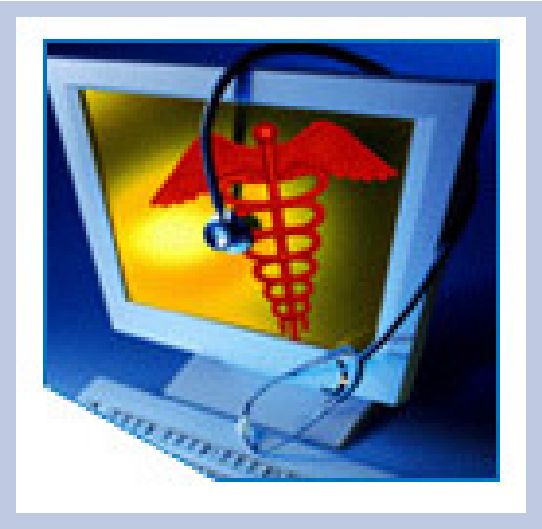
August 27, 2008
Version 1.2

HITSP Manage Consent Directives Transaction Package

HITSP/TP30



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	July 20, 2007
1.0.1	Review Copy	Security and Privacy Technical Committee	October 5, 2007
1.1	Released for Implementation	Security and Privacy Technical Committee	October 15, 2007
1.1.1	Review Copy	Security, Privacy and Infrastructure DomainTechnical Committee	August 20, 2008
1.2	Released for Implementation	Security, Privacy and Infrastructure DomainTechnical Committee	August 27, 2008

TABLE OF CONTENTS

1.0 INTRODUCTION 6

1.1 Overview 6

1.2 Transaction Package Document Map 6

1.3 Copyright Permissions 7

1.4 Reference Documents 8

2.0 TRANSACTION PACKAGE DEFINITION 10

2.1 Context Overview 10

2.1.1 Transaction Package Constraints 11

2.1.2 Technical Actors 12

2.1.3 Actor Interactions 13

2.1.3.1 Capture Consent Directive Transaction 14

2.1.3.1.1 Example Scenario: Create Consent Directive 15

2.1.3.1.2 Example Scenario: Update an Existing Consent Directive 16

2.1.3.2 Request Consent Directive Transaction 17

2.1.4 Pre-conditions 18

2.1.4.1 Process Triggers 19

2.1.5 Post-conditions 19

2.1.5.1 Required Outputs 19

2.1.6 Data Flows 20

2.2 List of Constructs 20

2.2.1 Construct Dependencies 20

2.2.2 Additional Constraints on Required Constructs 21

2.3 Standards 21

2.3.1 Regulatory Guidance 22

2.3.2 Selected Standards 22

2.3.3 Informative Reference Standards 23

3.0 TECHNICAL IMPLEMENTATION 25

3.1 Conformance 25

3.1.1 Conformance Criteria 25

3.1.2 Conformance Scoping, Subsetting and Options 25

4.0 APPENDIX 26

4.1 Consent Directives Concepts 26

5.0 CHANGE HISTORY 29

5.1 October 5, 2007 29

5.2 October 15, 2007 29

5.3 July 11, 2008 29
5.4 August 20, 2008 30
5.5 August 27, 2008 30

FIGURES AND TABLES

Figure 1.2-1 Transaction Package Document Map 7
Figure 2.1.3-1 Manage Consent Directive High Level Sequence Diagram 14
Figure 2.1.3.1-1 Capture Consent Directive 15
Figure 2.1.3.2-1 Request Consent Directive 18
Figure 4.1-1 Consent Directives Concepts 28

Table 1.4-1 Reference Documents 8
Table 2.1.1-1 Transaction Package Constraints 12
Table 2.1.2-1 Technical Actors 12
Table 2.1.4-1 Pre-conditions 19
Table 2.1.4.1-1 Process Triggers 19
Table 2.1.5-1 Post-conditions 19
Table 2.1.5.1-1 Required Outputs 20
Table 2.2-1 List of Constructs 20
Table 2.2.1-1 Construct Dependencies 20
Table 2.2.2-1 Additional Constraints on Required Constructs 21
Table 2.3.1-1 Regulatory Guidance 22
Table 2.3.2-1 Selected Standards 22
Table 2.3.3-1 Informative Reference Standards 23

1.0 INTRODUCTION

As an introduction to the HITSP Manage Consent Directives Transaction Package, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for this specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Transaction Package Definition.

1.1 OVERVIEW

This section describes the contents of this specification and provides a high level definition of this Transaction Package and background information about the underlying Transactions and Components that the Transaction Package is based on.

The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use, or disclose **Individually Identifiable Health Information (IIHI)**, and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 Manage Sharing of Documents. The registry that manages the consents may very well be different from the registry which manages the clinical documents; therefore the consents are not always managed in the same place as the clinical documents.

A consent directive is a record of a healthcare consumer's privacy policy, which is in accordance with governing jurisdictional and organization privacy policies that grant or withhold consent:

- To one or more identified entities in a defined role
- To perform one or more operations (e.g., collect, access, use, disclose, amend, or delete)
- On an instance or type of IIHI
- For a purpose such as treatment, payment, operations, research, public health, quality measures, health status evaluation by third parties, or marketing
- Under certain conditions, e.g., when unconscious
- For specified time period, e.g. effective and expiration dates
- In certain context, e.g., in an emergency

