Kingdom of Saudi Arabia

National Health Information Center (NHIC)

Enabling Standards-Based eHealth Interoperability

IS0101
Saudi eHealth Security and Privacy Interoperability Specification

Version 1.0
April 21, 2016

Document Control Number: IS0101 Saudi eHealth Security and Privacy Interoperability Specification

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Document Revision History

Version	Date	Type of update	Prepared
1.0	April 21, 2016	First Release	National Health Information Center

1. INTRODUCTION

1.1 DOCUMENT PURPOSE

The purpose of this document is to support several Core Interoperability Specifications and their associate Use Cases, in a specific area of interoperability. This area is centered on the technical security measures, data protection, and privacy management that will facilitate the implementation of the Saudi eHealth Policies for Health Information Exchange in the Kingdom of Saudi Arabia among communicating health IT systems. It also aligns with the Saudi e-Government Interoperability Standards (YEFI) to expedite national adoption.

The scope of this document is to specify the Saudi eHealth specific constraints when using the IHE Audit Trail and Node Authentication profile (ATNA), the IHE Consistent Time (CT) profile, the Cross-Enterprise User Assertion (XUA) profile and the Basic Patient Privacy Consents (BPPC) to secure and control the confidentiality of shared information. It complements these IHE Profiles when they are called upon by any of the Saudi eHealth Core Interoperability Specifications.

This supporting Interoperability Specification is applicable to existing and new information systems to be connected to the national Saudi eHealth Exchange (SeHE) System.

1.2 DESCRIPTION

The Saudi eHealth Security and Privacy Interoperability Specification specifies the interoperability standards and profiles along with the Saudi specific constraints that are required to provide the technical security measures, data protection, and privacy management that will facilitate the implementation of the Saudi eHealth Policies for Health Information Exchange in the Kingdom of Saudi Arabia among communicating IT systems.

It is used in conjunction with multiple Core Interoperability Specifications that enable the sharing of health information.

1.3 SCOPE

In Scope:

The scope of this document is the specification of Saudi eHealth specific constraints when using the IHE Audit Trail and Node Authentication profile (ATNA), the IHE Consistent Time (CT) profile, the Cross-Enterprise User Assertion (XUA) profile and the Basic Patient Privacy Consents (BPPC) to secure and control the confidentiality of shared information.

1.4 METHODOLOGY

This Interoperability Specification has been developed with input from various Saudi stakeholders collected during the development of the Saudi Health Information Exchange Policies over several months of workshops and teleconferences.

This document is a supporting Interoperability Specifications that may be referenced by a number of Core Interoperability Specifications, as shown in Figure 1.4-1 References to the

Security and Privacy Interoperability Specification Further descriptions and references for the documents identified below are provided in Section 4 Referenced Documents and Standards**Error! Reference source not found.**.

