August 27, 2008
Version 3.1

HITSP Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification

HITSP/IS03

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:
Consumer Perspective Technical Committee
(Formerly Consumer Empowerment Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Consumer Empowerment Technical Committee	September 7, 2006
1.1	Ready for Public Comment	Consumer Empowerment Technical Committee	September 12, 2006
1.2	Ready for Implementation Testing	Consumer Empowerment Technical Committee	October 20, 2006
2.0	Released for Implementation	Consumer Empowerment Technical Committee	May 11, 2007
2.0.1	Review Copy	Consumer Empowerment Technical Committee	September 18, 2007
2.0.2	Review Copy	Consumer Empowerment Technical Committee	December 5, 2007
3.0	Released for Implementation	Consumer Empowerment Technical Committee	December 13, 2007
3.0.1	Review Copy	Consumer Perspective Technical Committee	August 20, 2008
3.1	Released for Implementation	Consumer Perspective Technical Committee	August 27, 2008

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification, 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 the Interoperability 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 Interoperability Requirements.

1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

This section provides a high level definition of this Interoperability Specification and background information about the underlying Use Cases that it is based upon.

The HITSP Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification identifies a subset of the functional components of the healthcare enterprises and health information networks, called HITSP actors, and specifies their interactions in terms of a set of coordinated, standards based transactions. This document defines specific implementations of established standards intended to achieve integration goals that promote appropriate exchange of a consumer's personal health record information.

The HITSP Consumer Empowerment Use Case is the active involvement of consumers (i.e., individuals) in managing their healthcare and gaining the benefits of having their health information in a format easily accessible to them. This includes having a personal health record (PHR) system to track healthcare information, insurance, family history, medications, and other special conditions.

As part of a personal health record, this specification addresses several key areas: the patient's registration data and a healthcare summary including medication history, allergies, encounters, problems and conditions, immunizations, and key laboratory tests results.

A vital part of a personal health record is the registration information. A visit to the doctor or hospital frequently requires filling out multiple forms. These forms collect information such as name, address, insurance, medications, allergies, etc. When an individual requires laboratory work or other testing, the same information has to be collected again. A single electronic registration will make it easier for individuals to give their information and for clinicians to use it. Additionally, the consumer could update the information once and share it with all healthcare providers.

An electronic healthcare summary provides a set of key health related information at a point in time. It includes a medication history which provides the consumer with an updated list of all pertinent medications and allergies in an easily accessible format. Most individuals do not know the specific medications and exact dosages that have been prescribed to them, and often do not know their own

allergies. In addition, clinicians do not always have consistent prescription information about the same individual, nor do they have easy access to medication information directly from the consumer. Too often, this results in errors or unnecessary treatments. An electronic medication history would have all the current data available to the individual and to each authorized healthcare provider. The need for an electronic medication history was highlighted by the high interest in the KatrinaHealth.org web tool. A complete electronic medication list would also prevent drug-to-drug or allergic reactions when subsequent prescriptions are written. The consumer's healthcare summary should also include a list of allergies, encounters, identified conditions and problems diagnosed, the current list of immunizations, and laboratory test results as indications of the consumer's health status.

Traditionally, registration is viewed from the healthcare provider's perspective and consists of patient registration with the healthcare provider organization and the consumer giving their information to the healthcare provider. The concept of consumer empowerment creates a new perspective of healthcare providers and healthcare organizations that goes beyond traditional registration to provide the healthcare provider's contact and identification information to the consumer. This process of reciprocal registration and sharing of data are encouraged and facilitated by the Use Cases. It is desired, but not required or essential, that healthcare providers who register a patient should also enter their own information into the patient's registration summary. Ideally that would include contact information and the identifier, such as a medical record number, that the healthcare provider assigned to that patient. This will facilitate the PHR system to serve as a "Regional Health Information Organization (RHIO) of one" having all essential master patient index data and record locator data for a single patient.

This Interoperability Specification defines two types of interoperable documents. The first one is a registration and healthcare summary document and the second one is a laboratory report document (also used for the HITSP/IS01 Electronic Health Records Laboratory Results Reporting Interoperability Specification). One means to share these documents is by registering them in a record locator and retrieving them from the referenced document repository. Other types of interoperable documents may be defined by HITSP in the future such as radiology reports, images, electrocardiogram (ECG) reports, etc. These other types of documents are out of scope for the Use Cases presented to HITSP for consideration at this time.

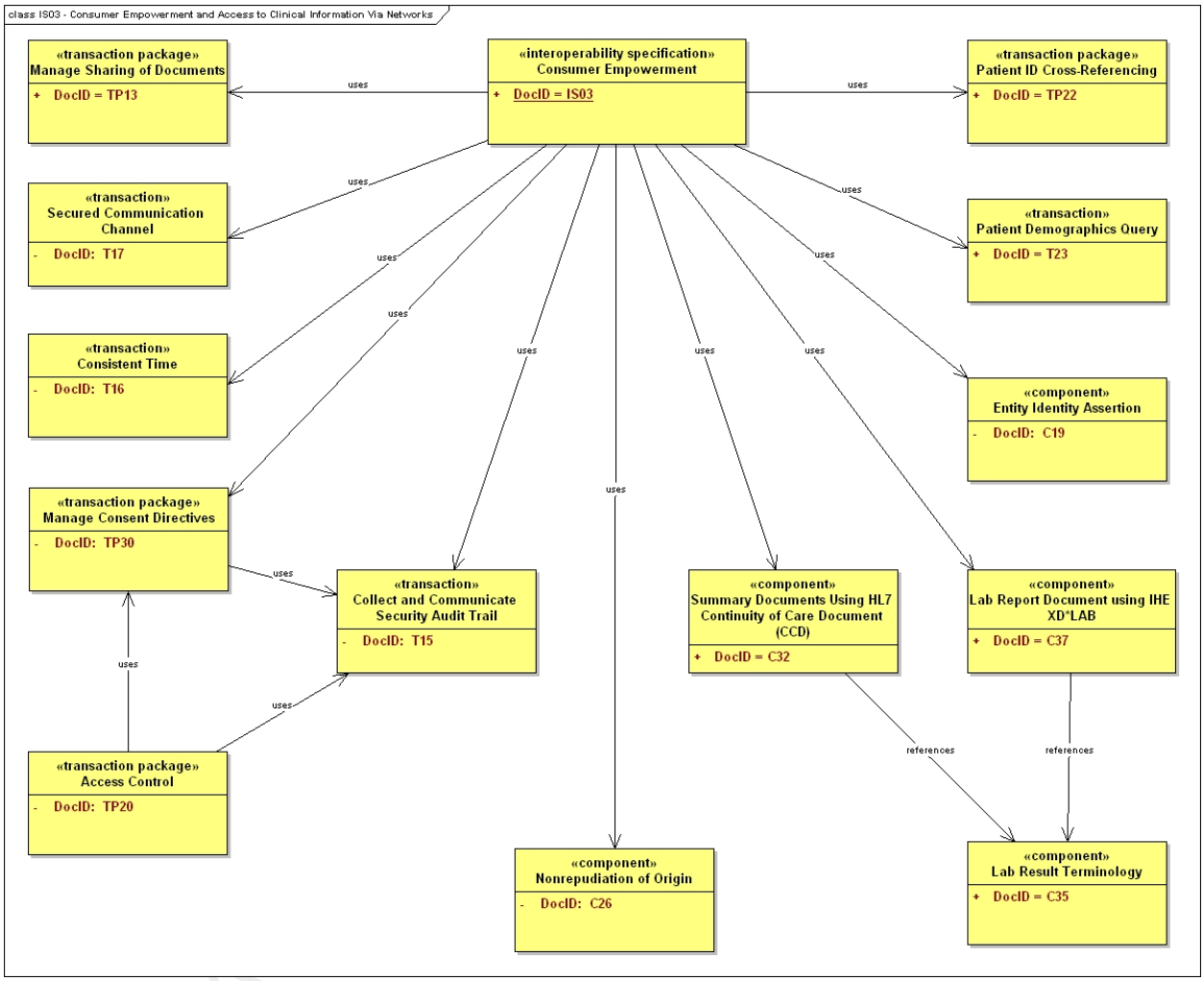
The interoperability requirements are based upon six well-defined scenarios related to a consumer's personal health record. This is the first document in a series of documents that need to be understood and implemented in order to conform to this specification.

1.2 INTEROPERABILITY SPECIFICATION DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant context(s) for the use of HITSP constructs that further identify and constrain standards where necessary. In addition to ISs, there are three other types of HITSP constructs called Transaction

Packages (TP), Transactions (T), and Components (C). The roadmap depicted in Figure 1.2-1 identifies the HITSP constructs used to meet the IS requirements. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

Figure 1.2-1 Interoperability Specification Document Map



1.2.1 LIST OF CONSTRUCTS

The following table lists and describes the HITSP constructs that are shown in the Unified Modeling Language (UML) diagram above and are used by the Interoperability Specification. All references to HITSP specifications are to the current and Panel approved versions of the specifications.

Table 1.2.1-1 List of Constructs

Construct	Description
HITSP/TP13 V2.0.1	HITSP Manage Sharing of Documents Transaction Package with Document Integrity Option

Construct	Description
HITSP/TP13 (provisional selection of XDS.b)	HITSP Manage Sharing of Documents Transaction Package with reference to the IHE XDS.b supplement to support Entity Identity Assertion (SAML support). See http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Supplement_XDS-2.pdf
HITSP/TP22	HITSP Patient ID Cross-Referencing Transaction Package
HITSP/T23	HITSP Patient Demographics Query Transaction
HITSP/C32	HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component
HITSP/C37	HITSP Lab Report Document Component
HITSP/C35	HITSP Lab Report Terminology Component
HITSP/T15	HITSP Collect and Communicate Security Audit Trail Transaction
HITSP/T16	HITSP Consistent Time Transaction
HITSP/T17	HITSP Secured Communication Channel Transaction
HITSP/TP20	HITSP Access Control Transaction Package
HITSP/TP30	HITSP Manage Consent Directives Transaction Package
HITSP/C19	HITSP Entity Identity Assertion Component
HITSP/C26	HITSP Nonrepudiation of Origin Component

1.3 COPYRIGHT PERMISSIONS

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.

This material includes SNOMED Clinical Terms® (SNOMED CT®) which is used by permission of the International Health Terminology Standards Development Organisation (IHTSDO). All rights reserved. SNOMED CT® was originally created by The College of American Pathologists.
"SNOMED" and "SNOMED CT" are registered trademarks of the IHTSDO.

OASIS materials used in this document have been extracted from relevant copyrighted materials with permission of the Organization for the Advancement of Structured Information Standards (OASIS). Copies of this standard are available from OASIS at www.oasis-open.org.

1.4 REFERENCE DOCUMENTS

This section contains links to key reference documents and background material.

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
Harmonized Use Case for Consumer Empowerment (Registration and Medication History), March 19, 2006 and the Consumer Access to Clinical Information Detailed Use Case, June 18, 2007	AHIC Use Case that is the basis of this Interoperability Specification.
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 INTEROPERABILITY REQUIREMENTS

This section provides a high level description of the Consumer Empowerment and the Consumer Access to Clinical Information Use Cases as well as the specific requirements that are extracted from each Use Case. It includes the following information:

- Mapping from the Use Case Requirements to the Derived Interoperability Requirements – this table lists the requirements grouped by actor for each event and related action
- Data Element Requirements – this table further describes the data requirements for each specified interoperability requirement and the business actor that is responsible for the data
- Business Actors – this table defines the business actors that are included for the Interoperability Specification
- High level Unified Modeling Language (UML) Business Sequence Diagrams – these diagrams are used to describe the interaction between the business actors, and the data involved in each scenario that is documented

2.1 USE CASE SYNOPSIS

This section provides a synopsis of the Consumer Empowerment and the Consumer Access to Clinical Information Use Cases, including any applicable scenarios that are part of the Use Cases.

The Consumer Empowerment and the Consumer Access to Clinical Information Use Cases identify the principal stakeholders and flow of events for the authorized and secure exchange of consumers' registration and healthcare summaries as well as laboratory reports. The Use Cases are not intended to define all system features; they identify and describe interactions between key systems and stakeholders and serve as a guide that leads to further development of functional requirements and other products. The Consumer Empowerment and the Consumer Access to Clinical Information Use Cases include:

- Querying other organizations for data and matching to the consumer
- Accepting "batch" data from other organizations and matching to the appropriate consumers
- Accessing, viewing, and sharing registration summaries and medication histories
- Ability for the consumer to retrieve, store, graph and share laboratory test results
- Ability for consumers to retrieve and store
  - lists of current and previous health conditions
  - lists of current medications, current environment, dietary, medication or medical supply allergies
  - a list of diagnosis codes
- The ability to access results, conditions, allergies, and diagnosis codes in layperson terms
- Ability to identify and maintain a list of all providers involved in the care of a specific patient, to use the provider list to communicate information about the patient to all or selected providers and forward the list of providers to another provider or entity

- Ability for a consumer to identify those providers which are permitted to access information in the consumers' PHR, and which of those data they are permitted to access and to communicate the consumer's decisions to other entities which also hold data about the consumer
- Ability for a consumer to request, consolidate, and access audit log information from multiple sources to create logical views of access to their information
- Ability to describe a consumer's access decisions using information which can be communicated among systems involved in information exchange

Based on the charge from the American Health Information Community, these Use Cases presume some level of linkage between a consumer's registration summary and their healthcare summary (e.g. medication history, allergies, encounters, and immunizations). This linkage is an important consideration for identifying and locating individual consumers and their available healthcare information across network systems. For the purposes of these Use Cases, the linking of a consumer's registration summary to the healthcare summary includes: (1) identity matching, (2) linkages between the data, (3) and the ability to incorporate both types of data simultaneously into a system (although they may come from different systems themselves). This linkage applies to including laboratory results in the healthcare summary or to sharing one or more laboratory reports as separate documents.

Certain parts of the most recent Use Case: Consumer Access to Clinical Information, have not yet been addressed by this Interoperability Specification. These gaps relate mostly to:

- Scenario 2: Provider Lists and permissions. It is important to note that this Interoperability Specification provides a level of Security and Privacy but not with the detailed control as expected in Scenario 2
- Scenario 3: Transfer of PHR Information. It is important to distinguish the transfer of PHR information on Networks, which is within the scope of this Interoperability Specification, from the transfer of PHR Information on portable media which is addresses by a companion Interoperability Specification, HITSP/IS05 - Consumer Empowerment and Access to Clinical Information via Media

These gaps relate to a number of more advanced interoperability capabilities that require the availability of standards under development. For a detailed discussion of these gaps, see Section 4.2.1.

2.2 USE CASE REQUIREMENTS

This section describes the Use Case requirements and outlines all the given scenarios at a high level.

This document specifies three scenario flows to satisfy the harmonized Use Cases:

1. **Consumer creates account to host and access registration summary and clinical information**
   This first scenario defines the flow for a consumer to create their account; obtain registration summary and healthcare summary data (including medication and other clinical data) and laboratory reports; access, view and generate new data through a PHR system.
   Important Note: This Scenario combines:

- *Scenario 1: Consumer creates account to host registration summary & medication history from the Consumer Empowerment Use Case (Events and Action starting with a number "2")*
- *Parts of Scenario 1: Consumers Receive and Access Clinical Information from the Consumer Access to Clinical Information Use Case (Events and Action starting with a number "6")*

Events and Actions as well as Perspectives from the two Use Cases have been matched as closely as possible, but as the two Use Cases are not aligned in their conventions and vocabulary, the "intent" of the Use Case has been preserved as well as possible.

2. Consumer visits healthcare provider and provides registration summary and clinical information

This second scenario defines the flow for a consumer to log onto their account, obtain registration summary and clinical data, allow a healthcare provider to review this data and update their EHR system.

Important Note: This Scenario combines:

- *Scenario 2: (Consumer visits healthcare provider and provides registration summary information from the Consumer Empowerment Use Case (Events and Action starting with a number "2")*
- *Parts of Scenario 1: Consumers Receive and Access Clinical Information from the Consumer Access to Clinical Information Use Case (Events and Action starting with a number "6")*

Events and Actions as well as Perspectives from the two Use Cases have been matched as closely as possible, but as the two Use Cases are not aligned in their conventions and vocabulary, the "intent" of the Use Case has been preserved as well as possible.

In addressing this second scenario, HITSP has ensured that the most up-to-date and complete information may be provided from the provider EHR systems back to the consumer PHR. Such an extension to the Consumer Empowerment Use Case is simply supported by recommending that at the end of a healthcare encounter the new registration/healthcare summary data are communicated to the PHR system (e.g. via a document repository/registry). This importance of such an extension is illustrated in this example:

> Mr. Everyperson is seen in the emergency department at a local hospital the night before a visit to Dr. Doctor. Dr. Doctor submits a new medication history request query, but there is an interval when MultiState Rx Plan has not yet processed the new medication (e.g. the night before) and published it to GM-HIN. If the emergency department did not send the information to the repository, Dr. Doctor would not have access to that information unless Mr. Everyperson enters the data into their WebPHR. Dr. Doctor's query would also not display any medications administered by the emergency department.