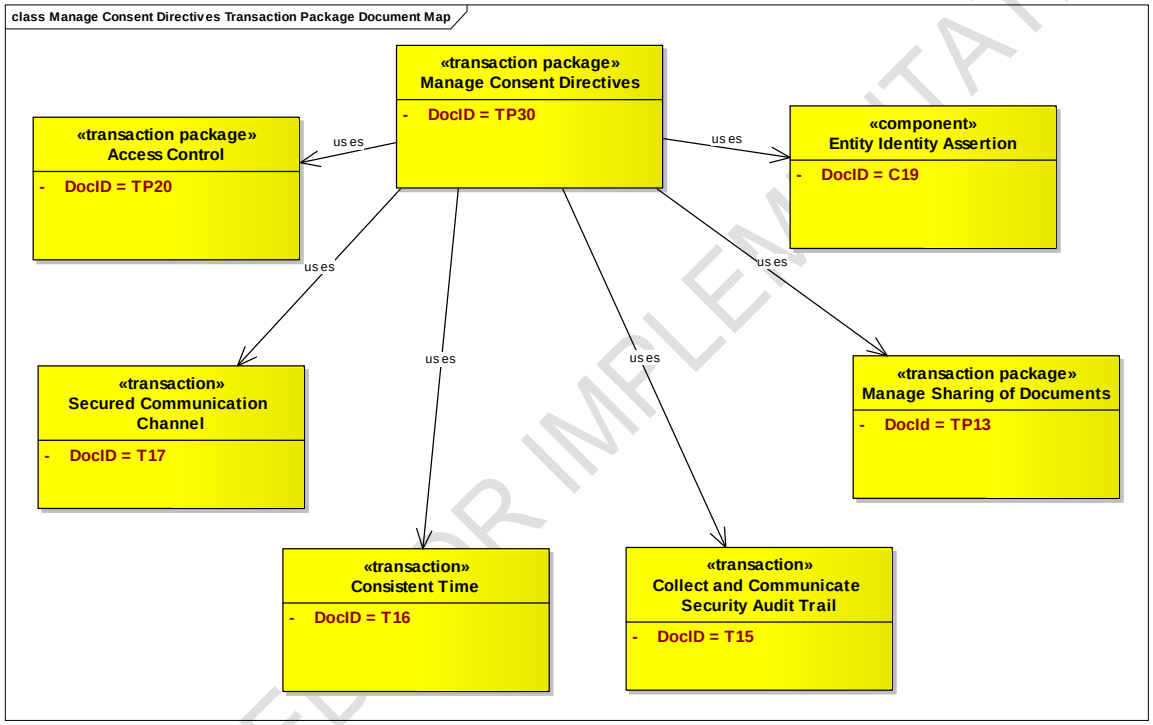
A consent directive is an instance of governing jurisdictional and organization privacy policies, which may or may not be backed up by a signed document (paper or electronic).

1.2 TRANSACTION PACKAGE DOCUMENT MAP

Each HITSP specification describes a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications that will satisfy the requirements for the HITSP construct. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). Interoperability Specifications define the

context(s) in which any other HITSP construct may be used. The current Manage Consent Directives Transaction Package specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 Interoperability Specification Document Map from the relevant IS to better understand the context, dependencies, and relationships between the constructs used to meet the IS requirements. The Document Map in Figure 1.2-1 depicts how this construct integrates and constrains HITSP constructs to support the information exchange, within the defined context of this document. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

Figure 1.2-1 Transaction Package Document Map



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

Certain materials contained in this Interoperability Specification are reproduced from Consent related vocabulary including Confidentiality Codes with permission of Health Level Seven, Inc. No part of the material may be copied or reproduced in any form outside of the Interoperability Specification documents, including an electronic retrieval system, or made available on the Internet without the prior written permission of Health Level Seven, Inc. Copies of standards included in this Interoperability Specification

may be purchased from the Health Level Seven, Inc. Material drawn from these standards is credited where used.

IHE materials used in this document have been extracted from relevant copyrighted materials with permission of Integrating the Healthcare Enterprise (IHE) International. Copies of this standard may be retrieved from the IHE Web Site at www.ihe.net.

1.4 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from the www.hitsp.org Web Site.

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built

Reference Document	Document Description
TN900 - Security and Privacy Technical Note	Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following: • The scope, reference policy background, and Security and Privacy principles used in the development of the constructs • A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs • A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases • A list of identified gaps and the recommended approaches to resolving those gaps • A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications • A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management • A glossary of terms used in all the Security and Privacy construct documents • A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.

2.0 TRANSACTION PACKAGE DEFINITION

Transaction Packages define how two or more transactions are used to support a stand-alone information exchange within a defined context between two or more systems.

2.1 CONTEXT OVERVIEW

This section provides a general description of the Transaction Package. It includes a detailed definition of the Transaction Package and the reason for its use. It also provides all the necessary background information that further describes the context in which the Transaction Package is needed, and the independent Transactions and Components that the Transaction Package is based on.

A consent directive is the record of a healthcare consumer's privacy policy that grants or withholds consent. A healthcare consumer may have zero to many consent directives per zero to many governing jurisdictional and organization policy sets. Consent directives may grant or withhold consent. Multiple consent directives may exist for the same IIHI. However, within the context of a specific patient and IIHI, if there are conflicting consent directives, it is strongly encouraged that they be detected and resolved per existing policy. A consent directive may be created, revised, or revoked. The consent directive concepts used by this construct are described in further detail in Section 4.1 of the Appendix.

An example of this capability would be electronic mechanisms for capturing and enforcing a restriction placed on the disclosure of a laboratory result for substance use under 42 CFR Part 2. In accordance with this federal statute which governs disclosure of IIHI generated by federally funded Substance Use Programs, a healthcare consumer has the right to invoke a consent directive and an IIHI source actor authorized to persist the consumer's IIHI (i.e., a federally funded Substance Use provider) is required to associate the applicable consent directive rules. Using the HITSP Manage Consent Directives Transaction Package, the IIHI is associated with these rules either as pointers to the location of the applicable consent directive and/or as confidentiality codes encoding the consent directives rules. An IIHI requester would be provisioned with the IIHI by a Security Access Control Service only in accordance with the applicable consent directive rules.

It is beyond the scope of HITSP to develop or select policies. The work of this construct supports the capturing and enabling of policies. Refer to the HITSP/TN900 document for a further discussion on policy, and the security and privacy principles used in the development of the construct.

The transactions described in this construct are intended to be carried out by HITSP/TP13 - Manage Sharing of Documents. The registry that manages the consents may very well be different from the registry which manages the clinical documents; therefore the consents are not always managed in the same place as clinical documents.