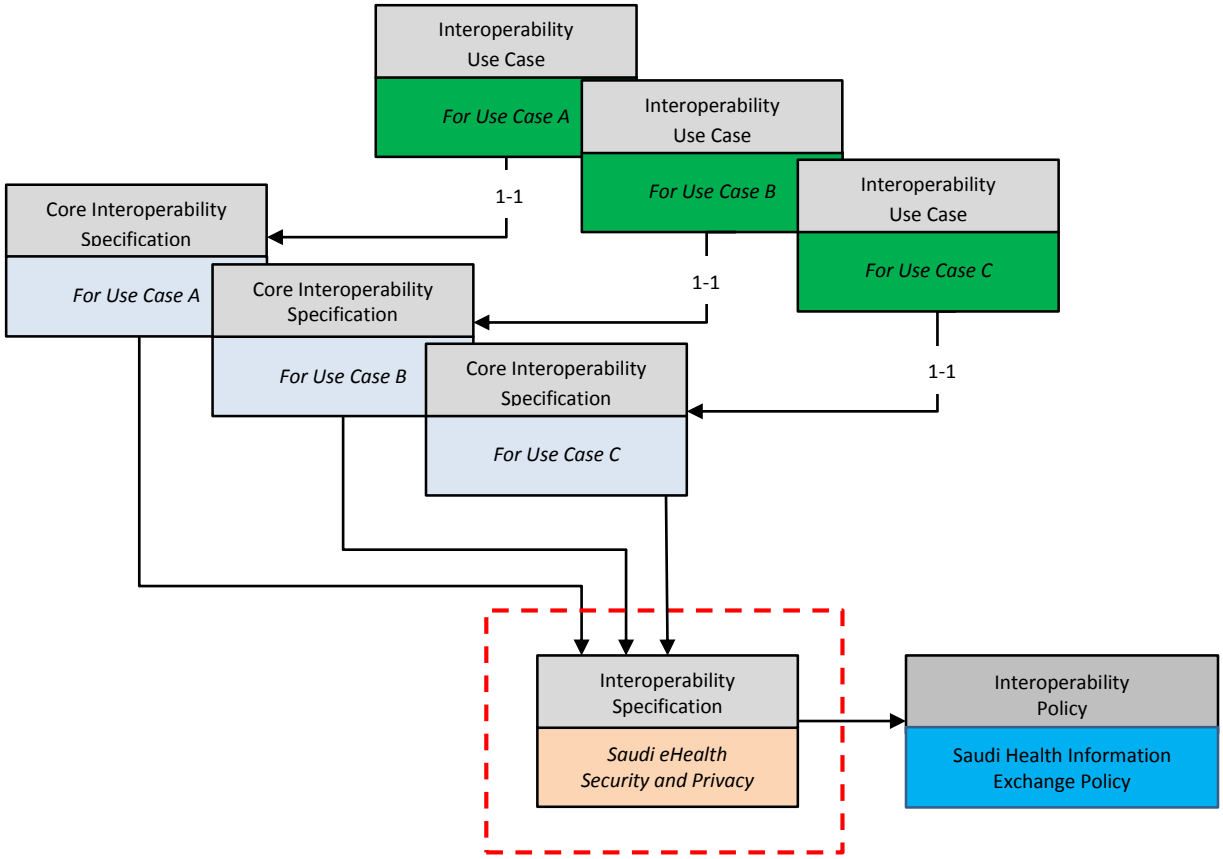

FIGURE 1.4-1 REFERENCES TO THE SECURITY AND PRIVACY INTEROPERABILITY SPECIFICATION

These Saudi Interoperability Specifications include precise references to internationally adopted profiles and standards as well as Saudi specific requirements.

Implementations are required to conform to the requirements within this Supporting Interoperability Specification as well as all referenced SeHE System Interoperability Specifications and the standards and profiles specified within.

1.5 HOW TO READ THIS DOCUMENT

The reader of this Interoperability Specification is expected to be familiar with the Saudi Health Information Exchange Policies that provide the high-level requirements for the security and privacy capabilities supported by this specification.

The reader of this Interoperability Specification is also assumed to be familiar with the IHE ATNA, CT, XUA, and BPPC Profiles. The IHE BPPC Profile offers a number of profile options and the ability to assign specific coded value sets to certain XDS Metadata attributes. The XUA Profile offers the ability to assign specific coded value sets to certain assertion attributes. These value sets are defined to enable definite and consistent choices throughout the Saudi eHealth Exchange (SeHE) System and to ensure effective interoperability between systems.

1.5.1 Where to Find Information

This document contains four normative sections, as well as informative appendices for your convenience. The document is structured as follows:

Section 1: Contains an introduction to the Interoperability Specification (IS). This section contains a summary of the IS purpose and scope, as well as other content to help orient the first time reader to the topic of the IS and how it relates to other specifications in the SeHE System.
Section 2: Outlines conformance requirements to this and related Interoperability Specifications.
Section 3: Details the constraints to international standards used in this IS.
Section 4: Lists the Saudi eHealth reference documents, as well as the international standards which underpin the Interoperability Specification.
Appendix A: Describes a sample BPPC Profile Consent document
Appendix B: Provides the access control decisions for individuals with a specific role when accessing health information with a specific confidentiality level

1.5.2 Document Conventions

1.5.2.1 REQUIREMENTS NUMBERING CONVENTIONS:

All Saudi eHealth 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 convenience purposes, and ### is the unique number for that requirement within the Interoperability Specification.
- Where a specific value set or code is required to be used, it can be found in the "IS0200 Saudi Health Information Exchange Data Dictionary". The location and process to access the Health Information Exchange Data Dictionary will be specified in mechanisms external to this document.