It is the intent of this specification to allow for a complete, up-to-date, relevant registration and/or medication (or other clinical and laboratory data) summary but it is not guaranteed by this specification (policies and appropriate applications are needed).

3. **Authorized Healthcare Provider reviews registration summary and clinical information**

This third scenario defines the flow for a consumer to log onto their account, obtain registration summary and clinical and laboratory data, allow a healthcare provider to review this data.

Important Note: This Scenario combines:

- *Scenario 3: Authorized Healthcare Provider reviews medication history from the Consumer Empowerment Use Case (Events and Action starting with a number "2.")*
- *Parts of Scenario 1: Consumers Receive and Access Clinical Information from the Consumer Access to Clinical Information Use Case (Events and Action starting with a number "6.").*

Events and Actions as well as Perspectives from the two Use Cases have been matched as closely as possible, but as the two Use Cases are not aligned in their conventions and vocabulary, the "intent" of the Use Case has been preserved as best as possible.

2.2.1 MAPPING OF USE CASE REQUIREMENTS TO INTEROPERABILITY REQUIREMENTS

This section contains an extraction of business actors, required interactions and conditions/scenarios from the Use Case into a matrix/table and an associated UML diagram.

Consumer Empowerment and Access to Clinical Information Use Cases – Scenario 1: Consumer Creates Account to Host and Access Registration Summary and Clinical Information

Table 2.2.1-1 Mapping of Use Case Requirements to Interoperability Requirements

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Consumer and PHR Service Provider	Event 6.1.1 Identify PHR of Choice Event 2.1.1 Select a provider of PHR Services	Action 6.1.1.1 Identify and communicate PHR of choice Action 2.1.1.1 Provide identification data	Identification of PHR Service / PHR instance {PHR Location-Gap} Identification of Consumer (Target of PHR) {Registry Patient Id/Id Domain OID} Authentication of Consumer-to-PHR-Service-Provider / Information Exchange-Leverage Entity Identity Assertion HITSP C19 {Authenticate Consumers-Partial Gap} Identification of providers -Leverage Entity Identity Assertion HITSP C19 {Partial Gap} Identification of Information Sources	9, 10, 11
		Event 2.2.1 Create account	Action 2.2.1.1 Confirm consumer's identity	Policies and internal PHR systems operation	
			Action 2.2.1.2 Create consumer's account	Internal PHR systems operation	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
			Action 2.2.1.3 Maintain consumer's permissions for system access	Internal PHR systems operation Manage Consent Directives	
		Event 2.2.2 Gather registration and/or medication data Event 6.1.3 PHR(s) receive available information from other sources	Action 2.2.2.1 Receive consumer request	Internal PHR systems operation	
			Action 2.2.2.2 Confirm consumer identity	Internal PHR systems operation plus policies	
			Action 2.2.2.3 Transmit request for registration / medication data to data or network system	Request for relevant records/documents/information	3
			Action 6.1.3.1 Receive Information Action 2.2.2.4 Receive registration / medication data	Standardized information {direct reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9,
			Action 2.2.2.5 Acknowledge receipt of registration / medication data	Request/response.	
			Action 6.1.3.2 Information is automatically populated for viewing using appropriate translations or transformations	Structured information {reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document} Translate to lay person terminology {Consumer-friendly sub task} The consumer receives personal information about his or her health from a healthcare provider. The information could be in the form of a laboratory test result, for example. The information may contain a term with which the consumer is not familiar, or about which the consumer wishes to learn more. The PHR application may provide a mechanism where the consumer clicks a button in the interface to request more information about a term. A multi-term query is created and transmitted to one or more Health Information Resource	1, 2, 4, 5, 10, 12

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				providers, with which the PHR Service Provider or the Consumer may have a business relationship	
			Action 2.2.2.6 Log interaction	Collect and communicate secured audit trail	
		Event 2.1.4 View registration/medication data Event 6.1.4 Access available information	Action 2.1.4.1 Authenticate to system	(PHR application functionality) plus policies	
			Action 6.1.4.1 Request information Action 2.1.4.2 Request data Action 2.1.4.3 Receive data	Structured communication request from consumer / PHR to Information Source; one-time-request} Allergies, Conditions, Health Problems and Diagnosis Codes are to be accessed. There needs to be both free text and controlled vocabulary data elements for each Condition/Problem/Diagnosis. Clinical status should be included (e.g. active, chronic, resolved, etc.) Date/time is needed for beginning and ending of the Condition/Problem/Diagnosis A key pre-condition needs to be documented involving consumer access via the PHR system to the document locator service (see pre-condition section)	1, 2, 4, 5, 11
			Action 6.1.4.2 View Information	Translate to lay person terminology {Consumer-friendly sub task}	5
		Event 6.1.5 Select and incorporate information	Action 6.1.5.1 Select Information	(PHR application functionality) Source information comes minimally from the document/record header and will be used as needed to facilitate the incorporation of Allergies/Condition/Problem/Diagnosis into the PHR	
			Action 6.1.5.2 Incorporate selected information into the PHR	(PHR user interface activity) Metadata to identify original source / context of information	7
		Event 6.1.6 Annotate information or request change	Action 6.1.6.1 Annotate Information	(PHR user interface activity) (PHR application functionality) The HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) Content Comment Module is already defined to describe annotation and target information being annotated. Need to request its explicit addition to IHE XD* Lab for extending HITSP/C37 -	1, 2, 3, 4, 7, 9,10

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				Lab Report Document	
			Action 6.1.6.2 Request Change	Request must be interpretable (structured information, structured interaction) This requires a new HITSP construct (See Section 3.1)	1, 2, 3, 4, 7, 9,
Consumer Empowerment	Consumer and PHR Service Provider	Event 2.1.2 Establish/ Change Permissions	Action 2.1.2.1 Authenticate to system	(PHR application functionality)	
			Action 2.1.2.2 Establish / Modify permissions for access to the system	(PHR application functionality) May also imply change in Consent Directives	
Consumer Empowerment and Access to Clinical Information	Consumer and PHR ServiceProvider	Event 6.1.2 Receive Notification	Action 6.1.2.1 Receive Notification	Standardized notification pursuant to "subscription". {Gap-reuse and expand existing constructs (HITSP/TP13 - Manage Sharing of Documents, HITSP/T29 - Notification of Document Availability)} Upon Notification receipt retrieve information interactions as defined by Events 6.1.3, 6.1.4, 6.1.5, and 6.1.6 above may be automatically triggered	12
Consumer Empowerment	Consumer and PHR Service Provider	Event 2.1.5 Modify registration/medication data	Action 2.1.5.1 Authenticate to system	(PHR application functionality)	
			Action 2.1.5.2 Request data	(PHR application functionality) or may require query and retrieve info from HIE	
			Action 2.1.5.3 Receive data	Query/retrieve information	
			Action 2.1.5.4 Modify data	(PHR application functionality)	
			Action 2.1.5.4a Annotate data	(PHR application functionality)	
			Action 2.1.5.5 Transmit modified and/or annotated data	Register/Make available for query/retrieve annotated information. If policy permit may "replace/Flag deprecated" previous version of information	
			Action 2.1.5.5a Transmit request to modify and/or correct data	Standardized notification pursuant to "subscription". {Gap-reuse and expand existing constructs (HITSP/TP13 - Manage Sharing of Documents, HITSP/T29- Notification of Document	5

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				Availability)}	
Consumer Empowerment and Access to Clinical Information	Health Information Source(s) EHR Systems Health Plans /Intermediaries PBM /Pharmacies	Event 2.4.1 Process request for registration/medication data	Action 2.4.1.1 Receive and validate the query request	Query for Information/Documents against a registry (may be supported by HIE)	
			Action 2.4.1.2 Authenticate and verify authorization of requestor	Validate Assertion in Query	
			Action 2.4.1.3 Authorize release of registration/medication information	(Application access control functionality)	
			Action 2.4.1.4 Transmit registration/medication information to an authorized system	Query response/Retrieve Information	
		Event 6.1.3 PHR(s) receive available information from other sources	Action 6.1.3.1 Receive Information		
		Event 2.4.1 Process request for registration/medication data	Action 2.4.1.5 Log interaction	Collect and communicate secured audit trail	
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Information Exchange Data or Network System (RHIO)	Event 6.1.1 Identify PHR(s) of choice	Action 6.1.1.1 Identify and communicate PHR(s) of choice	Identification of PHR Service/PHR instance {PHR Location-Gap} Identification of Consumer (Target of PHR) {Registry Patient Id/Id Domain OID} Authentication of Consumer-to-PHR-Service-Provider / Information Exchange-Leverage HITSP/C19 - Entity Identity Assertion {Authenticate Consumers-Partial Gap} Identification of providers Leverage HITSP/C19 - Entity Identity Assertion {Partial Gap} Identification of Information Sources	9, 10,11
		Event 2.4.1 Process Request for Registration and/or Medication Data Event 6.1.4 Access	Action 2.4.1.1 Receive and validate the query request Action 6.1.4.1 Request	Structured communicating request: from consumer / PHR to Information Source	7, 9, 11

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
		available information	information		
			Action 2.4.1.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.4.1.3 Authorize release of registration/medication data	(Application access control functionality)	
			Action 2.4.1.4 Transmit registration/medication data to an authorized system	Query response/Retrieve Information	
			Action 2.4.1.5 Log interaction	Collect and communicate secured audit trail	
		Event 6.1.2 PHR(s) receive available information from other sources	Action 6.1.2.1 Receive Information	Information-Source-to-PHR/ Information Exchange	1,2,4
			Action 6.1.2.2 Information is automatically populated for viewing using appropriate translations or transformations	Structured information {direct reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document} Translate to lay terminology {Consumer-friendly sub task}	1, 2, 4, 5
		Event 6.1.3 Receive Notification	Action 6.1.3.1 Receive Notification	Standardized notification pursuant to “subscription”. {Gap-reuse and expand existing constructs (HITSP/TP13 - Manage Sharing of Documents, HITSP/T29 - Notification of Document Availability)}	12
		Event 6.1.6 Annotate information or request change	Action 6.1.6.1 Annotate information	PHR application functionality Metadata to describe annotation and target information being annotated	7
			Action 6.1.6.2 Request Change	Request must be interpretable (structured information, structured interaction) This requires a new HITSP construct (See Section 3.1)	3, 7, 9, 11,

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment	Consumer	Event 2.1.6 Close Account	Action 2.1.6.1 Request to close PHR account	(PHR application functionality)	
			Action 2.1.6.1a Request registration/medication data sent to another provider of PHR service	To be addressed by Scenario 3 in the future	
			Action 2.1.6.2 Receive confirmation of account closure	To be addressed by Scenario 3 in the future	
			Action 2.1.6.2a Receive confirmation of account transfer	To be addressed by Scenario 3 in the future	

Consumer Empowerment Use Case – Scenario 2: Consumer visits Healthcare Provider and Provides Registration Summary information and Clinical Information
[Including Operationally Equivalent Events/Actions from the Consumer Access Use Case]

Table 2.2.1-2 Mapping of Use Case Requirements to Business Requirements

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Consumer	Event 2.1.3 Log on to system	Action 2.1.3.1 Authenticate to system	(PHR application functionality) plus policies	
	PHR Service Provider	Event 2.2.3 Process registration/medication data	Actor 2.2.3.1 Receive and validate query	Query for Information/Documents against a registry (may be supported by PHR service provider or via RHIO/HIE)	
			Actor 2.2.3.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.2.3.3 Transmit requested registration/medication information to authorized system	Query response/Retrieve Information	
			Actor 2.2.3.4 Log interaction	Collect and communicate secured audit trail	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
		Event 2.2.2 Gather registration and/or medication data Event 6.1.3 PHR(s) (or EHRs) receive available information from other sources	Action 2.2.2.1 Receive consumer request	Internal PHR systems operation	
			Action 2.2.2.2 Confirm consumer identity	Internal PHR systems operation plus policies	
			Action 2.2.2.3 Transmit request for registration/ medication data to data or network system	Request for relevant records/documents/information	3
			Action 2.2.2.4 Receive registration / medication data Action 6.1.3.1 Receive Information	Standardized information {direct reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
			Action 2.2.2.5 Acknowledge receipt of registration/medication data	Request/response	
			Action 6.1.3.2 Information is automatically populated for viewing using appropriate translations or transformations	Structured information {reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document} Translate to lay person terminology {Consumer-friendly sub task} The consumer receives personal information about his or her health from a healthcare provider. The information could be in the form of a laboratory test result, for example. The information may contain a term with which the consumer is not familiar, or about which the consumer wishes to learn more. The PHR application may provide a mechanism where the consumer clicks a button in the interface to request more information about a term. A multi-term query is created and transmitted to one or more Health Information Resource providers, with which the PHR Service Provider or the consumer may have a business relationship.	1, 2, 4, 5, 10, 12
			Action 2.2.2.6 Log interaction	Collect and communicate secured audit trail	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
		Event 2.2.3 Process request for registration and/or medication data	Action 2.2.3.1 Receive and validate the query process	Query for Information/Documents against a registry (may be supported by PHR service provider or via RHIO/HIE)	
			Action 2.2.3.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.2.3.3 Transmit registration/medication data to an authorized system	Query response/Retrieve Information	
			Action 2.2.3.4 Log interaction	Collect and communicate secured audit trail	
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Healthcare Provider	Event 2.3.1 View registration and/or medication data Event 6.1.3 PHR(s) (or EHRs) receive available information from other sources	Action 2.3.1.1 Submit authentication information to PHR	Validate Assertion in Query	
			Action 2.3.1.2 Receive registration/medication data Action 6.1.3.1 Receive Information	Standardized information {direct use or reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
Consumer Empowerment	Healthcare Provider	Event 2.3.2 Integrate registration data into EHR or other care system	Action 2.3.2.1 Transmit request for registration / medication data to provider of PHR service	Query for Information/Documents against a registry (may be supported by PHR service provider or via RHIO/HIE)	
			Action 2.3.2.2 Accept data into EHR system	(EHR application functionality)	
			Action 2.3.2.3 Confirm data integrity	(EHR application functionality)	
			Action 2.3.2.3a Produce exception list of errors	(EHR application functionality)	
			Action 2.3.2.4 Parse and validate results content	(EHR application functionality)	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
			Action 2.3.2.5 Acknowledge receipt of registration/medication data	Request/response	
			Action 2.3.2.6 Log interaction	Collect and communicate secured audit trail	
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Data or Network System Health Information Source(s)	Event 2.4.1 Process Request for Registration and/or Medication Data Event 6.1.3 PHR(s) (or EHRs) receive available information from other sources	Action 2.4.1.1 Receive and validate the query request Action 6.1.3.1 Receive Information	Query for Information/Documents against a registry (may be supported by HIE) Standardized information {direct use or reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
			Action 2.4.1.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.4.1.3 Authorize release of registration/medication data	Application access control functionality	
			Action 2.4.1.4 Transmit registration/medication data to an authorized system	Query response/Retrieve Information	
			Action 2.4.1.5 Log interaction	Collect and communicate secured audit trail	

Consumer Empowerment Use Case – Scenario 3: Authorized Healthcare Provider Reviews Registration Summary and Other Clinical Information
[Including Operationally Equivalent Events/Actions from the Consumer Access Use Case]

Table 2.2.1-3 Mapping of Use Case Requirements to Business Requirements

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment	Consumer	Event 2.1.3 Log on to system	Action 2.1.3.1 Authenticate to system	PHR application functionality plus policies	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	PHR Service Provider	Event 2.2.2 Gather registration and/or medication data Event 6.1.3 PHR(s) (or EHRs) receive available information from other sources	Action 2.2.2.1 Receive consumer request	Internal PHR systems operation	
			Action 2.2.2.2 Confirm consumer identity	Internal PHR systems operation plus policies	
			Action 2.2.2.3 Transmit request for registration/ medication data to data or network system	Request for relevant records/documents/information	3
			Action 2.2.2.4 Receive registration / medication data Action:6.1.3.1 Receive Information	Standardized information {direct reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
			Action 2.2.2.5 Acknowledge receipt of registration/ medication data	Request/response	
			Action 6.1.3.2 Information is automatically populated for viewing using appropriate translations or transformations	Structured information {reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab (Lab)} Translate to lay terminology {Consumer-friendly sub task} The consumer receives personal information about his or her health from a healthcare provider. The information could be in the form of a laboratory test result, for example. The information may contain a term with which the consumer is not familiar, or about which the consumer wishes to learn more. The PHR application may provide a mechanism where the consumer clicks a button in the interface to request more information about a term. A multi-term query is created and transmitted to one or more Health Information Resource providers, with which the PHR Service Provider or the consumer may have a business relationship.	1, 2, 4, 5, 10, 12