The following are the requirements derived from the AHIC Use Cases for the HITSP Manage Consent Directives Transaction Package construct:

1. Patient consent directives are captured electronically in a consent repository
2. Patient consent is withdrawn and that withdrawal is captured in a repository
3. Patient consent is revoked and that revocation is captured in a repository
4. Patient consent directives are transmitted to a Requester
5. Processing of patient consent directives is logged in audit trail

This Transaction Package utilizes the document content profile defined in the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Basic Patient Privacy Consents (BPPC) Content Profile (IHE-ITI-TF BPPC*)*. The BPPC content allows for the capturing of the patient acknowledgement to simple privacy domain policy. This BPPC content is managed using HITSP/TP13 - Manage Sharing of Documents. The BPPC content is very simple and supports only a pre-negotiated set of policies. This constraint is recognized as a gap, and there is work ongoing in the standards organizations (HL7, ISO TC215, and OASIS) to fill these gaps. HITSP expects to modify this construct as the standards organizations fill in the gaps.

The HITSP/TP13 – Manage Sharing of Documents used the Integrating the Healthcare Enterprise (IHE) Cross Enterprise Document Sharing (XDS) Integration Profile. The previous XDS Integration Profile[1] is now referred to as XDS.a, but remains technically without any change to the original XDS. The current XDS Integration Profile[2], referred to as XDS.b, employs different versions of OASIS eXtensible Markup Language (ebXML) Registry (versions 2.0 and 3.0), and specifications that have been superseded (like OASIS Web Services Security SOAP Messages with Attachments (SwA)). XDS.b introduces the new Patient Identity Feed HL7v3 transaction, in addition to the existing Patient Identity Feed [ITI-8] transaction based on HL7v2.

The BPPC profile calls upon and uses the Health Level 7 (HL7) Consent related vocabulary, including Confidentiality Codes, to provide information about permission directives to access, collect use and/or disclose IIHI; HL7 Permission Catalogue vocabulary that provides information to support access control decisions and enforcement; and HL7 Privacy Consent related specifications, including the Data Consent Revised Message Information Model (RMIM), to capture data an associations needed to record and convey consent directives. These standards provide access control information supporting access control decision and enforcement functions.

2.1.1 TRANSACTION PACKAGE CONSTRAINTS

This section describes the constraints that limit the context in which the Transaction Package construct may be used. A constraint describes a rule that limits the use of the actors, actions or data

[1] Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF), Volume 1, Revision 4.0, Section 10.

[2] Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007-2008 XDS.b.

within the given context, or to which the interactions must conform to be used within the described context. It is a description of the limits and scope of the interactions and can describe actions or events that are not part of the initial definition for the context.

Table 2.1.1-1 Transaction Package Constraints

Constraint
Constrained to support an IHE XDS document-centric architecture as described in HITSP/TP13 - Manage Sharing of Documents

The constraint to support IHE XDS document-centric architecture is necessary to support existing requirements at the time of publication. The HITSP/TP13 construct supports the implementation of one or more of the following:

- XDS.a: Management of Document Sharing within a community according to IHE XDS.a
- XDS.b: Functionally equivalent to XDS.a but with additional support for most recent Web Services standards
- XCA: Management of Cross-Community Access according to IHE XCA, to address the requirement for federating two or more communities

This constraint will continue to be reevaluated and may be expanded in the future as additional architectures are required to be supported.

2.1.2 TECHNICAL ACTORS

This section describes the technical actors that need to be integrated in order to meet the interoperability requirements for this Transaction Package. A Technical Actor represents an entity internal to a software application, which is engaged in one or more specific transactions to support a specific aspect of a real world information interchange (e.g. set of message exchanges). The table below lists the technical actors involved the relevant definition of their roles, and an indication of their requirements for the Transaction Package.

Table 2.1.2-1 Technical Actors

Technical Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Consent Originator	The Consent Originator captures consent directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry	IHE-ITI-TF-2 XDS.a IHE-ITI-TF-2 XDS.b IHE-ITI-TF-2 XCA	R

Technical Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Consent Repository	The Consent Repository is responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point	IHE-ITI-TF-2 XDS.a IHE-ITI-TF-2 XDS.b IHE-ITI-TF-2 XCA	R
Consent Registry	The Consent Registry is responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a *Manage Consent Directive Metadata Request*	IHE-ITI-TF-2 XDS.a IHE-ITI-TF-2 XDS.b IHE-ITI-TF-2 XCA	R
Consent Directive Requestor	The Consent Directive Requester accesses Consent Directives located through a Consent Registry from Consent Repositories	IHE-ITI-TF-2 XDS.a IHE-ITI-TF-2 XDS.b IHE-ITI-TF-2 XCA	R
Consenter	The Consenter is an individual consumer of healthcare services or a consumer delegate that selects a Consent Originator to capture and manage the consumer's consent directives so that these can be associated with personal health information. When a Consent Originator captures a consent directive request, it can issue a Resolve Consent Directive Request to the Consenter to resolve an apparent conflict between a proposed consent directive and a current consent directive. The Consenter sends a *Resolve Consent Directive Response* either modifying the consent directive or confirming that the conflict is an intended update of a current consent directive	IHE-ITI-TF-2 XDS.a IHE-ITI-TF-2 XDS.b IHE-ITI-TF-2 XCA	R

2.1.3 ACTOR INTERACTIONS

This section uses a UML workflow diagram to depict the business and technical actors, the relevant events or actions in which they are involved, and a mapping to the Transactions, and Components that encapsulate the defined events/actions. It describes the underlying events that fulfill the Transaction Package, the sequence and timing of the events, and the specific actors involved. Process flow diagrams are also provided to illustrate the process relationships. A description of the UML diagram is also provided below the diagram.