Saudi eHealth 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 that it is implementing.

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

1.5.2.2 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.
(Note: "SHALL …… IF KNOWN" means that the tag must be sent. However, if there were no information, then this tag should be sent with a <nullflavor>)
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.

1.6 DESIGN CONSTRAINTS AND ASSUMPTIONS

This specification addresses design constraints that are to be used by all Core Interoperability Specifications that exchange health information. The constraints may apply differently to different Core Interoperability Specifications based on a risk analysis related to the supported Use Case. Each Core Interoperability Specification may override and/or provide additional constraints based upon the specific requirements of the Use Case.

The technical interoperability security and privacy methods specified in this Interoperability Specification are consistent with, and contribute to, the enforcement of the Saudi Health Information Exchange Policies.

[1] Definitions based upon RFC 2119

2. CONFORMANCE TO THE SAUDI 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 that reference this document. The Core Interoperability Specifications deliver a user-relevant set of requirements corresponding to an Interoperability Use Case.

3. SAUDI EHEALTH CONSTRAINTS FOR SECURITY AND PRIVACY

This section specifies Saudi eHealth 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 Table 4-2 **Error! Reference source not found.** for more information on where to find these profiles).

3.1 REQUIREMENTS FOR MAINTAINING CONSISTENT TIME

3.1.1 Requirements for a Time Server

[SP-001] -The SeHE 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

[SP-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

[SP-003] - The Machines/Hosts connected to the SeHE System **SHALL** be Identified and Authenticated. As a result they will each be assigned by SeHE a specific digital certificate that shall be securely loaded into the secured certificate store of that Machine/Host and used for TLS mutual authentication. SeHE will also provide them a public key for the Identification and Authentication of a SeHE Secure Node.

[SP-004] – Two Trust models **SHALL** be supported by every Secure Node Actor:

- CA Trust approach: Node Certificates issued under the Saudi Health Information Exchange Policy to nodes under the authority of the NCDC (Saudi National Center for Digital Certificates) that creates a dedicated branch (Root CA for eHealth).

  > Note: These node certificates include the identity of the issuing CA proven by a signature of that CA. It is proposed that the CA has to support both the CRL (with http transport) and OCSP revocation checking protocols. This is compatible with the Saudi NCDC choices.

- SeHE Direct Trust Certificate approach: Node Certificates created under that process are communicated through secured means to each peer node and installed on the system as a certificate to be trusted directly by the system.

[SP-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 need 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

[SP-006] - The Machines/Hosts connected to SeHE System shall use encryption for the exchange of information to and from SeHE. The TLS encryption **SHALL** support the TLS_RSA_WITH_AES_128_CBC_SHA encryption algorithm.

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

3.3 REQUIREMENTS FOR AUDIT TRAIL

The Saudi Health Information Exchange Policies requirements for audit trail depend on the type of systems:

- HIE Nodes **SHALL** be supported. HIE Nodes are defined as nodes connected to the Saudi Health Information Exchange Systems by requiring the support of an application performing internal audit logging of policy-specified information per the audit events (and their attributes) required by the Core Interoperability Specification. For HIE Nodes, no electronic exchange of the audit events information with SeHE systems is required.

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

- SeHE HIE Systems are defined as systems to which HIE Nodes are connected by requiring the support on each system of an application performing audit logging of policy-specified event information in a manner for which electronic exchange of the audit events information is centralized on a SeHE Audit Record Repository using IHE ATNA Profile based interoperability. This provides the SeHE Security and Privacy officer a single access to all audit events collected by all SeHE HIE Infrastructure Systems.

  > Note: The rationale for this recommended approach is to ensure that any security or privacy investigation may be easily analyzed to designate 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 SeHE Security and Privacy Officer.

3.3.1 Requirements for Audit Trail Source Actor for SeHE Infrastructure Systems

[SP-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.

[SP-011] - An Audit Event **SHALL** be sent using the UDP transport.