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
			Action 2.2.2.6 Log interaction	Collect and communicate secured audit trail	
Consumer Empowerment	PHR Service Provider	Event 2.2.3 Process request for registration and/or medication data	Action 2.2.3.1 Receive and validate the query process	Query for Information/Documents against a registry (may be supported by PHR service provider or via RHIO/HIE)	
			Action 2.2.3.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.2.3.3 Transmit registration/medication data to an authorized system	Query response/Retrieve Information	
			Action 2.2.3.4 Log interaction	Collect and communicate secured audit trail	
Consumer Empowerment	Healthcare Provider	Event 2.3.1 View registration and/or medication data	Action 2.3.1.1 Submit authentication information to PHR	Validate Assertion in Query	
			Action 2.3.1.2 Receive registration/medication data	Standardized information {direct use or reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
Consumer Empowerment	Healthcare Provider	Event 2.3.2 Integrate registration data into EHR or other care system	Action 2.3.2.1 Transmit request for registration / medication data to provider of PHR service	Query for Information/Documents against a registry (may be supported by PHR service provider or via RHIO/HIE)	
			Action 2.3.2.2 Accept data into EHR system	(EHR application functionality)	
			Action 2.3.2.3 Confirm data integrity	(EHR application functionality)	
			Action 2.3.2.3a Produce exception list of errors	(EHR application functionality)	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
			Action 2.3.2.4 Parse and validate results content	(EHR application functionality)	
			Action 2.3.2.5 Acknowledge receipt of registration/medication data	Request/response	
			Action 2.3.2.6 Log interaction	Collect and communicate security audit trail	
Consumer Empowerment Consumer Empowerment and Access to Clinical Information	Data or Network System Health Information Source(s)	Event 2.4.1 Process Request for Registration and/or Medication Data Event 6.1.3 PHR(s) (or EHRs) receive available information from other sources	Action 2.4.1.1 Receive and validate the query request Action 6.1.3.1 Receive Information	Query for Information/Documents against a registry (may be supported by HIE) Standardized information {direct use or reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
			Action 2.4.1.2 Authenticate and verify the authorization of the requestor	Validate Assertion in Query	
			Action 2.4.1.3 Authorize release of registration/medication data	(Application access control functionality)	
			Action 2.4.1.4 Transmit registration/medication data to an authorized system	Query response/Retrieve Information	
			Action 2.4.1.5 Log interaction	Collect and communicate security audit trail	

Consumer Access Use Case – Scenario 2: Provider Lists and Permissions

Table 2.2.1-4 Mapping of Use Case Requirements to Business Requirements

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment and Access to Clinical Information	Consumer	Event 7.1.1: Request and access provider information	Action 7.1.1.2 Request provider information	Using the PHR, consumers request information about providers who they may wish to add to their provider list. Providers may include individuals, practices, and/or organizations. The PHR retrieves provider information from an HIE registry, EHRs, payors, etc	13
			Action 7.1.1.4 Access provider information	Consumers access the requested provider identifying information. Identifying information may include: services, place of practice, etc	13
		Event 7.1.2 Create/update provider lists	Action 7.1.2.1 Select and incorporate provider information	Consumers select the desired provider information and create and/or update their lists of providers in their PHR	13
		Event 7.1.3 Designate provider permissions	Action 7.1.3.1 Designate provider permissions	Consumers designate which information in their PHR can be accessed by which providers. Methods for designating the consumer's decisions could include designating access for individual providers, designating access based on roles assigned to providers, designating access for provider practices or organizations, designating access by type of health information or some other criteria. In addition, the models may need to accommodate various approaches or a combination of approaches for designating permissions. These approaches may include an inclusive model, an exclusive model, and/or the utilization of pre-determined defaults. A generalized process for access control is described in Appendix A: Create and Maintain Access Control Lists. Consumers may have the ability to allow (or not allow) providers to override the permissions in necessary situations. Reasons for "breaking the glass" are recorded in a consistent manner and incorporated into access and disclosure logs	13, 14
		Event 7.1.4 Review access and disclosure logs	Action 7.1.4.1 Review access and disclosure logs	Consumers review information describing who has viewed their health information. The ability to merge or integrate this information from multiple sources into a time-	15

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				sequence or other logical view may also be important for consumers. Information describing access to and disclosure of PHR information, "break the glass" access, HIE information exchange information access, and, at times, may include access to information in EHRs, etc	
Consumer Empowerment and Access to Clinical Information	Provider	Event 7.2.1 Request and access available clinical information	Action 7.2.1.1 Request and access information	Providers request and are able to access information from the consumers' PHR and other sources based upon access permissions established by the consumer. Providers may be informed that some information is not accessible as a result of the consumers' access decisions. Providers are able to identify the original source of the data as well as whether the information has been subsequently modified. If modification has occurred, the identity of the source of the modification is also available to providers. A generalized process for access control is described in Appendix A: Create and Maintain Access Control Lists. A generalized process for matching patients is described in Appendix A: Arbitrating Identities	10, 11, 15
		Event 7.2.2 Select and incorporate clinical information	Action 7.2.2.1 Select information	After accessing the available consumer information based upon permissions set by consumers, providers may choose to incorporate selected information into EHRs. This information may be selected at various levels of specificity, such as discrete pieces of information and/or groups of information (e.g. data sets)	None
			Action 7.2.2.2 Incorporate data into EHRs	The providers' EHR incorporates the selected information. The original source of the data are also incorporated into the EHR	None
		Event 7.2.3 Systems log the activity	Action 7.2.3.1 Log access to information	The consumers' PHR and data intermediaries create logs of the information exchanges. The logs identify who has accessed the consumers' information. The access and disclosure logs could be reviewable by the consumers. It may be helpful to combine log information from several systems in order to establish a complete view of who has accessed the consumers' information	15

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				over a period of time	

Consumer Access Use Case – Scenario 3: Transfer of PHR Information

Table 2.2.1-5 Mapping of Use Case Requirements to Business Requirements

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
Consumer Empowerment and Access to Clinical Information	Consumer	Event 8.1.1 Access PHR(A)	Action 8.1.1.1 Access PHR(A)		
		Event 8.1.2 Request and access available information in PHR(A)	Action 8.1.2.1 Review PHR(A) Information	Consumers request and are able to access information in their PHR. Consumers are able to identify the original source of the data as well as whether the information has been subsequently modified. If modification has occurred, the identity of the source of the modification is also available	10, 11, 15
		Event 8.1.3 Select Information to send PHR(B)	Action 8.1.3.1 Select data elements and/or data sets	Standardized information {direct use or reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab, HITSP/C35 - Lab Result Terminology}	1, 2, 4, 9
			Action 8.1.3.2 Select providers and permissions		
		Event 8.1.4 Identify PHR(B) which is to receive the information	Action 8.1.4.1 Identify PHR(B) which is to receive the information		
		Event: 8.1.5 PHR(A) sends information to PHR(B)	Action: 8.1.5.1 Forward information to PHR B)	Write selected information on device/interchange media. Ensure consistent management of organization on media	
			Action: 8.1.5.2 Confirm delivery of information to PHR(B)	Confirm delivery of information not applicable for media interchange as media is provided to consumer who will be responsible for delivery to other PHR or EHR Action. Consider this to be the confirmation of reading	

Use Case	Perspective/ Business Actor	Event	Action	Interoperability Requirement(s)	Data Requirement Number
				of media as acceptable to consumers. May review media content and select documents of interest and import content.	

2.2.2 DATA AND INFORMATION REQUIREMENTS MATRIX

This section contains an extraction of data and information requirements with a listing of the actual data elements and information that meet the described data requirements.

Table 2.2.2-1 Table and Information Requirements Matrix

Data Requirement Number	Description	Data Element(s)	Scenario
1	Diagnosis Codes	"Ability for a consumer to retrieve and store a list of diagnosis codes." Patient Class (outpatient, inpatient, and ER (UHDDS) Diagnosis/Injury Code (ICD 9/10) Diagnosis Type (UHDDS) Diagnosis Date and Time (UHDDS) Date/time of first symptoms Discharge Disposition (UHDDS) Chief Complaint (ICD9/10) Date/time of first symptoms of illness (UHDDS) Identity of diagnosing provider or institution Diagnostic procedure(s) HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) Section 4.2.3.1.7	1
2	Allergies / Medication Allergies	"Ability for consumer to retrieve and store lists of current environment, dietary, or medical supply allergies" "Ability for consumer to retrieve and store lists of current medication allergies" Allergy type Date/time of first symptoms HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) Section 4.2.3.1.6	1
3	Change request	Information source identifier Consumer identifier Original entry identifier Data enterer identification/authorization information Annotation/change request information (relate to standard clinical content structures) Rational for change request (free text?) Requestor contact information	1

Data Requirement Number	Description	Data Element(s)	Scenario
4	Clinical data are provided, including (but not limited to)	Laboratory test results (see HITSP/C35 - Lab Result Terminology, HITSP/C37 - Report Document Using IHE XD* Lab) Medication History (see HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD))	1
5	Context-aware Information Retrieval Message Model	A query to an information resource will contain at least one Main Search Criteria as described below. In addition, the query may contain any of the other classes listed below (Using a subset of the criteria defined by HL7 v3 InfoButton): MainSearchCriteria SeverityObservation class: SubTopic TaskContext Encounter type DeliveryLocation / id AssignedEntity username certificateTex Organization Organization.id AuthorizedPerson: PatientContext PatientPerson.administrativeGenderCode PerformerChoice: Patient or HealthCareProvider Age AgeGroup LanguageCommunication: InfobuttonEventNotification.id InfobuttonEventNotification.effectiveTime	

Data Requirement Number	Description	Data Element(s)	Scenario
7	Document metadata/ Source/context metadata	One or more sets of documents Documents should be of any format, structure and content. This is critical to support any currently defined documents by HITSP as well as future documents Selected metadata about each document, forming the entries of a media table of content. One entry per document stored on the media. Metadata should contain information such as: Patient ID and basic demographics Class of Document Document Type Source Care-Setting/Specialty Date/time Format/MIME Type Source identifier Entry identifier Date of original datum Last update date Updated by identifier(s) (Look at document metadata in HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Report Document Using IHE XD* Lab)	3 (Consumer Empowerment and Consumer Access)
9	Information Source identification data	URL Service Provider Service Type (e.g., laboratory, pharmacy, healthcare entity, etc)	1, 3 (Consumer Empowerment and Consumer Access)
10	Secure consumer identification data	Consumer Demographic Information (DOB, age, gender, resident zip code, state of residence) Consumer identifiers (identifier and authority)	1, 3 (Consumer Access)
11	Structured information request	Information Service Identifier Requested information type Patient (target) identification Requested information parameters (date range, limiting criteria) Requestor authentication and authorization information Type of request: One time request, notification request, subscription request Request active dates (how long to continue request) Per HITSP/IS03 - Consumer Empowerment and Access to Clinical Information via Networks, the current HITSP/TP13 - Manage Sharing of Documents, query and retrieve transactions, provides the same service to both EHRs and PHR service providers. This should remain in place to support this Use Case	1, 3 (Consumer Access)

Data Requirement Number	Description	Data Element(s)	Scenario
12	Structured Notification	Information Source identification Consumer (target) identification Information type (e.g., laboratory, pharmacy, etc) Notification Identifier or Record reference identifier	1
13	Provider identification, details, location	Superset of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) & C37 - Lab Report Document provider identification, and additional elements as needed for entity resolution Consistent representation of practice sites, nature of practice, all alternatively presented in lay person friendly terms	2 (Consumer Access)
14	Access Control Lists	Identification of entity being authorized Identification of entity granting authorization Type of authorization (read/no-read, write/no-write, etc) Criteria defining the application of the authorization (e.g., document type, procedure/test results, etc.)	2 (Consumer Access)
15	Access log summary/detail: what was accessed, when, by whom, stated purpose	Access log information, available in both summary and detail format: What information was accessed Who accessed the information When was the information accessed Stated purpose for the access Override criteria, if applicable (e.g., "break-glass") Is the access log all-event or exception-event-only?	2 (Consumer Empowerment and Consumer Access)

2.2.3 IDENTIFICATION OF BUSINESS ACTORS, INTERACTIONS, AND SCENARIOS

This section describes the business actors that impact interoperability requirements for each scenario. A HITSP business actor should generally be an IT system that is directly engaged, and benefits from the real world information interchange defined within a business Use Case action. A business actor may also be a person or organization, however, only IT systems have associated technical actors (see Section 3.2 for technical actors). The table below identifies the significant Use Case business actors, their descriptions and the Use Case scenarios in which they are used.

Other business actors not explicitly mentioned may be able to benefit from this Interoperability Specification. NOTE: While Pharmacies and Pharmacy Benefits Managers (PBMs) are distinct and different entities, within these Use Cases they perform the same functions. Either or both may provide demographic information and/or medication history. For simplicity of discussion and diagrams, they are described together.

Table 2.2.3-1 Business Actors

Business Actor	Description	Scenario
Consumer	The individual who receives healthcare services and selects a provider of PHR services to maintain their personal health record consisting of registration data and medication history. This individual determines which business actors are authorized to review, access, and update their personal health record	1, 2, 3
Personal Health Record (PHR) Service Provider	The organization that supplies the Personal Health Record (PHR), a secure, real-time, point-of-care, person-centric information resource, for consumers	1, 2, 3
Regional Health Information Organizations (RHIO)/Health Information Exchange (HIE)	A Regional Health Information Organization (RHIO)/Health Information Exchange (HIE) is a multi-stakeholder organization that enables the exchange and use of health information, in a secure manner, for the purpose of promoting the improvement of health quality, safety and efficiency	1, 2, 3
Electronic Health Record (EHR) System	The Electronic Health Record (EHR) System is a secure, real-time, point-of-care, patient-centric information resource for clinicians	1, 2, 3
Health Plan/Intermediary	The organization or its designated intermediary that pays for healthcare, may participate as a data or network system of registration summary information, and can act as a provider of PHR services	1, 2, 3
Pharmacy Benefit Manager (PBM)/Pharmacy	The organization that has been delegated authority from the payer to process pharmaceutical claims, intermediary, pharmacy or sub network to provide data for medication history, and can act as a provider of PHR services	1, 2, 3

These business actors are identified as separate actors in the various scenario actor Transactions descriptions below in section 3.2.1 and 3.2.2. This descriptive approach does not prevent business actors from being grouped in a variety of ways. A number of such implementation variants are depicted in Sections 3.2.2 to illustrate in part the architecture flexibility provided by this Interoperability Specification.

2.2.4 HIGH-LEVEL UML INTERACTION (BUSINESS SEQUENCE) DIAGRAM

This section contains an explanation of the relationship between the business actors and data interactions between the primary actors and alternative actors for each Use Case scenario. The diagrams that follow illustrate each scenario with a representation of a normal sequence of exchange between the primary actors.