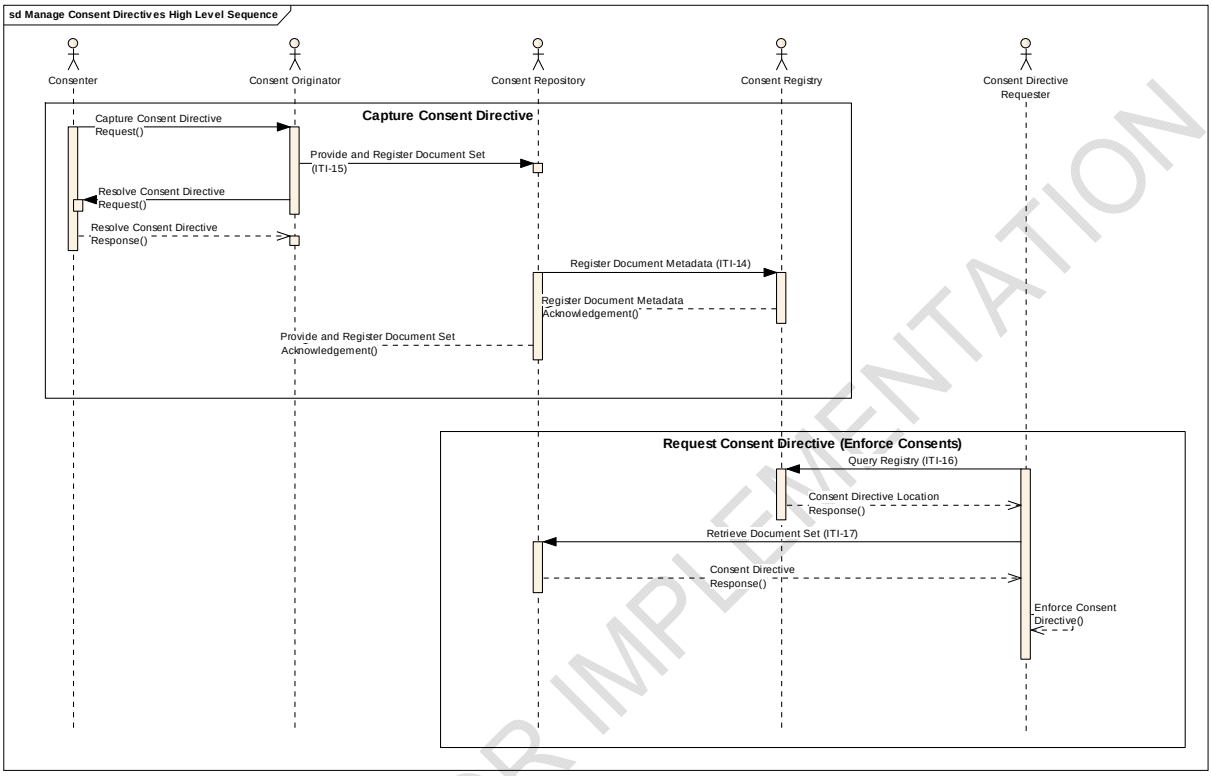
The HITSP Manage Consent Directives Transaction Package contains the following transactions which are shown in a high level sequence diagram in Figure 2.1.3-1, and further described in the sections below:

- Capture Consent Directive
- Request Consent Directive

These transactions are intended to be carried out by the HITSP/TP13 - Manage Document Sharing construct. The registry that manages the consents may very well be different from the registry

which manages the clinical documents; therefore the consents are not always managed in the same place as the clinical documents.

Figure 2.1.3-1 Manage Consent Directive High Level Sequence Diagram



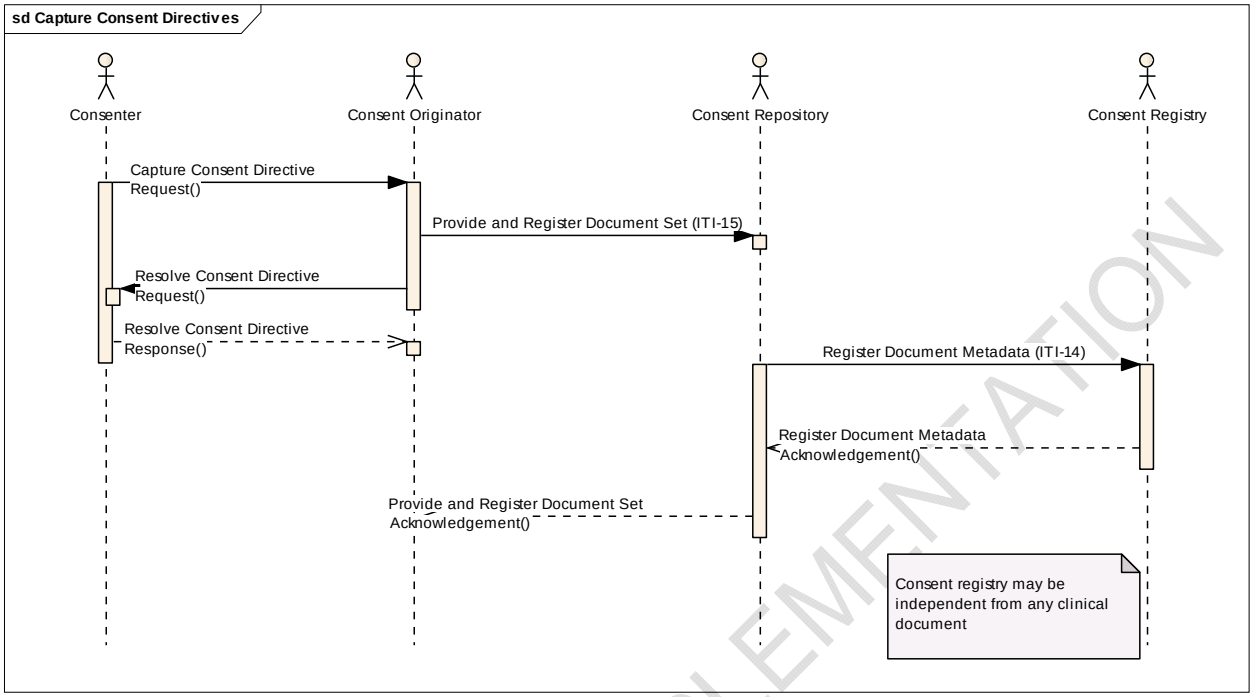
2.1.3.1 Capture Consent Directive Transaction

The Capture Consent Directive Transaction includes the following components:

- Create a new consent directive: This component is triggered when a Consenter establishes a new consent directive
- Update an existing consent directive: This component is triggered when a Consenter updates or revises a Consent Directive based on a request from an IIHI requester who may or may not have previously requested IIHI
- Revoke an existing consent directive: This component is triggered when a Consenter terminates an existing consent directive

Further detail is shown for the Capture Consent Directive transaction in Figure 2.1.3.1-1.

