information	Provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives. In particular, Table 2 Healthcare Personnel that Warrant Differing Levels of Access Control provides the necessary content for structural roles for user-based access controls enforcing patient consent directives
IHE IT Infrastructure (ITI) Technical Framework– Volume 1 (ITI TF-1) Integrations Profiles, Final Text Section 7 – IHE Consistent Time (CT)	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 synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. May be obtained at https://www.ihe.net/resources/technical_frameworks/#IT
IHE IT Infrastructure (ITI) Technical Framework – Volume 1 (ITI TF-1) Integrations Profiles, Final Text Section 9: Audit Trail and Node Authentication (ATNA)	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. May be obtained at https://www.ihe.net/resources/technical_frameworks/#IT
IHE IT Infrastructure (ITI) Technical Framework – Volume 1 (ITI TF-1) Integrations Profiles, Final Text Section 13 Cross-Enterprise User Assertion (XUA) profile	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. May be obtained at https://www.ihe.net/resources/technical_frameworks/#IT
IHE IT Infrastructure (ITI) Technical Framework – Volume 1 (ITI TF-1) Integrations Profiles, Final Text Section 19 – Basic Patient Privacy Consent (BPPC)	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 describe how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. EHR systems). May be obtained at https://www.ihe.net/resources/technical_frameworks/#IT
IHE IT Infrastructure (ITI) Technical Framework – Supplement – Secure Retrieve (SeR)	Secure Retrieve (SeR) profile defines a framework able to enforce a centralized Access Control system, conveying between actors involved in a XDS environment the evidence of the reliable decisions already made by an Access Decision Manager. May be obtained at https://www.ihe.net/resources/technical_frameworks/#IT
International Health Terminology Standards Development Organization (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	SNOMED CT consists of a technical design, core content architecture, and Core content. SNOMED CT Core content includes the technical specification of SNOMED CT and fully integrated multi-specialty clinical content. The Core content also includes a concepts table, description table, relationships table, history table, ICD-9-CM mapping, and Technical Reference Guide. Additionally, SNOMED CT provides a framework to manage language dialects, clinically relevant subsets, qualifiers and extensions, as well as concepts and terms unique to particular organizations or localities. For more information visit www.ihtsdo.com

5 Appendix A – SAMPLE BPPC Consent Document

EXAMPLES WILL BE PROVIDED AS PART OF THE IS SPECIFICATION VALIDATION PROCESS. UNTIL THEN THIS SECTION WILL REMAIN BLANK.

6 Appendix B – Access Control Decision Matrices

The following matrix (Table B-1) provides the access control decisions per the IrishHealth Information Exchange Policies where individuals with a specific role are granted access to health information with a specific confidentiality level. These individuals' roles are defined in the Irish Health Information Exchange Policies. This matrix is integral to supporting the Irish Opt-In policy and the situations when the subject of care has elected to Opt-In. This Opt-in Policy is identified by the following OID (Object Identifier): 1.2.372.980010.2.2

TABLE B-1: ACCESS CONTROL MATRIX FOR OPT-IN POLICY

CONFIDENTIALITY ROLES	N (NORMAL)	R (RESTRICTED)
Subject of care	Access granted	Access granted
Subject of care Agent*	Access granted	Access granted
Privileged Healthcare Professional**	Not Applicable**	Not Applicable**
Healthcare Professional	Access granted	Access granted if purpose of use is breakglass.
Health related Professional	No Access	No Access
Administrator	No Access	No Access

**A Subject of care Agent is a person generally designated by the patient to help in supporting care. It may be a relative, a friend, or a person of trust designated by the patient.*

***Privileged Healthcare Professional is a concept of a physician designated by the patient with extended care coordination responsibilities and privileges. This type of physician role is not formalised at this point in Ireland (In other countries it is called "physician of trust", "gate keeper"). It is included in the table to illustrate a possible extension.*

The following matrix (Table B-2) provides the access control decisions per the Irish Health Information Exchange Policies where health professionals with a specific role are granted access to health information with a specific confidentiality level. This matrix is integral to supporting the Irish Opt-Out policy identified by the following OID (Object Identifier): 1.2.372.980010.2.1

TABLE B-2: ACCESS CONTROL MATRIX FOR OPT-OUT POLICY

CONFIDENTIALITYROLES	N (NORMAL)	R (RESTRICTED)
Subject of care	Access granted	Access granted
Subject of care Agent*	No Access	No Access
Privileged Healthcare Professional**	Not Applicable**	Not Applicable**
Healthcare Professional	Access granted if purpose of use is breakglass.	Access granted if purpose of use is breakglass.
Health related Professional	No Access	No Access
Administrator	No Access	No Access

**A Subject of care Agent is a person generally designated by the patient to help in supporting care. It may be a relative, a friend, or a person of trust designated by the patient.*

***Privileged Healthcare Professional is a concept of a physician designated by the patient with extended care coordination responsibilities and privileges. This type of physician role is not formalized at this point in Ireland (In other countries it is called "physician of trust", "gate keeper"). It is included in the table to illustrate a possible extension.*