Figure 2.2.4-1 Scenario 1: Consumer Creates Account to Host and Access Registration Summary and Clinical Information High-Level Business Sequence Diagram - Part A

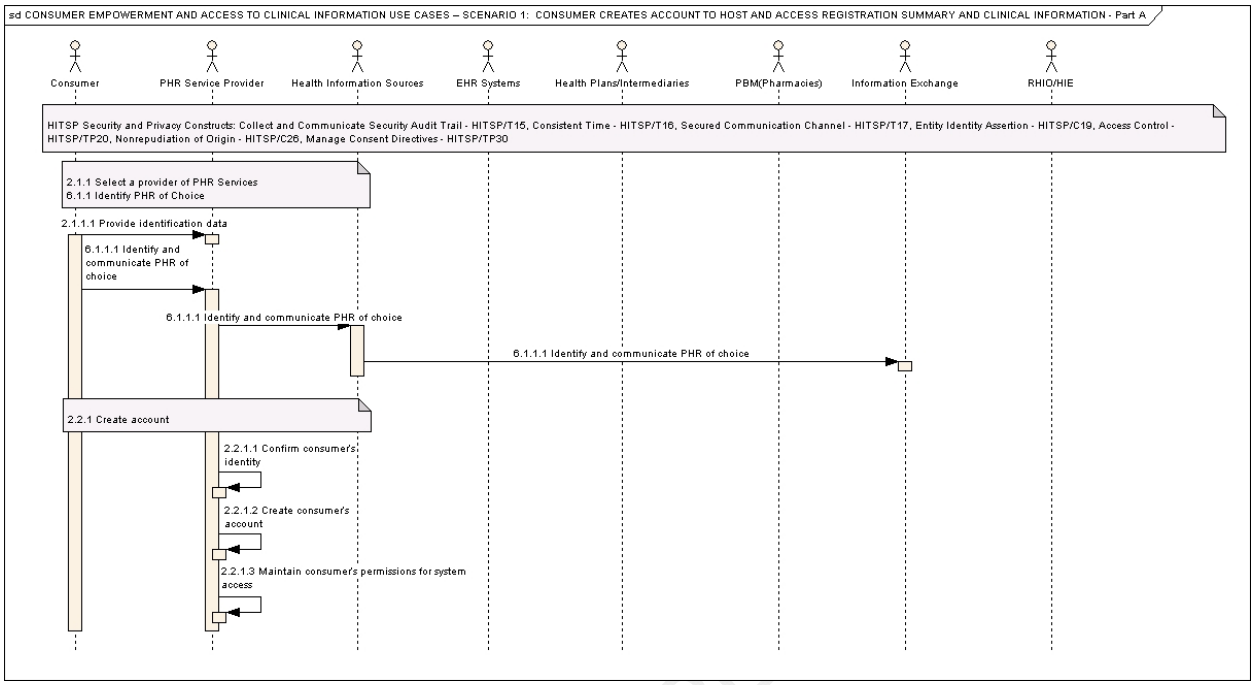


Figure 2.2.4-1 Scenario 1: Consumer Creates Account to Host and Access Registration Summary and Clinical Information High-Level Business Sequence Diagram - Part B

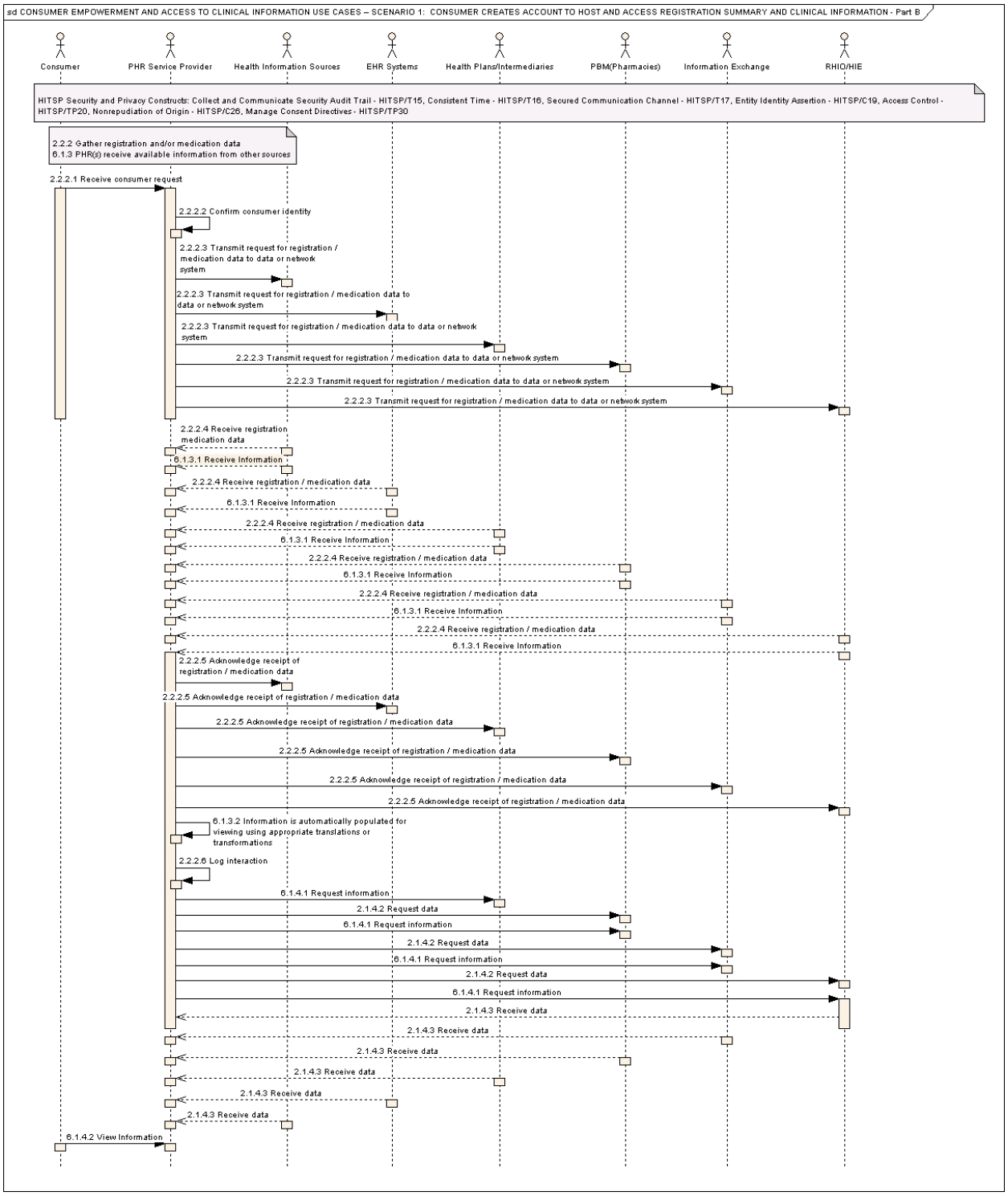


Figure 2.2.4-1 Scenario 1: Consumer Creates Account to Host and Access Registration Summary and Clinical Information High-Level Business Sequence Diagram - Part C

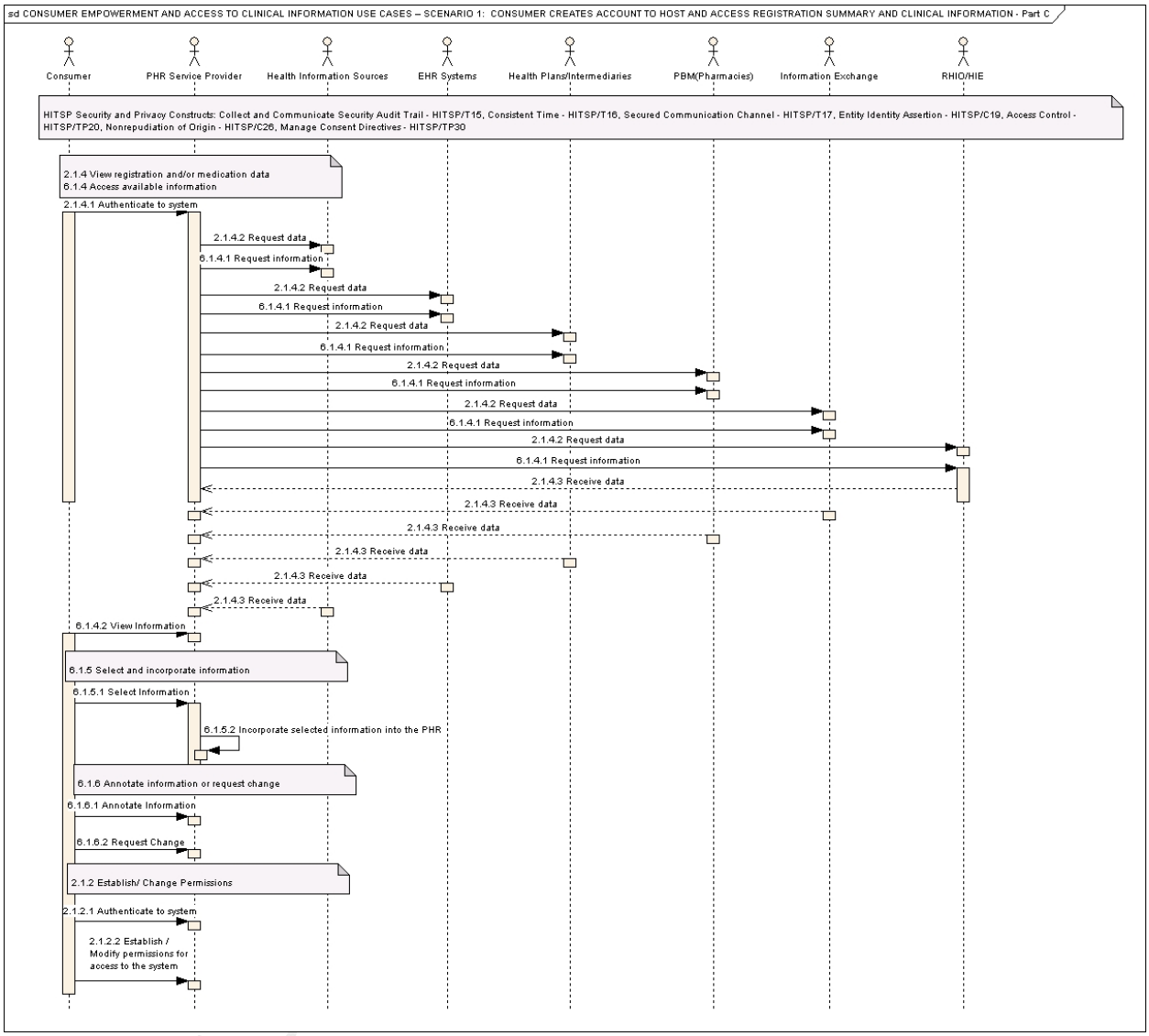


Figure 2.2.4-1 Scenario 1: Consumer Creates Account to Host and Access Registration Summary and Clinical Information High-Level Business Sequence Diagram - Part D

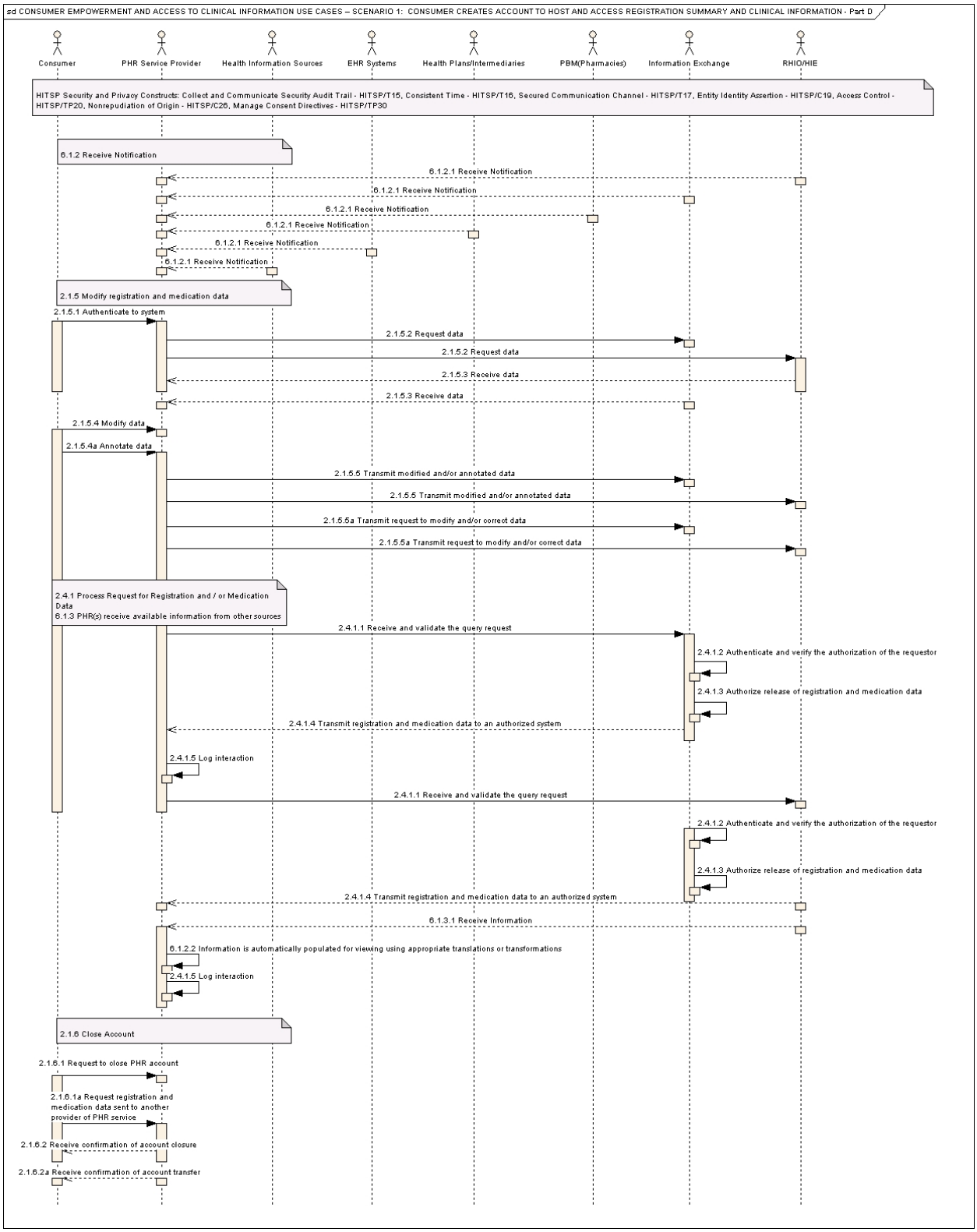


Figure 2.2.4-2 Scenario 2: Consumer Visits Healthcare Provider and Provides Registration Summary Information and Clinical Information High-Level Business Sequence Diagram

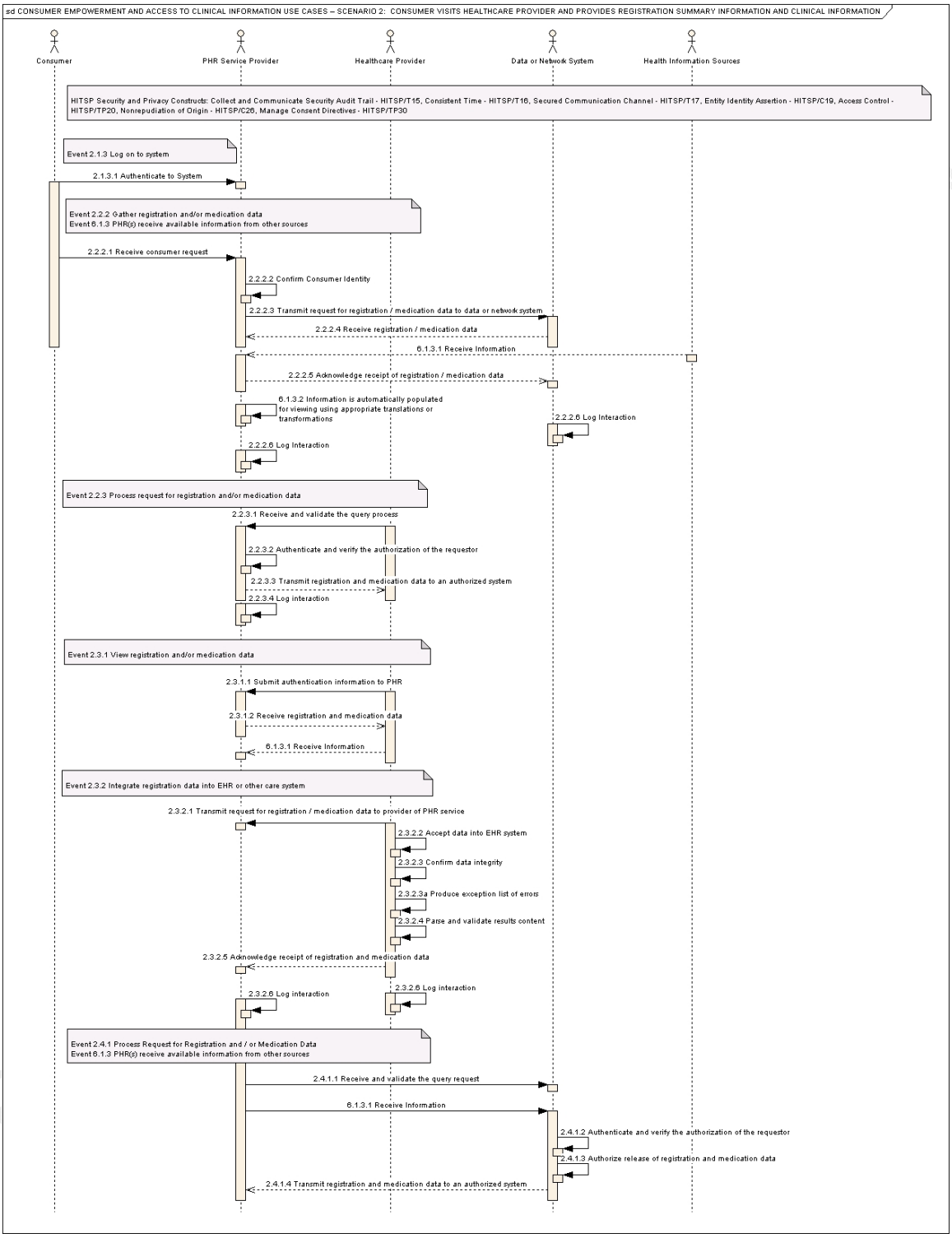
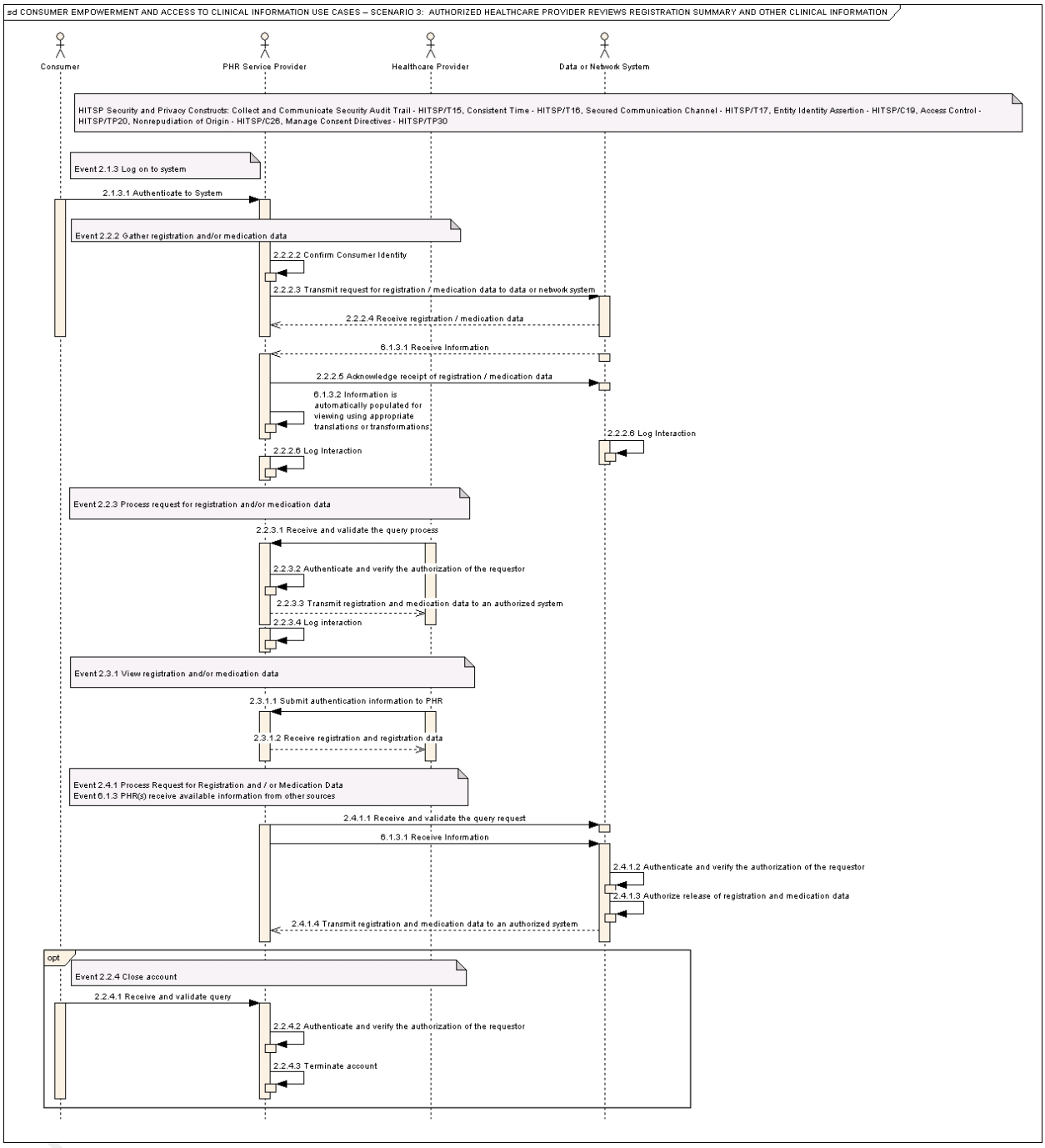