Figure 2.1.3.1-1 Capture Consent Directive



This transaction is carried out by HITSP/TP13. The IHE XDS transactions Provide and Register Document Set (ITI-15) and Register Document Metadata (ITI-14) are used in the Capture Consent Directive transaction. Note that the registry that manages the consents may very well be different from the registry which manages the clinical documents; therefore the consents are not always managed in the same place as the clinical documents.

The sections below illustrate example scenarios of the Capture Consent Directives workflow: Create Consent Directive, and Update Consent Directive.

2.1.3.1.1 Example Scenario: Create Consent Directive

The following scenario is an example of the creation of a consent directive based on the Capture Consent Directive transaction described above. Additional descriptions of key Consent Directives concepts are provided in Appendix 4.

In this example, the Capture Consent Directive transaction is triggered when a Consent Originator sends a Capture Consent Directive to capture a new, a revised (general or ad hoc), or a deleted Consent Directive that a Consenter has issued (using, for example, a consumer assistive Graphical User Interface (GUI)). In this scenario, only Consent Directives in accordance with applicable jurisdictional or organizational privacy policies may be entered. Control over the appropriate Consent Directives based on applicable jurisdictional or organizational privacy policies can be enforced through the GUI.

The Consent Originator forwards the new, revised, or deleted Consent Directive issued by the Consenter via a Manage Consent Directive Request message (Provide and Register Documents Set - ITI-15) to the Consent Repository specified by the Consenter. The Consenter specifies a Consent Repository and communicates this to the Consent Originator during the issuance of a Consent Directive (using, for example, a GUI), or at other times. If the Consent Directive is captured as structured data[3], the Consent Repository evaluates any new submission algorithmically against existing Consent Directives for inconsistencies. The evaluation involves the use of a well-defined, systematic set of instructions to perform the inconsistency validation. The Consent Repository will issue a Provide and Register Document Set Acknowledgement that can either:

- Confirm that no inconsistencies were found and the consent directive document metadata has been registered with the Consent Registry; or
- If inconsistency is detected, request information required for reconciliation via a Manage Consent Directive Response (utilizing the Provide and Register Document Set Acknowledgement)

If inconsistency is detected, the Consent Originator sends a Resolve Consent Directive Request to the Consenter. The Consenter sends a Resolve Consent Directive Response, which triggers the Consent Originator to resend a reconciled Manage Consent Directive Request. Otherwise, the Consent Repository will respond to the Consent Originator with an acceptance or rejection of the request based on the message conformance to required standards.

The Consent Repository sends a Manage Consent Metadata Request (Register Document Metadata – ITI-14) to the Consent Registry, which evaluates message conformance against specified standards for the Individually Identifiable Health Information (IIHI) requester's[4] Security Access Control Service. The Consent Registry sends an acceptance or rejection Manage Consent Metadata Response message (Register Document Metadata Acknowledgement) to the Consent Repository based on the message conformance to required standards. In the case of an update, the Consenter may request that the Consent Originator notify an IIHI requester that the Consent Directive has been updated.

2.1.3.1.2 Example Scenario: Update an Existing Consent Directive

The following scenario is an example of the update of a consent directive based on the Capture Consent Directive transaction described above. Additional descriptions of key Consent Directives concepts are provided in Appendix 4.

The Capture Consent Directive transaction is triggered when a Consenter updates a Consent Directive based on a request from an IIHI requester who may or may not have previously requested IIHI.

[3] Structured Data are coded, semantically interoperable data that are based on a reference information model. The Consent Directive may be captured as a scanned image, which is not semantically interoperable and would preclude the ability of the Consent Repository to analyze it for conflicts with previously persisted Consent Directives.

[4] IIHI includes Consent Directives, so there may be Consent Directives specifying users and uses of Consent Directives associated with IIHI.

The Consent Originator sends an Update Consent Directive to the Consent Repository via a Provide and Register Documents Set - ITI-15. The Consent Repository sends an Update Consent Directive Metadata (via a Register Document Metadata – ITI-14) to the Consent Registry. This Update Consent Directive Metadata includes the location(s) where IIHI about the Consenter resides. The location(s) information is derived from the IIHI Repository Location Notice (See Appendix 4). The Consent Registry sends an Update Consent Directive Metadata (via a Register Documents Metadata - ITI-14) to any IIHI Repository holding IIHI to which the updated Consent Directive applies. The IIHI Repository sends an Update Consent Directive Metadata to the IIHI Registry indexing IIHI to which the updated Consent Directive applies.

The Consenter may request that the Consent Originator notify an IIHI requester that the Consent Directive has been updated.

Note that one of the possible outcomes of an Update Consent Directive transaction is the revocation of an existing consent directive.