3.3.2 Requirements for Audit Trail Source Actor for HIE Nodes

[SP-012] - HIE Nodes connected to the SeHE 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 but may meet the IHE ATNA specific encoding and transport. This persistent store **SHALL** support security and privacy inquiries (see Saudi 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

3.4 REQUIREMENTS FOR USER ASSERTION

3.4.1 Requirements for an X-Service User Actor

[SP-020] - The means to communicate identity claims about an authenticated principal (user, application, system, etc.) in the services requested by systems connected to SeHE using one of the Core Interoperability Specifications **SHALL** support the identification of the user with a number of attributes. These attributes enable the receiver to make access decisions and proper audit entries. The following attributes shall be supported:

- [SP-021] -Subject Role. The value **SHALL** be one of the values of "Healthcare Specialty Identifier".
- [SP-022] - Purpose of Use (including breakglass). The value set is specified in *IS0200 Saudi Health Information Exchange Data Dictionary*.
- [SP-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 SeHE.

- [SP-023] -Subject Id is the local login username
- [SP-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 KSA Healthcare Provider Directory service when deployed.

- [SP-025] - National Provider Identifier

  This Provider Identifier is expected to be the Saudi Council for Health Specialties (SCHS) issued Professional ID.

3.4.2 Requirements for an X-Service Provider Actor

[SP-030] - In order to enable the receiver to make access decisions and proper audit entries the following attributes **SHALL** be supported:

- [SP-031] - Subject Role. The value SHALL be one of the values of the "Healthcare Specialty Identifier" Value Set.
- [SP-032] - Purpose of Use (including breakglass). Coded value set.
- [SP-033] - Subject ID is the local login username
- [SP-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 KSA Healthcare Provider Directory service when deployed.

- [SP-035] - National Provider Identifier

  This Provider Identifier is expected to be the Saudi Council for Health Specialties (SCHS) issued Professional ID.

3.5 REQUIREMENTS FOR CONFIDENTIALITY LEVEL

3.5.1 Requirements for an Actor That Is the Source of Information

[SP-040] - A source of an information element (e.g. a document) **SHALL** place the appropriate confidentiality level given the privacy sensitivity of the information communicated with SeHE. This requirement results in using the restricted confidentiality level per the Saudi Health Information Exchange Policy: See Section 8.3. The Confidentiality Code values to be used are specified in the "Confidentiality Code" value set.

[SP-075] – When a source of information publishes a document (e.g. laboratory order, laboratory result, imaging report, imaging study manifest) to the Document Repository with a restricted Confidentiality Level, the source of information **SHALL** also publish a normal sensitivity document, where the sensitive information has been removed. This normal Confidentiality Level document **SHALL** be linked to the document of restricted Confidentiality Level using an XDS document transform association between the two documents.

3.5.2 Requirements for an Actor that accesses of information

[SP-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. The control resulting from an information element (e.g. a document) with the restricted confidentiality level **SHALL** apply requirements from the Saudi Health Information Exchange Policy: See Section 8.3, Item 8.

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 SeHE Infrastructure such as a client portal system. It allows the patient to express preferences in term of privacy.

[SP-042] - A Privacy Consent Creator **SHALL** implement the IHE Basic Patient Privacy Consents Profile (BPPC). It results in the creation of one or more of the following policies:

- [SP-043] –Opt-Out Policy identified with an OID specified in Appendix A.
- [SP-044] –Opt-In after Opt-Out Policy identified with an OID specified in Appendix A.

[SP-065] - The Privacy Consent Creator **SHALL** support the creation of shared BPPC Consent Document along with XDS Metadata that **SHALL** include the following attributes:

- [SP-066] An eventCodeList Attribute **SHALL** be created and contain the OID of the selected policy. (See Section 5.1.2.1.1.2 XDSDocumentEntry.eventCodeList from IHE ITI TF-3)
- [SP-067] A Title Attribute **SHALL** be created and contain the “Privacy Policy Acknowledgement Document” display name with one of the display name values defined in the "Laboratory Specialty/Departments" value set.
- [SP-068] A documentClass Attribute **SHALL** contain the coded value “PATIENT“as defined in the "documentClass" value set.
- [SP-069] The typeCode Attribute **SHALL** contain the LOINC code “57016-8” “Privacy Policy Acknowledgement Document” with a codeSystem OID: 2.16.840.1.113883.6.1.
- [SP-070] The mimeType attribute **SHALL** contain one coded value which **SHALL** be "text/xml" as described in the "MimeType" value set.
- [SP-071] The formatCode attribute **SHALL** contain one coded value which shall be "urn:ihe:iti:bppc-sd:2007" for BPPC with scanned part or "urn:ihe:iti:bppc:2007" for BPPC with no scanned part.
- [SP-072] All other XDS Metadata Attributes **SHALL** contain values as specified in the IS0102 *Saudi eHealth Document Sharing Interoperability Specification* - Section 4.2.1.
- [SP-073] All other XDS Metadata Attributes with corresponding data elements in the Consent document **SHALL** be consistent with the value in the Consent document.

[SP-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 optionally a Body as an enclosed PDF (e.g. with a wet signature).

[SP-049] - Any update to the expression of this consent (opt-out or opt-in) **SHALL** result in the Privacy Content Creator to replace the associated Privacy Consent Document as specified by IHE Basic Patient Privacy Consent Profile.

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

[SP-050] - Document Repository and Document Registry Actor **SHALL** act as an Integrated Document Repository and Document Registry Actor to support the XDS Basic Patient Privacy Consent Enforcement action access control of the following policies:

- [SP-051] – Default Opt-In Policy. The access control matrix specified in Appendix B table B-1 **SHALL** be enforced.
- [SP-052] - Opt-Out Policy. The access control matrix specified in Appendix B table B-2 **SHALL** be enforced.
- [SP-053] - Opt-In after Opt-Out Policy. The access control matrix specified in Appendix B section B-2 **SHALL** be enforced.

3.7 REQUIREMENTS FOR BASIC PATIENT PRIVACY ENFORCEMENT

3.7.1 Basic Patient Privacy Enforcement on XDS Document Repositories and Registries

[SP-060] - The requirement identified by the IHE XDS Profile for a Document Source Actor **SHALL** be applied to the XDS Document Repository and Registry actors specified by IS0102 *Saudi eHealth Document Sharing Interoperability Specification*.

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
IS0200 Saudi Health Information Exchange Data Dictionary.	Specifies the interoperability standards and profiles along with the Saudi specific constraints that are required to provide the technical security measures, data protection, and privacy management that will facilitate the implementation of the Saudi eHealth Policies for Health Information Exchange in the Kingdom of Saudi Arabia among communicating IT systems.
Saudi Health Information Exchange Policies	Contains the policies and supporting definitions that support the security and privacy aspects of the Saudi Health Information Exchange. The Saudi Health Information Exchange Policies apply to all individuals and organizations that have access to the Saudi Health Information Exchange managed health records, including those connected to the Saudi Health Information Exchange, their Business Associates, as well as any subcontractors of Business Associates. These policies apply to all information provided to or retrieved from the Saudi Health Information Exchange.

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 http://www.ihe.net/Technical_Frameworks/#iti
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 http://www.ihe.net/Technical_Frameworks/#iti

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 http://www.ihe.net/Technical_Frameworks/#iti
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 describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. EHR systems). May be obtained at http://www.ihe.net/Technical_Frameworks/#iti
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

1. APPENDIX A – SAMPLE BPPC CONSENT DOCUMENT

1.1 SAMPLE

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

1.2 SAMPLE

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

2. APPENDIX B – ACCESS CONTROL DECISION MATRICES

The following matrix provides the access control decisions per the Saudi health 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 Saudi Health Information Exchange Policies See Section 1.5. This matrix is integral to supporting the Saudi Opt-In policy and the situations when the subject of care has not yet elected to Opt-Out. This policy is identified by the following OID (Object Identifier):
2.16.840.1.113883.3.3731.1.0101.01

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

The following matrix provides the access control decisions per the Saudi 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 Saudi Opt-Out policy identified by the following OID (Object Identifier):
2.16.840.1.113883.3.3731.1.0101.02

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

**There is no concept of physician designated with extended care coordination responsibilities and privileges by a patient (physician of trust, gate keeper, etc.) in Saudi Arabia.