Figure 2.2.4-3 Scenario 3: Authorized Healthcare Provider Reviews Registration Summary and Other Clinical Information High-Level Business Sequence Diagram



3.0 DESIGN

The design for the Interoperability Specification is the result of the requirements analysis and iterative standards selection process. This section describes the events and actions of the design from the specified requirements. It also provides a detailed mapping of the specified requirements to the business and technical actors, and data elements. Groupings of specific actions and actors are illustrated to further describe the relevant interactions as existing or new HITSP constructs required for interoperability.

3.1 SCOPE OF DESIGN

This section describes the scope of the design as it relates to the requirements for the Use Cases that were identified in Section 2.2 above. The scope identifies the assumptions that provide the boundaries for the specification and the constraints that limit the use of the specification. In addition, any pre-conditions, post-conditions and triggers that underlie the interactions between the various actors, data and Transactions are provided.

Considering the relationship to previous constructs, known gaps, potential activities by SDOs, and other initiatives that are either in-progress or pending results that might impact the Interoperability Specification development, the Use Cases were broken down in high-level Work Items to one of two Work Sets.

- Addressed by this update to this Interoperability Specification HITSP/IS03 - Consumer Empowerment and Access to Clinical Information via Networks and the new HITSP/IS05 Consumer Empowerment and Access to Clinical Information via Media shown in table below
- Gaps to be addressed during next year's HITSP cycle shown in Table 4.2.1

Table 3.1-1 Scoping

Work Items	Work Set	Reason for Classification Result
LAB/Results-to-PHR-to-other using lab report document	Addressed by this update to IS03 and the new IS05.	Reference existing HITSP/C37 - Lab Report Document for inclusion of complete lab reports into a PHR.
LAB/Results-to-PHR-to-other using structured elements in registration/medication history document	Addressed by this update to IS03 and the new IS05.	Extend HITSP/C32 artifact with a lab results section for inclusion of selected lab results extracts. Subset of CDA structure in HITSP/C37 - Lab Report Document
Allergies, Conditions, Immunizations, Health Problems and Diagnosis Codes	Addressed by this update to IS03 and the new IS05.	Extend HITSP/C32 artifact with relevant sections.
PHR Portability – using portable media	Addressed by this update to IS03 and the new IS05.	Given lack of a strong source attestation on media construct, media usage may be restricted by policy to single consumer health information in a number of environments. In some environments consumer and dependent health information may be allowed on the same portable media (up to a certain age).

3.1.1 ASSUMPTIONS

This section provides an overview of the assumptions, including the circumstances, actors, policies and/or technologies that need to be in place for the design to be completed as specified. Assumptions are different from constraints which are specifically used to narrow the definition, or indicate limitations of the specified interactions.

Table 3.1.1-1 Assumptions

Assumption	Use Case Scenario
Regarding provider-specified restrictions to clinical information, either (1) Providers do not have the option of limiting the consumer's access to clinical information that directly relates to that consumer, or, (2) The specification, interoperability requirements, and policy considerations of such restrictions are outside the scope of this Use Case	Consumer Access to Clinical Information / 1
Although the Use Case is focused on the Information Transfer from one PHR to another, HITSP has opted to ensure that the constructs produced not only support the Use Case but other Use Cases where the interchange takes place between a PHR and an EHR or between two EHRs	Consumer Access to Clinical Information / 3
Regarding statutory limitations on a consumer's access to clinical information: (1) Statutory and policy considerations are beyond the scope of this Use Case (2) Unless precluded by statute, the consumer shall be informed (via the PHR) of the existence and unavailability of the document per statute. Consumer escalation procedures should be available, at minimum, by reference	Consumer Access to Clinical Information / 1
Consumers have access to appropriate identification information for Information Sources and Recipients, and Providers	Consumer Access to Clinical Information / 1, 2

3.1.2 CONSTRAINTS

This section describes the constraints that limit the context in which the Interoperability Specification may be used. A constraint describes a rule that limits the use of the actors, actions or data 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 3.1.2-1 Constraints

Constraint	Use Case Scenario
Available HITSP constructs (i.e., HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD), HITSP/C35 - Lab Result Terminology and HITSP/C37 - Lab Report Document) do not support the entire range of potential information included in a PHR or clinical information that may be communicated to a PHR. This constrains the information that can be supported in the Interoperability Specification. Further extension to this as written does not address the notification of a change request rejection	Consumer Access to Clinical Information / All
The physician has an EHR capable of exporting media.	Consumer Access to Clinical Information / 1

3.1.3 PRE-CONDITIONS

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

Table 3.1.3-1 Pre-conditions

Pre-condition	Use Case Scenario
Network infrastructures that enable secure, appropriate, and accurate information exchange across data sources and systems to view the data. This includes, but is not limited to: methods to identify and authenticate users a. methods to identify and determine providers of care b. methods to enforce data access authorization policies c. methods to correctly match consumers/patients across systems d. methods to identify and determine health insurers e. methods to identify and determine pharmacy benefits managers (NOTE: pharmacy benefit information is obtained through NCPDP transactions) f. methods to identify data sources including but not limited to provider EHR systems	All
Ability to identify and request corrections to errors is available	All
Ability to apply notes, corrections and comments on original entries is available	All
Appropriate standards are developed, approved, and widely adopted supporting data content and structure, allowing universal access by compliant systems	All
Core datasets are defined and adhered to	All
Authenticate consumers, designated caregivers, and health professionals for access to the consumer's PHR service providers	All
Method to query other organizations for data and matching to the consumer is available	All
Support the technical measures to ensure Security and Privacy of consumer/patient health information	All
Authentication service to authenticate requestors and/or data submissions from various locations	All
Security and Privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient Security and Privacy	All
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	All
Support the following HITSP Security and Privacy constructs: HITSP/T16 Consistent Time – Maintain time HITSP/T17 Secured Communication Channel – Authenticate node HITSP/T15 Collect and Communicate Security Audit Trail – Record audit event in repository HITSP/TP30 Manage Consent Directive – Capture/Request consent directive HITSP/TP20 Access Control – Access control request -	All

In order to implement the information interchange conforming to this Interoperability Specification and its constructs in a real world environment, the implementer must insure that the implementing systems operate within a secure infrastructure that ensures the privacy, integrity and availability of all individually identifiable health information as prescribed by the Health Insurance Portability and Accountability Act, all other applicable laws and regulations and terms of any contracts and agreements. The information interchange standards may also assume that certain information technology infrastructure and functions are in place. These assumptions collectively are the general pre-conditions for conforming to this Interoperability Specification and its constructs.

The HITSP Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification requires that sharing of personal demographic data, healthcare summary, and laboratory reports is based on patient consent. The management of Patient Consent Directives is supported by this Interoperability Specification.

As a pre-condition of the Use Case, appropriate security and privacy controls must be in place to implement role based access. The registration and healthcare summary document has been designed to provide a clear separation between demographic and financial data that are not restricted and clinical data (advance directives, conditions, allergies, laboratory results and medications) that must be restricted. It is also acknowledged that some demographic or financial data may justify fine grained access control in special situations. For example, some consumers may wish to conceal some contact information (such as a cell phone number), some healthcare provider information (such as a same sex spouse or partner), or a condition specific health plan (that might reveal a medical diagnosis) from some individuals.

3.1.4 POST-CONDITIONS

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

Table 3.1.4-1 Post-conditions

Post-condition	Use Case Scenario
The consumer's PHR is available to be accessed by the consumer and any persons/organizations that have been given consent by the consumer	All

3.1.5 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary to start any scenarios, actions or events. It can be an automatic or manual process or result that in turn starts off another scenario, action or event. 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 3.1.5-1 Process Triggers

Process Trigger	Use Case Scenario
The consumer decides to create a PHR	Consumer Empowerment (Registration and Medication History) / 1
The consumer receives information from outside sources	Consumer Empowerment (Registration and Medication History) / 1 Consumer Access to Clinical Information / 1
The consumer decides to share PHR information with a care provider or another PHR	Consumer Empowerment (Registration and Medication History) / 2 Consumer Access to Clinical Information / 3
A consumer-authorized user elects to export health information	Consumer Access to Clinical Information /3

3.2 DETAILED DESIGN

This section provides a detailed description of the technical design, along with an analysis of the main interactions and decisions between all actors, actions and data in support of the specific requirements for each scenario of the Use Cases. In addition, this section provides the data element details and an overview of the HITSP constructs used to meet the business and technical requirements for these Use Cases.

Local implementation policy as determined by risk assessment, including assessment of jurisdictional and regulatory requirements, will determine which assurance level of nonrepudiation of origin is needed. For instance, in document-based transmissions, a low level is offered by the basic use of HITSP\TP13 - Manage Sharing of Documents. A medium level of assurance is offered by use of the HITSP\TP13 - Manage Sharing of Documents option called “Document Integrity”; a high level of assurance is offered by the use of the HITSP\C26 - Nonrepudiation of Origin Component. This later construct requires the existence of a Public Key Infrastructure (PKI) (See HITSP\TN900 - Security and Privacy Technical Note which discusses challenges with PKIs).

3.2.1 TECHNICAL ACTORS ROLE DESCRIPTIONS

This section contains technical actor role descriptions for all scenarios. Note that a business actor is a representation of a person, IT system, organization or any combination that is engaged, and benefits from the real world information interchange defined by a business Use Case, while 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 describes the Technical actor roles involved and the correlation between active actors.

Table 3.2.1-1 Technical Actor Role Descriptions

Technical Actor(s)	Actor Role
Patient Identity Source	Sends a patient identification number and demographic information to the Patient Identifier Cross-Reference (PIX) Manager
PIX Consumer	The Patient Identifier Cross-Reference Consumer queries the Patient Identifier Cross-Reference Manager for a master patient identifier that is a cross-reference to the patient identifiers supplied. It may also receive notifications about cross-reference changes
PIX Manager	The Patient Identifier Cross-Reference Manager is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains
Patient Demographics Consumer	The Patient Demographics Consumer queries the Patient Demographics Supplier to obtain patients that match the patient demographic data supplied in order to obtain a patient identification number. It may receive matches for one or more patients that enable the selection of the desired patient
Patient Demographics Supplier	The Patient Demographics Supplier receives patient registration and update messages from other systems in the enterprise (e.g., ADT Patient Registration or Health Plan Membership Management systems), which may or may not represent different Patient ID Domains. It responds to queries for information
Content Creator	The Content Creator is responsible for the creation of content and transmission to a Content Consumer
Content Consumer	A Content Consumer is responsible for viewing, import, or other processing of content created by a Content Creator
Document Source	The Document Source is the producer and publisher of documents and information. It is responsible for sending documents to a Document Repository. It also supplies metadata to the Document Repository for subsequent registration of the documents with the Document Registry
Document Consumer	The Document Consumer queries a Document Registry for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors
Document Registry	The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumers about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
Document Repository	The Document Repository is responsible for both the persistent storage of documents as well as for their registration with the appropriate Document Registry. It assigns a URI to documents for subsequent retrieval by a Document Consumer The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumers about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
Audit Record Source	The Audit Record Source is the actor that, on behalf of another actor that performs an action requiring logging, creates and communicates an Audit Record to the Audit Record Repository
Audit Record Repository	The Audit Record Repository provides a repository for audit events. IHE does not specify what analysis and reporting features should be implemented for an audit repository
Time Client	Time Client establishes time synchronization with one or more Time Servers using the NTP protocol and either the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) algorithms. Maintains the local computer system clock synchronization with Coordinated Universal Time (UTC) based on synchronization with the Time Servers
Time Server	Time Server provides NTP time services to Time Clients. It is either directly synchronized to a UTC master clock (e.g. satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s)
Node	The Node is the originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the Secure Node in the IHE ATNA Transaction

Technical Actor(s)	Actor Role
Service User	The Service User entity represents any individual entity (such as a clinician or an EHR/PHR system) that needs to make a service request of a Service Provider. The entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transaction
Identity Provider	The Identity Provider receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider)
Service Provider	The Service Provider represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion
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
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
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 a Uniform Resource Identifier (URI) and 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
Consent Directive Requester	The Consent Directive Requester access consent directive located through a Consent Registry from Consent Repositories. (lack of definition in current public comment version)
User	The User is the entity that takes on the actor role of initiator or claimant. This is an initiator actor
User Access Control Service (UACS)	The UACS is the enterprise security service that supports and implements user-side access control capabilities. This is an initiator actor
Service Provider (SP)	The SP is the information resource, representing the information repositories and all capabilities that receive, process and fulfill authorized requests. The Service Provider includes any local access decision and enforcement components that are part of the distributed capabilities
Service Provider Access Control Service (SP ACS)	The SP ACS service supports and implements the service-side access control capabilities. This is a service provider actor

3.2.2 SEQUENCE DIAGRAM FOR PROCESS FLOW

The technical design incorporates the comprehensive business and technical requirements and a detailed analysis of the interactions and decisions undertaken for the primary actions in each Use Case scenario. The UML sequence diagrams used in this section incorporate the detailed data requirements for the selected standards with the technical actors, and their specific and detailed interactions (encapsulated in HITSP constructs). The detailed actor interactions described in these more detailed diagrams show which HITSP constructs are used for the Interoperability Specification. Diagrams show all common or independent actors, data, actions, and groupings of actions around common actors.

The following narrative provides a high level walk though of the flow in the context of a fictitious scenario. The legend used to read the fictitious scenario is shown below. This legend and background explanation applies to all scenarios.

<Consumer> = Adam Everyperson
<PHR> = WebExcellent Personal Health Record (WebPHR)
<RHIO> = Greater Metropolitan Health Information Network (GM-HIN)
<Primary Provider> = Dr. Doctor
<EHR> = Physician's Choice Office-base Electronic Health Record (OfficeEHR) used by Dr. Doctor
<Health Plan> = Evergreen Health
<PBM> = MultiState Rx Plan
<Pharmacy> = SmallTown Pharmacy

Adam Everyperson has decided to exert greater control over his health and healthcare. As part of his self-reliant approach, Mr. Everyperson decides that he will maintain his own Personal Health Record. After examining various options, Mr. Everyperson decides to use the web-based Personal Health Record available from WebExcellent (WebPHR). Mr. Everyperson provides basic demographic information to identify himself to WebPHR and establishes an account [Select PHR]. Mr. Everyperson also establishes that his spouse, Mary Everyperson, and primary physician, Dr. Doctor, can view the information in his PHR and that his PHR can be accessible, on an emergency basis, via the Greater Metropolitan Health Information Network (GM-HIN) [Consumer Consent].