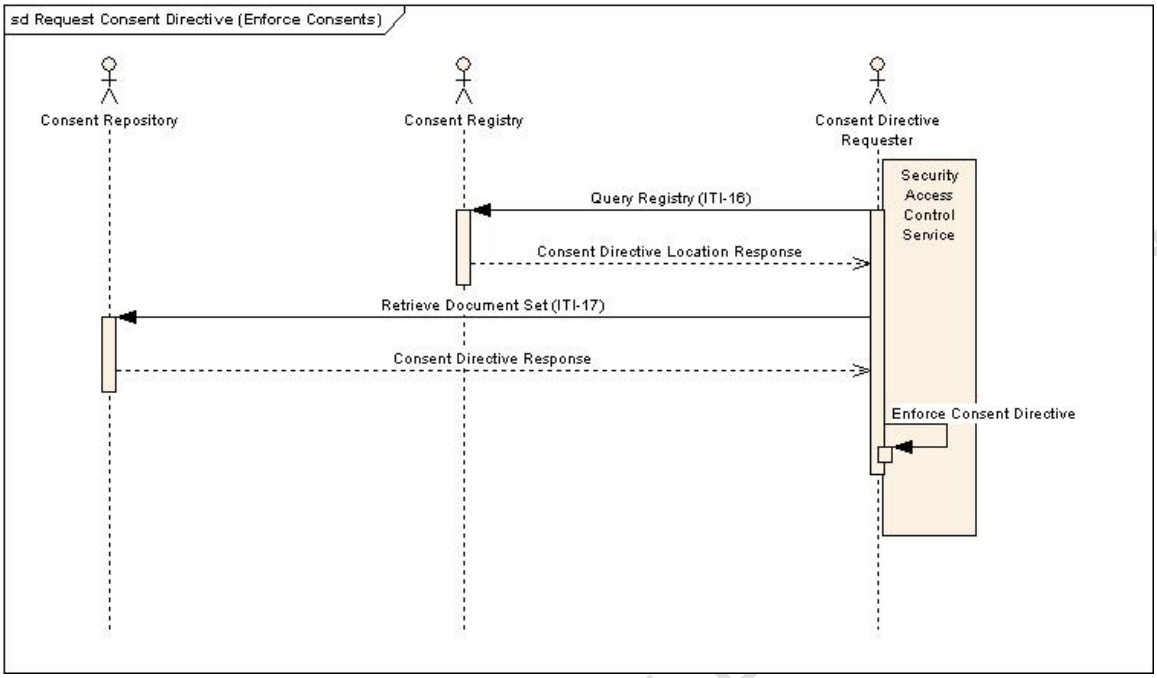
2.1.3.2 Request Consent Directive Transaction

The Request Consent Directive transaction is triggered when a Consent Directive Requester, such as a Security Access Control Service, searches for the applicable Consent Directive to apply to a request for individually identifiable health information.

This transaction is intended to be carried out by the HITSP/TP13 - Manage Document Sharing construct. The registry that manages the consents may very well be different from the registry which manages the clinical documents; therefore the consents are not always managed in the same place as the clinical documents.

Further detail for the Request Consent Directive transaction is shown in Figure 2.1.3.2-1.

Figure 2.1.3.2-1 Request Consent Directive



The Consent Directive Requester sends a Consent Directive Location Request (Query Registry – ITI-16) to the Consent Registry. The Consent Registry may evaluate the request in accordance to its own Policies, or assume or confirm via other mechanisms that the Requester has authorization for access. The Consent Registry sends a Consent Directive Location Response that provides or denies provision of the Consent Directive Location.

If the Consent Directive Location is provided, the Consent Directive Requester sends a Consent Directive Request (Retrieve Document Set query – ITI-17) to the Consent Repository and receives a Consent Directive Response. The Security Access Control Service functions as the policy enforcement for the Consent Directive Requester by applying the Consent Directive rules about permitted users and uses to IIHI under its protection, including the Consent Directive itself.

2.1.4 PRE-CONDITIONS

This section describes the necessary conditions that must be in place prior to the start of the workings of the Transaction Package. The pre-conditions are used to convey any conditions that must be true at the outset of a Transaction Package. They describe the context that must be established before the Transaction Package is executed. They are not however the triggers that initiate the Transaction Package. Where one or more pre-conditions are not met, the behavior of the Transaction Package should be considered uncertain.

Table 2.1.4-1 Pre-conditions

Pre-condition
Consistent Time construct is a pre-requisite for this Transaction Package
Secure Nodes is a pre-condition to this Transaction Package
A policy exists defining what is to be audited
Audit record source is initialized to the audit policy
Audit record repository is active and designated as the destination for recorded audit events
Policy exists defining the protection of the log and audit exists is being enforced
Identities are managed (by a HITSP construct, or through an out of band agreement, or local administration)
Consenter must have an account with a Consent Originator (for Capture Consent Directive transaction)
All preconditions that are specified in the IHE BPPC specification

2.1.4.1 Process Triggers

This section describes the process triggers, including actors and/or processes, which are necessary to start the Transaction Package. They can invoke an automatic or manual process or result that in turn starts off the Transaction Package. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

Table 2.1.4.1-1 Process Triggers

Process Trigger
Consent Originator captures or updates a consent directive (for Capture Consent Directive transaction)
Consent Directive Requester searches for the applicable Consent Directive to apply to a request for personal health information (for Request Consent Direct transaction)

2.1.5 POST-CONDITIONS

This section provides an overview of the post-conditions or results that must occur at the end of the Transaction Package in order for the Transaction Package to be deemed successfully completed. This includes any required outputs from the Transaction Package, or specific actor states.

Table 2.1.5-1 Post-conditions

Post-condition (for each transaction from Figure 2.1.3-1)
Consent Directive is captured/updated (Capture Consent Directives transaction)
Consent Directives are evaluated to obtain confidentiality codes which are subsequently associated with IIHI as Metadata (Request Consent Directive transaction)

2.1.5.1 Required Outputs

This section identifies the required outputs that must be produced at the end of the Transaction Package in order for the Transaction Package to be deemed successfully completed. This includes the format and usage of the required output.

Table 2.1.5.1-1 Required Outputs

Required Output	Format/Usage
A record of new/updated consent directives is available (Capture Consent Directives transaction)	
A security audit event is generated	As specified in HITSP/T15
Consent Directive Location is provided (or denied) (Request Consent Directive transaction)	
Consent Directive is provided (or denied) (Request Consent Directive transaction)	

2.1.6 DATA FLOWS

This section describes the basic data flows that are supported by this Transaction Package. It also describes the format of the data, the data sources, and the relevant actors involved in the successful flow of data for the Transaction Package. Any prevailing pre and post-conditions are identified, as well as the purpose of each data post-condition associated with each Transaction Package. Any data that need to be made available to particular actors are highlighted, as well as the conditions and processes that will use the data to achieve the stated post-conditions.

Data flows are illustrated in the transaction diagrams above.

2.2 LIST OF CONSTRUCTS

The following list of constructs and their definitions are used by the Transaction Package specification.

Table 2.2-1 List of Constructs

Construct Name	Description	Event/Action Code	Content
No additional HITSP constructs are used other than those shown in Section 2.2.1 as dependencies			

2.2.1 CONSTRUCT DEPENDENCIES

The following table shows a list of constructs with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific Transaction specification.