Based upon information provided by Mr. Everyperson, WebPHR establishes relationships [Subscribe] with GM-HIN, Dr. Doctor's Electronic Health Record (OfficeEHR), Evergreen Health (Mr. Everyperson's Health Plan), MultiState Rx Plan (a Pharmacy Benefit Manager), SmallTown Pharmacy (Pharmacy) and other similarly related applications as Mr. Everyperson's PHR.

In the course of its operation, GM-HIN receives documents from a number of participating organizations, including Dr. Doctor's OfficeEHR. This requires that patient identities must be matched [Patient Identity Feed & PIX Query or Patient Demographics Query] and documents must be appropriately indexed and stored [Provide & Register (Registration/MedicationHx)]. GM-HIN may interact with additional information sources, such as Evergreen Health, SmallTown Pharmacy and MultiState Rx Plan. Alternatively, these additional sources can send information into WebPHR directly or through another application. The level of detail of data exchanged between PHR and EHR systems depends upon information contained in these systems. The definition of problems as major medical conditions depends upon the clinical judgment of the consumer's trusted healthcare providers.

In order to initially populate Mr. Everyperson's PHR, WebPHR requests information from GM-HIN on behalf of Mr. Everyperson. This requires first matching that WebPHR and GM-HIN both recognize Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query] and determining what relevant documents are contained in GM-HIN [Query Documents]. Once the documents are identified, WebPHR retrieves particular documents of interest [Retrieve Documents. This may happen multiple times because of multiple documents].

WebPHR consolidates the information provided by Mr. Everyperson and the documents that have been retrieved and presents that information to Mr. Everyperson [Retrieve Document Set (using HITSP/C32)].

The nature of this consolidation and, in particular the reconciliation of duplicates, is outside the scope of this document. Mr. Everyperson reviews the information and realizes that some of the information is out of date and other information is not correct from his recollection. Mr. Everyperson updates the information as it is stored in WebPHR [Provide and Register Document Set (using HITSP/C32)]. WebPHR passes updated documentation along to GM-HIN, as allowed by the access and consents set up by Mr. Everyperson.

Summary Documents Using HL7 Continuity of Care Document (CCD) Component

The Summary Documents Using HL7 Continuity of Care Document (CCD) Component (HITSP/C32) describes the document content that summarizes a consumer's registration and healthcare summary data information for the purpose of information exchange with a PHR system.

NOTE: This does not describe the content of the PHR, but the exchange of information with a PHR system.

The document consists of content modules that contain multiple data elements. The list of content modules is presented in Table 3.2.2-1. Subsequent sections indicate those content modules which are required in particular transaction/content subsets.

Table 3.2.2-1 HITSP/C32 Content Modules in this IS

Content Module
Person Information
Language Spoken
Support
Healthcare Provider
Insurance Provider
Allergies and Drug Sensitivity
Condition
Medications – Prescription and Non-Prescription
Pregnancy
Information Source
Comments
Advance Directive
Immunization
Vital Sign
Result
Encounter
Procedure

HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD), as a whole, contains a designated author that is the consumer and/or their designated agent, such as the parent of a minor child. Every content module; such as a medication, allergy, or problem; contains an author that defaults to the document author or authors unless otherwise specified. When data are copied from another source, such as medication history information from a PBM, the original source and author (such as the prescribing healthcare provider) shall be retained. A consumer shall only edit data that they entered themselves, but they may add a comment (for which they will be the author) to specific content modules in the record or delete any data element they wish to remove from their record. Users should be aware that changing consumer demographics or financial data may cause future consumer linkages and queries to fail. Requesting changes to data in external systems, such as a health plan system that would correct errors in a field such as name or indicate changes in address or phone number is not addressed by this specification and has been identified as a gap.

Lab Report Document

HITSP/C37 - Lab Report Document describes the document content that summarizes a set of consumer's laboratory test results for the purpose of information exchange with a PHR system.

This document is intended to hold a complete set of laboratory test results (e.g. resulting from one or more orders). It allows the consumer to maintain the structured and coded form in his or her PHR system a laboratory report in a source attested manner (laboratory or EHR system where the report was created). The laboratory results section in the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) serves a complementary purpose in allowing selected lab results relevant in the context of the summary to be included (e.g. abnormal results that resulted in a specific diagnosis or in medication being prescribed).

3.2.2.1 Consumer Creates Account to Host Health Information Scenario Actor Interactions

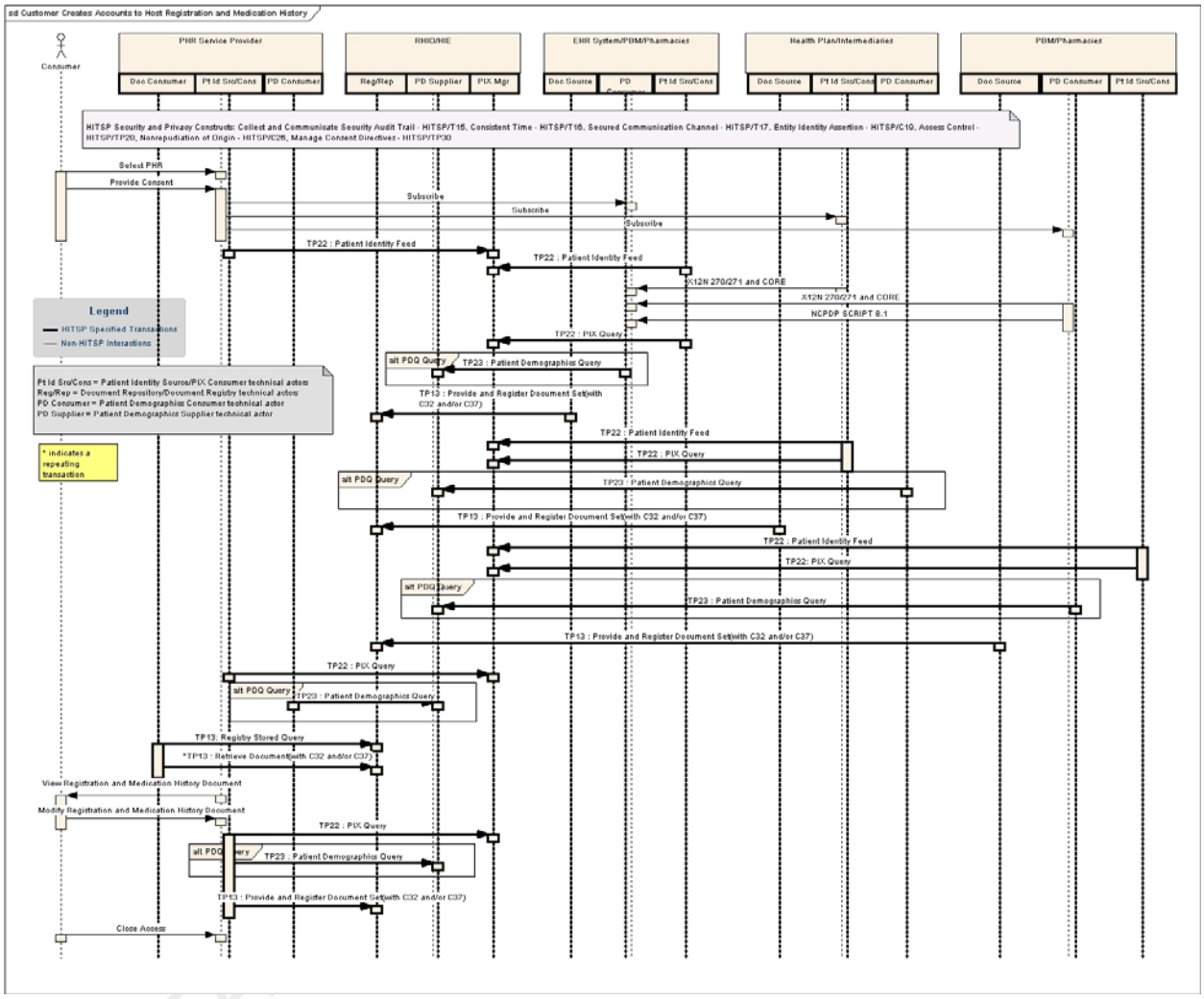
Health Plans/Intermediary and PBM/Pharmacy have two approaches for conveying information to their member's/enrollee's PHRs:

- They may choose to act as a direct source of information as a Document Source by using the X12 270/271 and CORE or NCPDP SCRIPT mapping defined in Section 6.2 and Section 6.1 of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) respectively.
- Alternatively, a provider may act as an intermediary for its consumers in retrieving their information from Health Plans/Intermediary and PBM/Pharmacy through the use of X12 270/271 and CORE or NCPDP SCRIPT transactions and convey it to their PHR as defined by this Interoperability Specification (see EHR system as Document Source)

Health Plans/Intermediary and PBM/Pharmacy may in addition provide PHR services. This is simply the grouping of the technical actors (and collapse of the transactions) defined for the combined business actors.

The sequence diagram for this scenario is shown in Figure 3.2.2.1-1. For simplification, please note that Security and Privacy transactions may not be reflected in the following detailed technical design UML diagram.

Figure 3.2.2.1-1 Customer Creates Accounts to Host Registration and Medication History



3.2.2.1.1 Transaction Descriptions

The transactions shown with thin lines, are either out of scope (not specified in this Interoperability Specification) because they do not pose specific interoperability issues (e.g. web browsing) to support the Use Case, or are handled at this time through non-electronic communication (e.g. subscribe transaction).

The directions of the arrows are based upon the initiator of the transaction, not the primary flow of data or document. For example, when a Document Consumer wishes to obtain documents from a Document Repository, the arrow flows from the Document Consumer to the Document Repository (i.e. the arrow shows the Retrieve request). The transactions actually include the request, response and acknowledgements.

The Subscribe Transaction is intended to represent the necessary establishment of a business relationship between a consumer's PHR service provider and a source of data for the consumer such as a provider, health plan/intermediary or PBM/pharmacy. In a future version of this Interoperability Specification one may envision the need to specify a standards based Subscribe Transaction for the consumer to establish a reciprocal information path into the consumer's PHR.

All gaps and standards overlaps for each scenario are identified in Section 4.2 and Section 4.3.

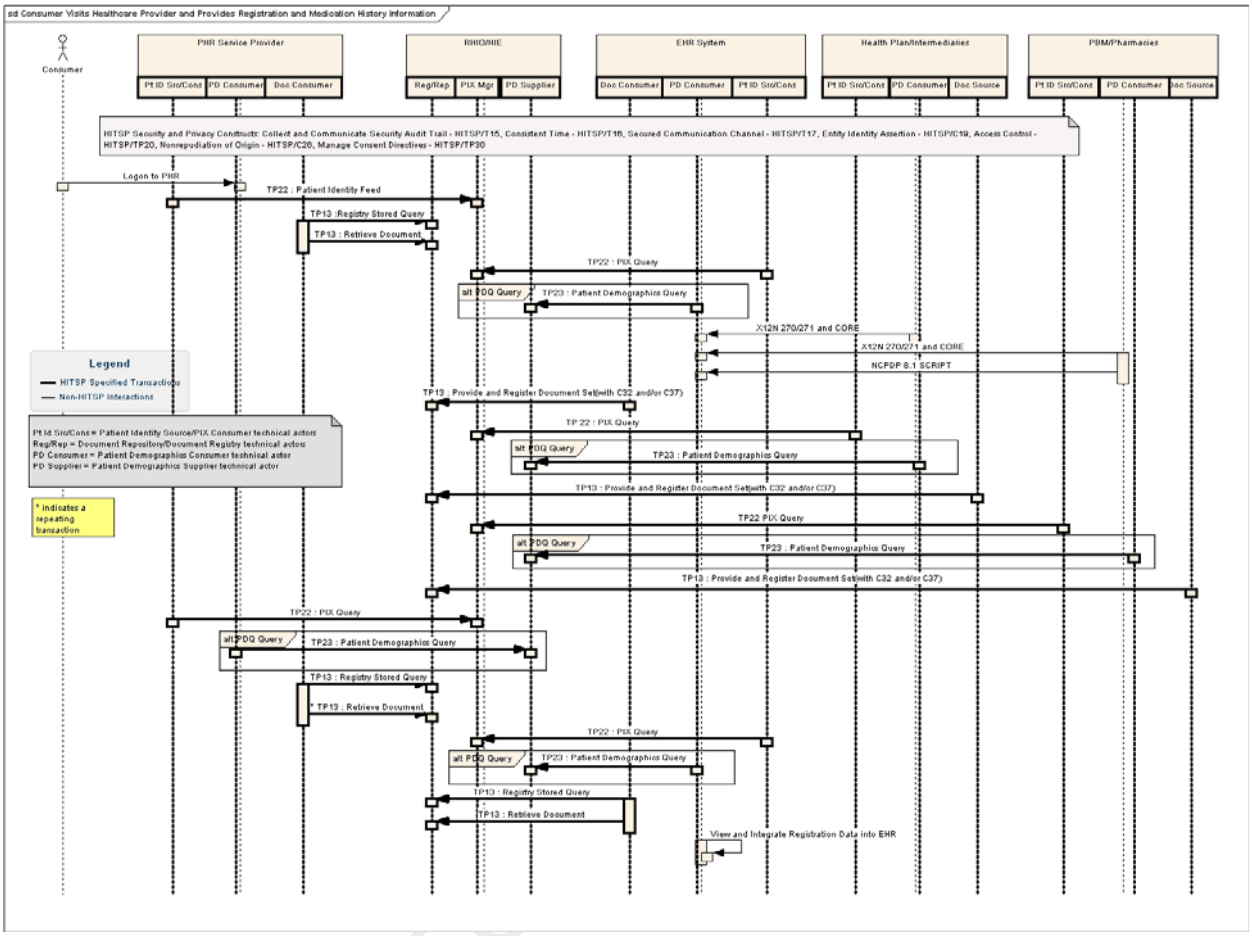
The detailed technical requirements for the transactions shown in Figure 3.2.2.1-1 are specified further in section 3.2.3.

3.2.2.2 Consumer Visits Healthcare Provider and Provides Registration and Medication History and/or Laboratory Information Scenario Actor Interactions

Adam Everyperson has an appointment coming up with his primary provider, Dr. Doctor. He wants to make sure that his address, insurance and other similar information is up to date in his PHR and, thus, available to Dr. Doctor. Mr. Everyperson selects pertinent information from his PHR system (<PHR>), extracts it from this system (<PHR>), formats into the appropriate document format (as per HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and/or HITSP/C37 - Lab Report Document) and transfers it to WebPHR for sharing with his provider as described in HITSP/T13 - Manage Sharing of Documents. WebPHR has established relationships to GM-HIN (or other systems). Prior to sending any documents to be shared, WebPHR ensures that the patient identity of the documents being submitted for transfer is cross-referenced to the patient identity that the GM-HIN will recognize.

The sequence diagram for this scenario is shown in Figure 3.2.2.2-1. For simplification, please note that Security and Privacy transactions may not be reflected in the following detailed technical design UML diagram.

Figure 3.2.2.2-1 Consumer Visits Healthcare Provider and Provides Registration and Medication History Information



3.2.2.2.1 Transaction Descriptions

The detailed technical requirements for the transactions shown in Figure 3.2.2.2-1 are specified in Section 3.2.3. The follow narrative provides a high level walk though of the flow in the context of a fictitious scenario.

Adam Everyperson has an appointment coming up with his primary provider, Dr. Doctor. He wants to make sure that his address, insurance and other similar information is up to date in his PHR and, thus, available to Dr. Doctor.

Mr. Everyperson connects to WebPHR and identifies himself [Logon to PHR]. For external information, WebPHR requests documents from GM-HIN on behalf of Mr. Everyperson. This requires first matching that WebPHR and GM-HIN both recognize Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query] and determining what relevant documents are contained in GM-HIN [Registry Stored Query]. Once the documents are identified, WebPHR retrieves particular documents of interest [Retrieve Documents Set, this may happen multiple times because of multiple documents].

In the course of its operation, GM-HIN receives documents from a number of participating organizations, including Dr. Doctor's OfficeEHR. Patient identities must be matched [Patient Identity Feed & PIX Query OR Patient Demographics Query] and documents must be appropriately indexed and stored [Provide & Register Document Set].

Mr. Everyperson requests an update of the external information in his PHR. WebPHR requests updated information from GM-HIN, and other information sources, on behalf of Mr. Everyperson. This requires that WebPHR has established relationships to GM-HIN (or other system) [subscribe], and then match that WebPHR and GM-HIN both recognize Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query] and determine what relevant documents are contained in GM-HIN [Registry Stored Query]. Once the documents are identified, WebPHR retrieves particular documents of interest [Retrieve Documents Set (using HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and/or HITSP/C37 - Lab Report Document)].

Upon arriving for his appointment with Dr. Doctor, Mr. Everyperson is handed the standard visit forms to fill out. He advises the office staff that his information is available via WebPHR. The office staff enters the appropriate information (e.g. patient identification, authorization, etc) into OfficeEHR to retrieve Mr. Everyperson's information from WebPHR via GM-HIN. OfficeEHR queries GM-HIN to match that OfficeEHR and GM-HIN both recognized Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query]. OfficeEHR requests information on relevant documents contained in GM-HIN [Registry Stored Query], and retrieves the current Registration and Medication History as well as Laboratory Reports document(s) [Retrieve Documents Set (using HITSP/C32 and/or HITSP/C37].

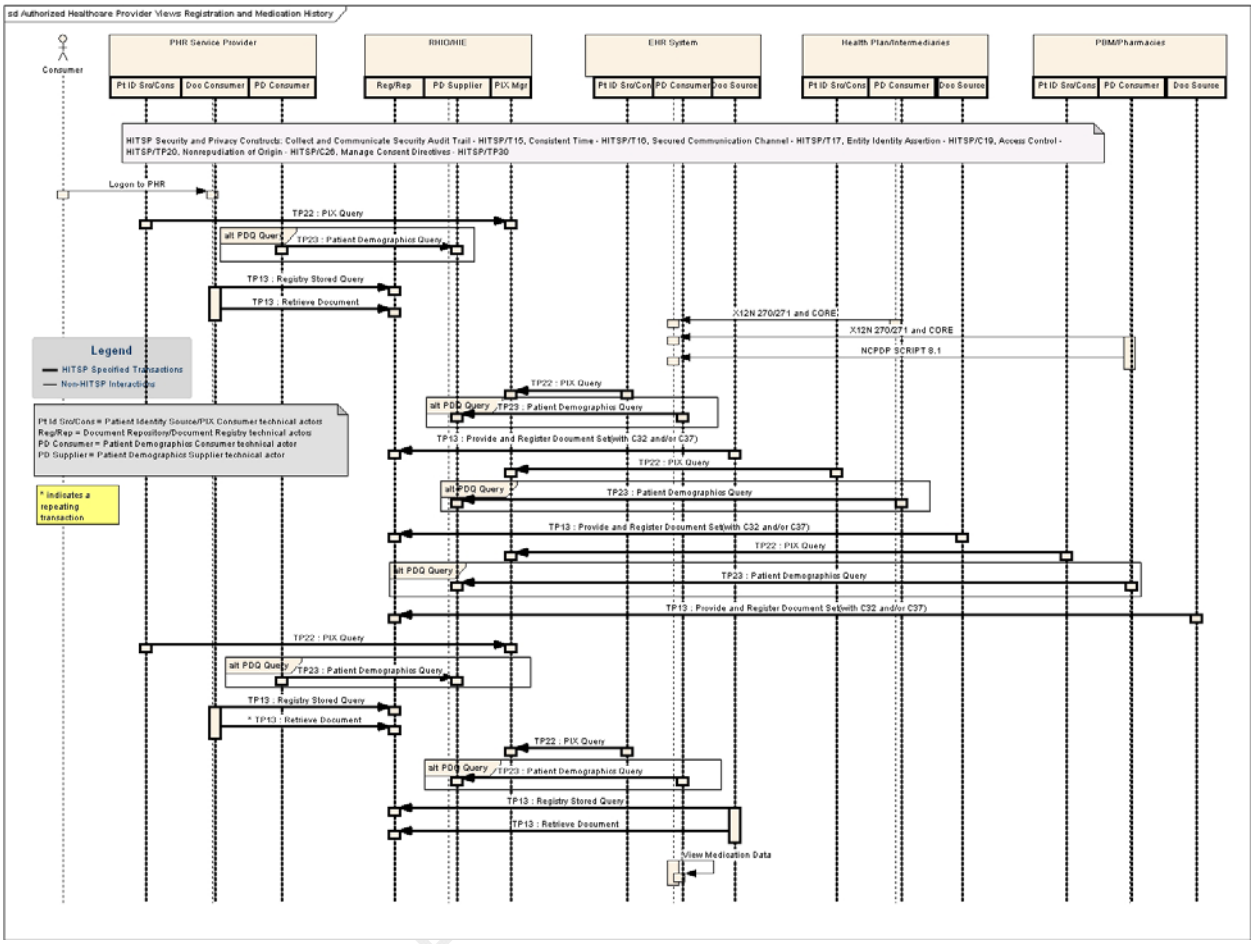
OfficeEHR presents the Summary Document to the office staff and Dr. Doctor, who then determine if the information should be posted into the OfficeEHR record for Mr. Everyperson [Document Consumer (with Content Consumer/Document Import Option)].

3.2.2.3 Authorized Healthcare Provider Reviews Registration and Medication History Scenario Actor Interactions

Upon arriving for his appointment with Dr. Doctor, Mr. Everyperson advises the office staff that his information is available via WebPHR. The office staff enters the appropriate information (e.g. patient identification, authorization, etc) into OfficeEHR to retrieve Mr. Everyperson's information from WebPHR (via GM-HIN). OfficeEHR queries GM-HIN to match that OfficeEHR and GM-HIN both recognized Mr. Everyperson. OfficeEHR requests information on relevant documents contained in GM-HIN, and retrieves the current Registration Summary and Medication History document(s). OfficeEHR presents the retrieved documents to the office staff and Dr. Doctor, who then determine if the information should be posted into the OfficeEHR record for Mr. Everyperson.

The sequence diagram is shown in Figure 3.2.2.3-1. For simplification, please note that Security and Privacy transactions may not be reflected in the following detailed technical design UML diagram.

Figure 3.2.2.3-1 Authorized Healthcare Provider Views Registration and Medication History



3.2.2.3.1 Transaction Descriptions

The detailed technical requirements for the transactions shown in Figure 3.2.2.3-1 are specified in Section 3.2.3. The following narrative provides a high level walk through of the flow in the context of a fictitious scenario.

Adam Everyperson has an appointment coming up with his primary provider, Dr. Doctor. He wants to make sure that his latest medications, including over-the-counter and herbals, are appropriately listed in his PHR and, thus, available to Dr. Doctor.

Mr. Everyperson connects to WebPHR and identifies himself [Logon to PHR]. For external information, WebPHR requests documents from GM-HIN on behalf of Mr. Everyperson. This requires first matching that WebPHR and GM-HIN both recognize Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query] and determining what relevant documents are contained in GM-HIN [Registry Stored Query]. Once the documents are identified, WebPHR retrieves particular documents of

interest [Retrieve Documents Set (using HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and/or HITSP/C37 - Lab Report Document].

In the course of its operation, GM-HIN receives documents from a number of participating organizations, including Dr. Doctor's OfficeEHR. Patient identities must be matched [Patient Identity Feed & PIX Query OR Patient Demographics Query] and documents must be appropriately indexed and stored [Provide & Register Document Set]. GM-HIN may interact with additional information sources, such as Evergreen Health, SmallTown Pharmacy, and MultiState Rx Plan. Alternatively, these additional sources can send information into GM-HIN through another application, such as OfficeEHR, that consolidates the information into a common format.

Mr. Everyperson requests an update of the external information in his PHR. WebPHR requests updated information from GM-HIN, and other information sources, on behalf of Mr. Everyperson. This requires that WebPHR has established relationships to GM-HIN (or other system) [subscribe], and then ensures that WebPHR and GM-HIN both recognize Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query] and determines what relevant documents are contained in GM-HIN [Registry Stored Query]. Once the documents are identified, WebPHR retrieves particular documents of interest [Retrieve Documents Set (using HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and/or HITSP/C37 - Lab Report Document].

Upon arriving for his appointment with Dr. Doctor, Mr. Everyperson is handed a current medication form to fill out. He advises the office staff that his information is available via WebPHR. The office staff enters the appropriate information (e.g. patient identification, authorization, etc) into OfficeEHR to retrieve Mr. Everyperson's information from WebPHR (via GM-HIN). OfficeEHR queries GM-HIN to match that OfficeEHR and GM-HIN both recognized Mr. Everyperson [Patient Identity Feed & PIX Query OR Patient Demographics Query]. OfficeEHR requests information on relevant documents contained in GM-HIN [Registry Stored Query], and retrieves the current Registration and Medication History document(s) [Retrieve Documents Set (using HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and/or HITSP/C37 - Lab Report Document].

OfficeEHR presents the Summary Document to the office staff and Dr. Doctor, who then determine if the information should be posted into the OfficeEHR record for Mr. Everyperson [Document Consumer (with Content Consumer / Document Import Option)].

For the most up-to-date and complete information, it is recommended that at the end of a healthcare encounter the new registration/medication history data are pushed to the document repository/registry. For example, Mr. Everyperson is seen in the emergency department at a local hospital the night before a visit to Dr. Doctor. Dr. Doctor submits a new medication history request query, but there is an interval when MultiState Rx Plan had not yet processed the new medication (e.g. the night before) and published it to GM-HIN. If the emergency department did not push the information to the repository, Dr. Doctor would not have access to that information unless Mr. Everyperson enters the data into their WebPHR. Dr. Doctor's query would also not return any medications administered by the emergency department.

It is the intent of this specification to allow for a complete, up to date, relevant registration and/or medication (or other clinical and laboratory data) history but it is not guaranteed by this specification.

3.2.2.4 Implementation and Architecture Variants

The three scenarios depicted in Section 3.2.2 assume a specific implementation architecture which is just one of the possible architectural variants that are supported for this HITSP/IS03 - Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification. Such flexibility is necessary to support environments where:

- No RHIO/HIE is established
- Data are stored in a centralized way or distributed among several repositories
- Some of the repositories are grouped with the source of Registration and Medication History Documents, and Laboratory Report Documents, others being shared as part of the RHIO/HIE infrastructure

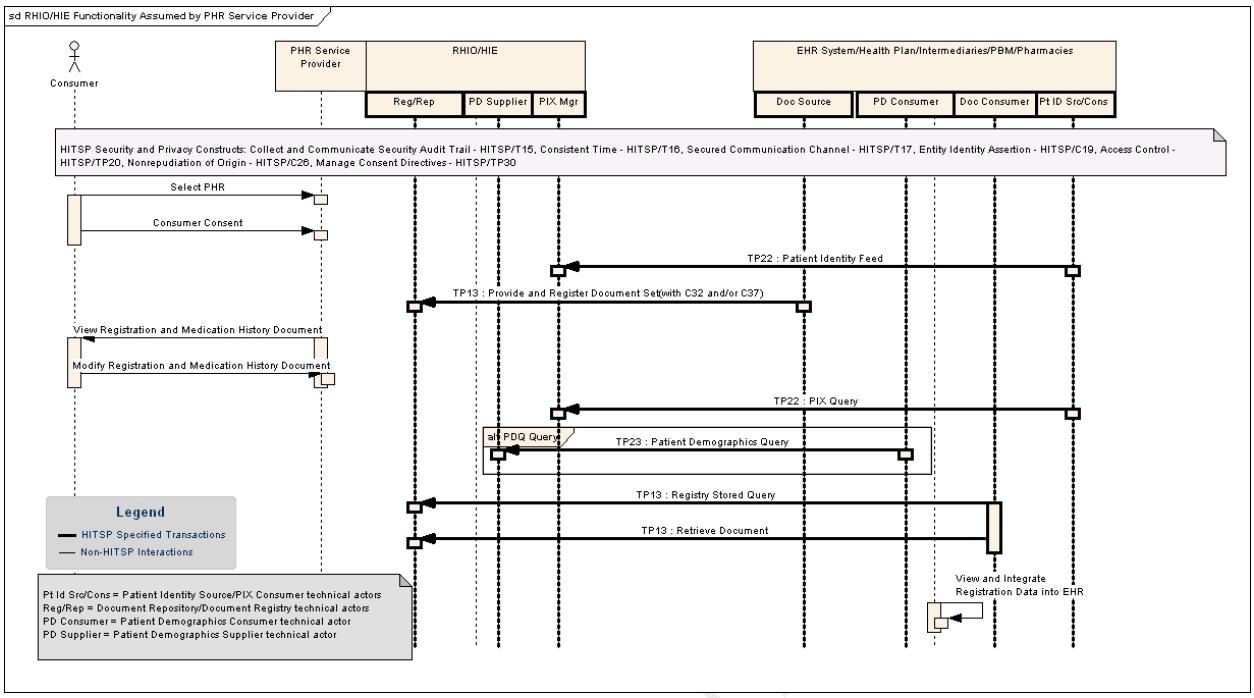
In some situations, some business actors may be grouped to support cases such as when a PHR Service is provided by a Healthcare Provider or a Payer; or the functionality of a RHIO/HIE may be subsumed by the PHR Service Provider,

Five examples are provided to illustrate these many possible variants. This is a fluid and evolving area of healthcare technology and, as such, the examples shown are only a small subset of all possible variants. They leverage a subset of the transactions and business actors defined for the Use Cases, but do not attempt to present all business actors or transactions. Note that these examples include "actors" subsumed by other actors. This is intended to point out where functionality is consolidated, not to imply that those actors are separate and distinct. For simplification, please note that Security and Privacy transactions may not be reflected in the following detailed technical design UML diagrams.

Implementation/Architecture Variant A

In this variant, the PHR Service provider cannot rely on a RHIO/HIE. The tasks of the RHIO/HIE are performed by the PHR Service Provider and a number of transactions disappear and technical actors are combined. One should note that the other business actors (e.g. the Health Plan or the EHR system) use the very same transactions as when the RHIO/HIE exists as a separate business actor. Figure 3.2.2.4-1 is an example of this variant.

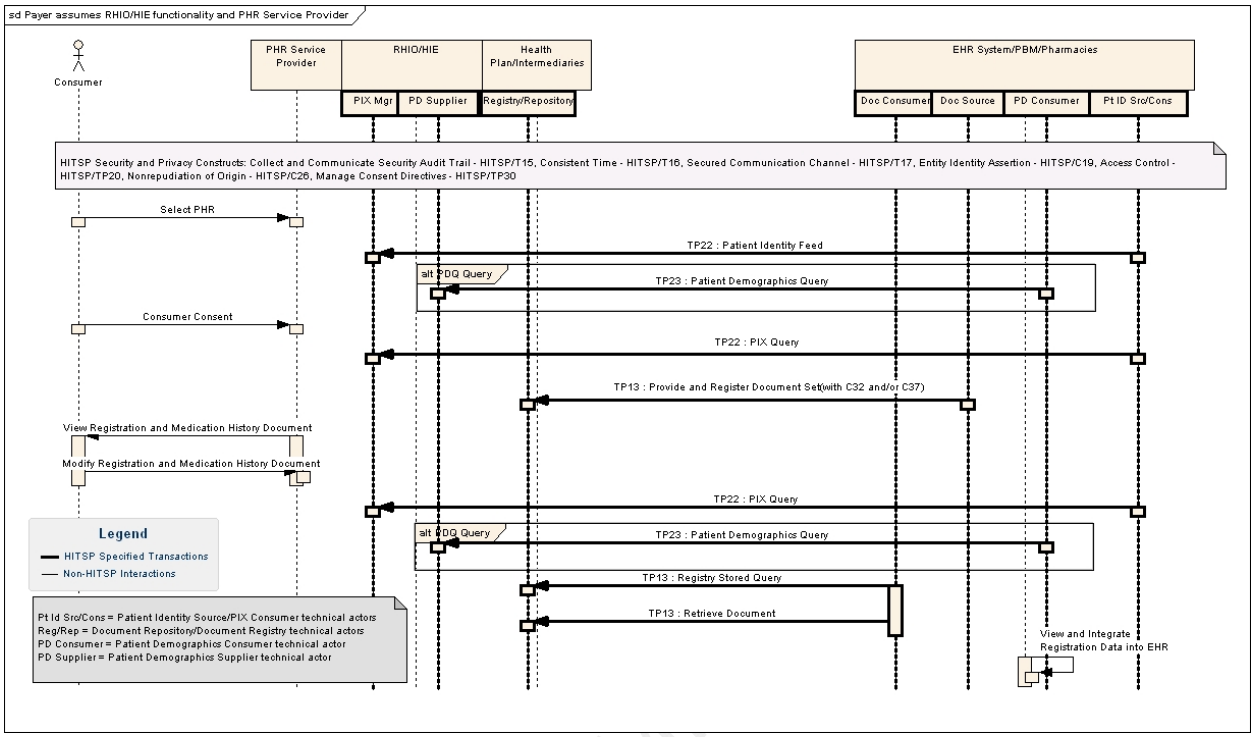
Figure 3.2.2.4-1 RHIO/HIE Functionality Assumed by PHR Service Provider



Implementation/Architecture Variant B

In this variant, the PHR Service provider cannot rely on a RHIO/HIE similar to as shown in variant A, and the PHR service is being offered by a payer. By combining three business actors, a number of transactions further disappear and technical actors are combined. One should note that the other business actors (e.g. the PBM, Pharmacy or the EHR system) use the very same transactions as when the business actors exist as separate entities. Figure 3.2.2.4-2 is an example of this variant.