Table 2.2.1-1 Construct Dependencies

Construct	Depends On (Name of Component that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
HITSP/TP30 - Manage Consent Directives	HITSP/TP13 - Manage Sharing of Documents	General	Used to deploy consent directive, and to make IIHI requests with a consent directive

Construct	Depends On (Name of Component that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
HITSP/TP30 - Manage Consent Directives	HITSP/T17 - Secured Communication Channel	Pre-condition	Pre-requisite for Use Case
HITSP/TP30 - Manage Consent Directives	HITSP/T16 - Consistent Time	Pre-condition	Pre-requisite for Use Case
HITSP/TP30 - Manage Consent Directives	HITSP/T15 - Collect and Communicate Security Audit Trail	General	Used for audit requirements throughout execution of construct
HITSP/TP30 - Manage Consent Directives	HITSP/C19 - Entity Identity Assertion	Pre-requisite	Pre-requisite for Use Case The Entity Identity Assertion helps to ensure that an entity requesting a consent directive location or consent directives is the person or application that claims the identity provided
HITSP/TP30 - Manage Consent Directives	HITSP/TP20 - Access Control	Pre-requisite	Pre-requisite for Use Case The Access Control provides the mechanism to administer security authorizations which control the execution of consent directives

2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

This section describes the constraints that further limit the constructs that are used by this Transaction Package.

Table 2.2.2-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
Not applicable at this time				

2.3 STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. The standards used by this Transaction Package specification fall into the following categories:

- Regulatory guidance is a legal or other authoritative declaration that HITSP must abide by in standards selection (see Section 2.3.1)
- Selected standards are necessary for interoperability. These are standards that are used to meet information exchange requirements of associated constructs. For example, they are used to realize

direct information exchange, to provide the transport mechanism, to specify the content, or to address security (see Section 2.3.2)

- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Transaction Package specification (see Section 2.3.3)

2.3.1 REGULATORY GUIDANCE

The following table provides a list of legal or other authoritative guidelines that HITSP must abide by, or has agreed to use as guidance in the selection of standards. Note that only the referenced sections of the regulations are relevant to this Transaction Package specification.

Table 2.3.1-1 Regulatory Guidance

Standard	Description
No applicable regulatory standards	

2.3.2 SELECTED STANDARDS

The following table provides a list of standards that are used to meet information exchange requirements of the Transaction Package specification, and a detailed description of each standard.

Table 2.3.2-1 Selected Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. This supplement is available at www.ihe.net

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. This supplement is available at www.ihe.net
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	The Data Consent RMIM captures the data and associations needed to (1) record or report a consumer's consent or dissent to authorize the access, collection, use, or disclosure of personally identifiable information; (2) convey a provider's request or intent to override a patient's recorded consent or dissent; (3) convey a type of consent directive associated with a privacy policy; or (4) to record or report a consumer's consent directive, which is to be applied to future access, collection, use or disclosure of personally identifiable information. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	The Basic Patient Privacy Consents (BPPC) profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS 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. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Actors can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. The latest version of specification is available at www.ihe.net

It is important to note, with regards to the standards listed above, the approach of using Confidentiality Codes to encompass the entire range of possible consumer policies in a given jurisdiction would most likely not be effective for fine-grained privacy policy management. While IHE BPPC in its current version is the only standard solution to begin to meet the privacy requirements identified in the Use Cases evaluated, the industry should be aware that the management of consumer-selected, fine grained privacy policy is not satisfied by this standard, nor will this approach likely be sufficient to satisfy future Use Cases.

2.3.3 INFORMATIVE REFERENCE STANDARDS

The following table lists standards that provide additional background information or guidance; however, they are not required for the implementation of the Transaction Package specification.

Table 2.3.3-1 Informative Reference Standards

Standard Name	Description/Usage
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org

Standard Name	Description/Usage
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org

3.0 TECHNICAL IMPLEMENTATION

3.1 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

3.1.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also be constrained as specified in Table 2.1.1-1, and implement all of the required actors from Table 2.1.2-1, within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification with which this construct is associated.

3.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for actor scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.

4.0 APPENDIX

The following section includes relevant materials for this document.

4.1 CONSENT DIRECTIVES CONCEPTS

This section provides a comprehensive listing of the various components that form the basis of an Information Rights Policy.

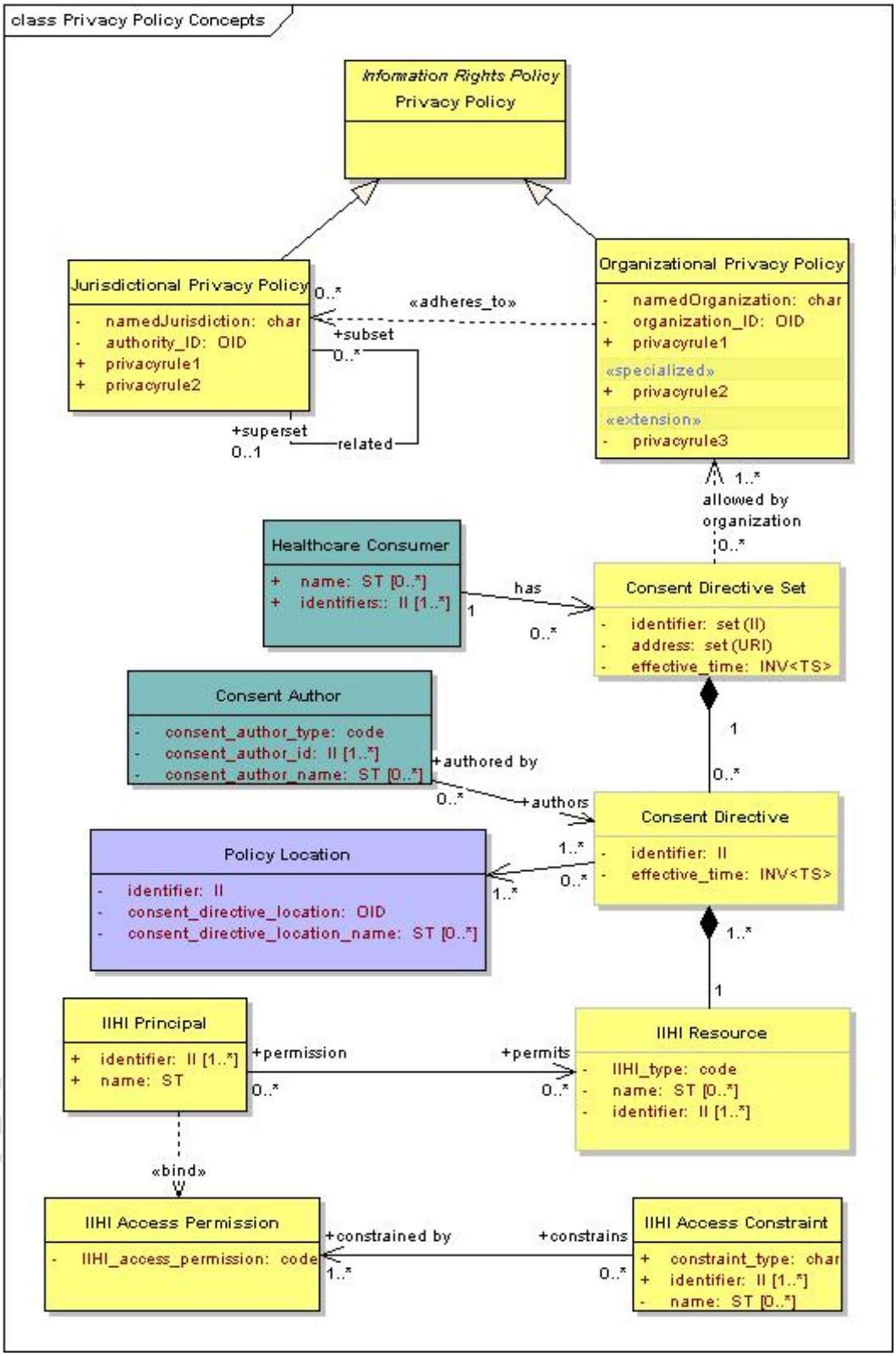
A Healthcare Consumer defines a Consent Directive Set, formed by one or more Consent Directives. The location of these Consent Directives is established in the Policy Location. Access to IIHI is defined by the IIHI Access Permissions and IIHI Access Constraints. The Consent Directive Set is allowed by Organizational Privacy Policy, which in turn is bound by the Jurisdictional Privacy Policy. The combination of all these interactions results in an overarching Information Rights Policy/Privacy Policy.

The entities involved in an Information Rights Policy are described below. Figure 4.1-1 further describes the relationship between these entities.

- Information Right Policy/Privacy Policy is the policy expression of a consumer consent directive
- Jurisdictional Privacy Policy is the privacy policy that is applicable within a specified jurisdiction
- Organizational Privacy Policy is the privacy policy that is applicable within a specified organization
- Healthcare Consumer is the individual establishing his/her personal consent directives (i.e. Consenter)
- Consent Directive Set is the combination of all consent directives within the facility domain
- Consent Directive is the record of a healthcare consumer's privacy policy that grants or withholds consent for:
    - one or more principals (identified entity or role)
    - performing one or more operations (e.g., collect, access, use, disclose, amend, or delete)
    - purposes such as Treatment, Payment, Operations, Research, Public Health, Quality Measures, Health Status Evaluation by third parties, or Marketing
    - certain conditions (e.g., when unconscious)
    - a specified time period (e.g., effective and expiry dates)
    - a certain context (e.g., in an emergency)
- Policy Location is the location (i.e., consent repository) where the consent directive resides
- IIHI Principal is the individual that is subject to the IIHI
- IIHI Resource is the resource in which IIHI resides
- IIHI Requester is the person or system requesting access to or disclosure of Individually Identifiable Health Information (IIHI) by an IIHI source or repository
- IIHI Repository Location Notice is a message containing the location(s) where IIHI about a consumer reside
- IIHI Access Permission is the ability to reach IIHI consistent with privacy policies and consent directives

- IIHI Access Constraint is the restriction or limitation imposed on a user of IIHI, based on consent directives and privacy policies

Figure 4.1-1 Consent Directives Concepts



5.0 CHANGE HISTORY

The following sections provide the history of all changes made to this document since the last publication.

5.1 OCTOBER 5, 2007

The changes in this cycle address the following comments received during the Public Comment and Inspection Testing period (July 23, 2006 - August 17, 2007):

272, 627, 631, 633, 635, 637, 638, 641, 644, 652, 716, 859, 861, 864, 866, 868, 871, 873, 878, 882, 883, 885, 888, 889, 893, 895, 905, 908, 909, 912, 914, 915, 917, 918, 919, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 984, 1197, 1198, 1199, 1200, 1201, 1229, 1231, 1232, 1233, 1244, 1245, 1246, 1247, 1250, 1251

The full text of the comments along with the Technical Committee's disposition can be reviewed on the HITSP Public Web Site.

5.2 OCTOBER 15, 2007

Upon approval by the HITSP Panel on October 15, 2007, this document has been moved to Version 1.1. This document is now Released for Implementation.

5.3 JULY 11, 2008

- Updated to place standards into 3 categories: Regulatory, Selected, and Informative References.
- Also clarified text surrounding transactions within the construct, as well as the examples provided to illustrate the transactions.
- Updated associated UML diagrams to align with transaction flow
- Added clarification on how standards listed in tables of standards are used within the construct.
- Added names of standards that were being referenced within specification, however, were mistakenly not being listed in the table of standards.
- Updated names/descriptions of HL7 v3 RBAC and Privacy Consent related specifications

5.4 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References.

The following standards have been added as Selected:

- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)
- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)
- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]
- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement
- Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent

The following standards have been designated as Informative Reference:

- Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes

The following standard was designated as Informative Reference and updated from:

- Health Level Seven (HL7) Healthcare Permissions Catalogue

to:

- Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008

5.5 AUGUST 27, 2008

Upon approval by the HITSP Panel on August 27, 2008, this document is now Released for Implementation.