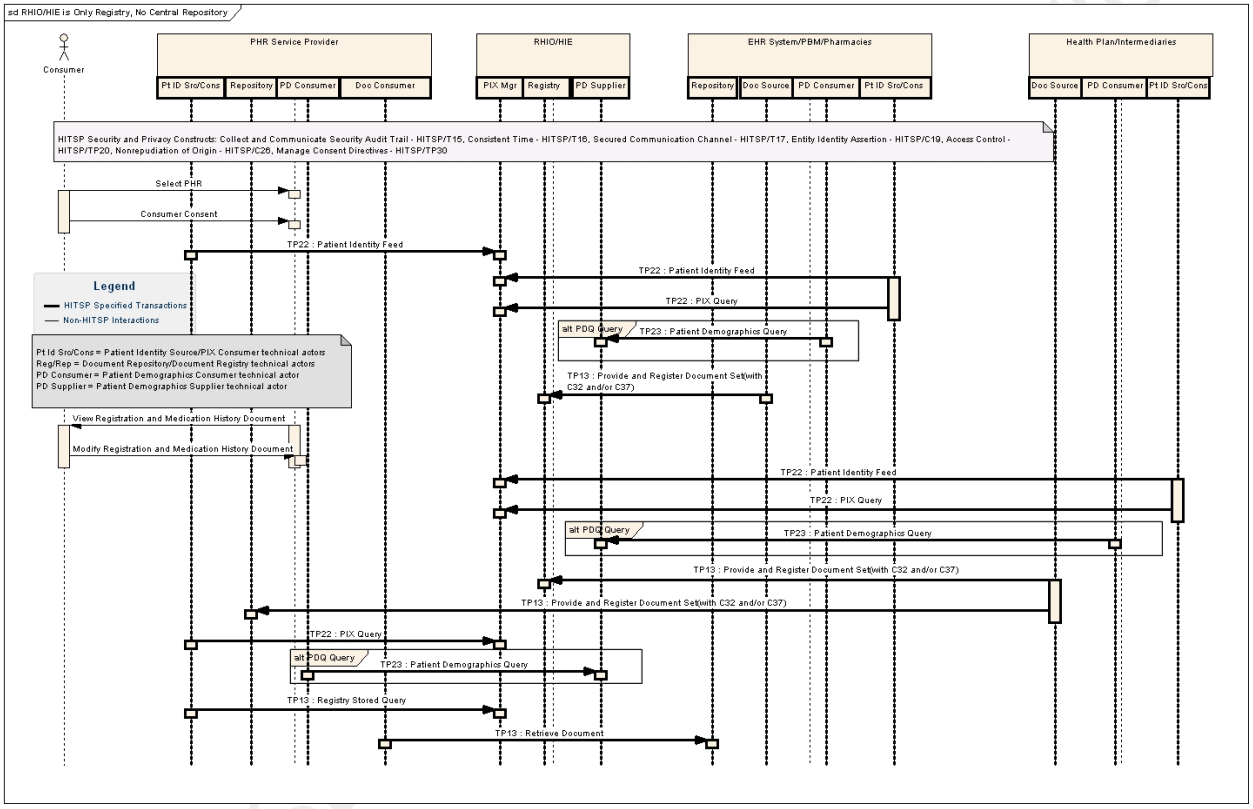
Figure 3.2.2.4-2 Payer assumes RHIO/HIE functionality and PHR Service Provider



Implementation/Architecture Variant C

In this variant, the RHIO/HIE does not offer any centralized document repository. Repositories are supported by the PHR for the Registration/Medication History (and Laboratory Report) documents the consumer creates and by the EHR system for the documents it creates. In this architecture, the RHIO/HIE supports only a record locator service (Document Registry technical actor) and an MPI (Patient ID Cross-Reference Manager). Again, there is no interoperability impact on the other business actors. Figure 3.2.2.4-3 is an example of this variant.

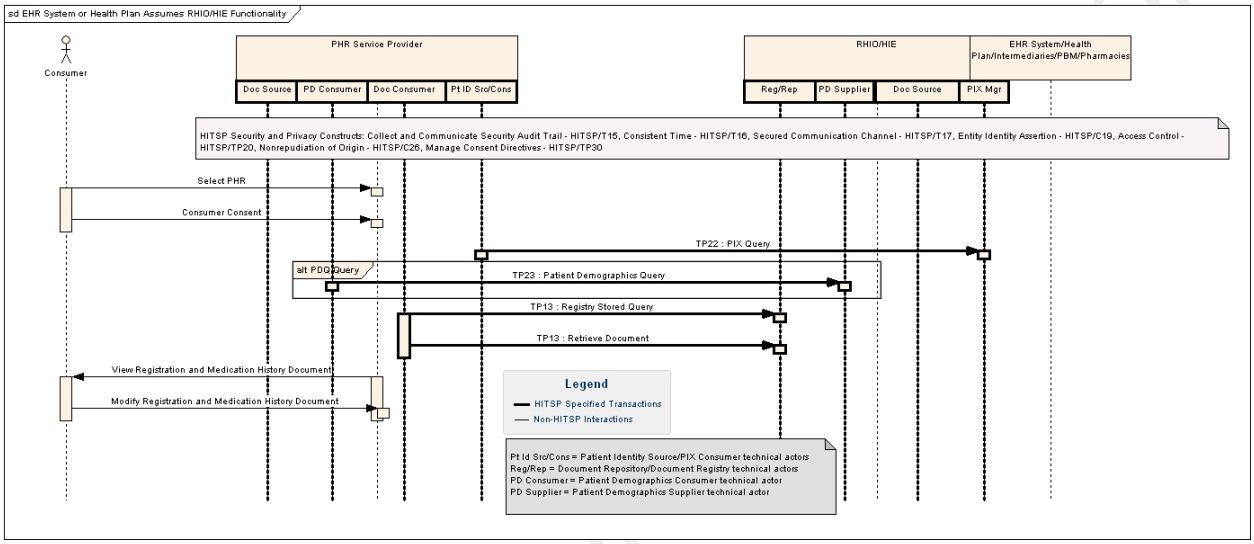
Figure 3.2.2.4-3 RHIO/HIE is Only Registry, No Central Repository



Implementation/Architecture Variant D

In this variant, the EHR system, PBM, Pharmacy or Health Plan is shown acting as a RHIO/HIE to expose access to consumer information stored in these systems. Once again, by combining business actors, a number of transactions have disappeared and technical actors are combined. In this architecture variant, consumer information flows to the PHR using the request/response model. Figure 3.2.2.4-4 is an example of this variant.

Figure 3.2.2.4-4 EHR System or Health Plan Assumes RHIO/HIE Functionality

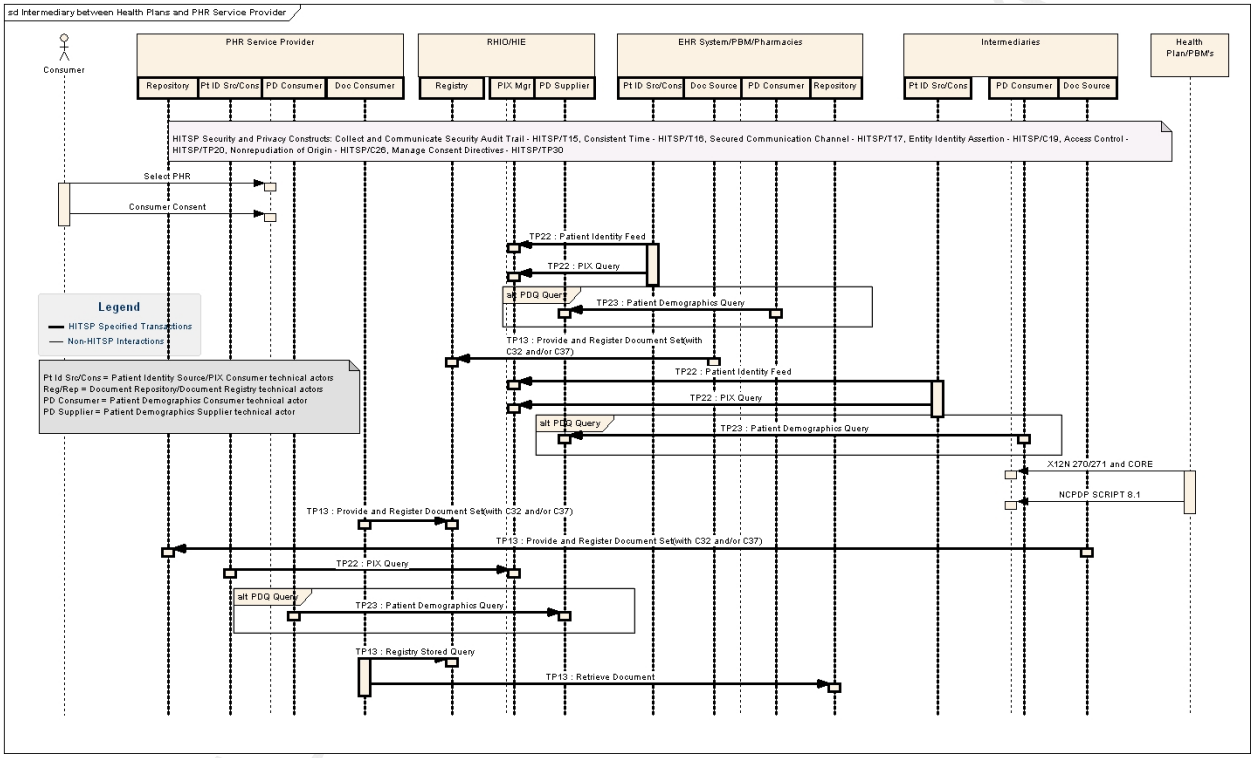


Implementation/Architecture Variant E

In this variant, there is a scenario technical actor serving as an intermediary acting as the Document Source between the Health Plan/PBM/Pharmacies and the PHR Service provider (the Document Repository) to perform message translation. Figure 3.2.2.4-5 is an example of this variant.

It should be noted, that the Documents need not be persisted by the source (e.g. Health Plan, Pharmacy/Intermediaries, etc.). It may either provide an X270/X271 to another party (e.g., EHR system or intermediary as shown in this variant E) or create and provide the Registration and Medication History documents to an entity where it will be persisted (e.g., RHIO/HIE, PHR system such as variant A, B, C).

Figure 3.2.2.4-5 Intermediary between Health Plans and PHR Service Provider



The architectural flexibilities illustrated in the five variants allow the same edge system implementations to be supported, and a wide range of architectures to be supported.

3.2.3 MAPPING OF BUSINESS ACTORS TO TECHNICAL ACTORS AND CONSTRUCTS WITH OPTIONALITY

The table below maps the individual business actors defined in the Interoperability Specification and depicted in the above detailed UML sequence diagram. Table 3.2.3-1 below specifies the requirements associated to each business actor in the Interoperability Specification. For each implemented business actor, the table specifies:

1. All Required or Conditionally Required technical actors listed for the business actor shall be supported as specified in the associated construct
2. Optional technical actors listed for the business actor may be supported as specified in the associated construct
3. All Required or Conditionally Required transactions and content subsets listed for each implemented technical actor assigned to the business actor shall be supported as specified in the associated construct
4. Optional transactions and content subsets listed for each implemented technical actor assigned to the business actor may be supported as specified in the associated construct

This table also includes the corresponding technical actors associated with the relevant Security and Privacy constructs that are used for this Interoperability Specification. Section 1.2 provides a summary description of all the referenced HITSP constructs.

Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
Personal Health Record (PHR) Service Provider	Patient Identity Source	C [101]	HITSP/TP22	Patient Identity Feed	R
	PIX Consumer	C [101]	HITSP/TP22	PIX Query	R
				PIX Update Notification	O
	Patient Demographics Consumer	C [101]	HITSP/T23	Patient Demographics Query	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set-b	R
	Document Consumer	R	HITSP/TP13	Registry Stored Query	R
				Retrieve Document Set	R
	Document Repository	O	HITSP/TP13	Retrieve Document Set	R
				Register Document Set-b	R
				Provide & Register Document Set-b	R
	Document Registry	O	HITSP/TP13	Patient Identity Feed	R
				Registry Stored Query	R
				Provide and Register Document Set-b	R
	Content Creator	R	HITSP/C32	Creator-Registration Subset (see Section 3.2.3.1)	C[201]
				Creator-Registration-Coded Subset (see Section 3.2.3.2)	C[201]
				Creator-Medication and Immunization History Subset (see Section 3.2.3.3)	C[201]
				Creator-Medication and Immunization History - Coded Subset (see Section 3.2.3.4)	C[201]
				Creator-Conditions and Allergy Subset (see Section 3.2.3.5)	C[201]
				Creator-Conditions and Allergy-Coded Subset (see Section 3.2.3.6)	C[201]

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Creator-Laboratory Section Subset (see Section 3.2.3.7)	C[201]
				Creator-Laboratory Section -Coded Subset (see Section 3.2.3.8)	C[201]
		R	HITSP/C37	Laboratory Report Document Component	C[201]
		R	HITSP/TP30	Consent Document Component	R
	Content Consumer	R	HITSP/C32	Consumer-Document Display Subset (see Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
		R	HITSP/C37	Consumer-Document Display Subset (see Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
		R	HITSP/TP30	Consent Document Component	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	C [103]	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R
	Consent Registry	O	HITSP/TP30	Register Document Set	R
				Stored Query	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Consent Repository	O	HITSP/TP30	Provide and Register Document Set	R
				Register Document Set	R
	Consent Directive Requester	R	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	User	R	HITSP/TP20	Access Control Request	O
	User Access Control Service (UACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	C [102]	HITSP/TP20	Access Control Request	O
	Service Provider Access Control Service (SP ACS)	C [102]	HITSP/TP20	Access Control Request	O
Regional Health Information Organizations /Health Information Exchange (RHIO/HIE)	PIX Manager	R	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
				PIX Update Notification	R
	Patient Demographics Supplier	R	HITSP/T23	Patient Demographics Query	R
	Document Registry	R	HITSP/TP13	PIX Identity Feed	R
				Registry Stored Query	R
				Register Document Set-b	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Document Set-b	R
				Provide & Register Document Set-b	R
	Initiating Gateway	O	HITSP/TP13	Cross Gateway Query	R
				Cross Gateway Retrieve	R
	Responding Gateway	O	HITSP/TP13	Cross Gateway Query	R
				Cross Gateway Retrieve	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Identity Provider	R	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	R	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Registry	R	HITSP/TP30	Register Document Set	R
				Stored Query	R
	Consent Repository	R	HITSP/TP30	Provide and Register Document Set	R
				Register Document Set	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	User	R	HITSP/TP20	Access Control Request	O
	User Access Control Service (UACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
	Service Provider Access Control Service (SP ACS)	R	HITSP/TP20	Access Control Request	O
Electronic Health Record (EHR) System	Patient Identity Source	C [101]	HITSP/TP22	Patient Identity Feed	R
	PIX Consumer	C [101]	HITSP/TP22	PIX Query	R
				PIX Update Notification	O
	Patient Demographics Consumer	C [101]	HITSP/T23	Patient Demographics Query	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set-b	R
	Document Consumer	R	HITSP/TP13	Registry Stored Query	R
				Retrieve Documents	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Documents Set-b	R
				Provide & Register Document Set-b	R
	Content Creator	R	HITSP/C32	Creator-Registration Subset (see Section 3.2.3.1)	C[201]
				Creator-Registration-Coded Subset (see Section 3.2.3.2)	C[201]
				Creator-Medication and Immunization History Subset (see Section 3.2.3.3)	C[201]
				Creator-Medication and Immunization History - Coded Subset (see Section 3.2.3.4)	C[201]
				Creator-Conditions and Allergy Subset (see Section 3.2.3.5)	C[201]
				Creator-Conditions and Allergy -Coded Subset (see Section 3.2.3.6)	C[201]
				Creator-Laboratory Section Subset (see Section 3.2.3.7)	C[201]
				Creator-Laboratory Section -Coded Subset (see Section 3.2.3.8)	C[201]
			HITSP/C37	Laboratory Report Document Component	C[201]
			HITSP/TP30	Consent Document Component	R
	Content Consumer	R	HITSP/C32	Consumer-Document Display Subset (see Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
			HITSP/C37	Consumer-Document Display Subset (see Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
			HITSP/TP30	Consent Document Component	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	C [103]	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Stored Query	R
	Consent Registry	O	HITSP/TP30	Provide and Register Document Set	R
				Register Document Set	R
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	User	R	HITSP/TP20	Access Control Request	O
	User Access Control Service (UACS)	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
	Service Provider Access Control Service (SP ACS)	R	HITSP/TP20	Access Control Request	O

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
Health Plan/Intermediary	Patient Identity Source	C [101]	HITSP/TP22	Patient Identity Feed	R
	PIX Consumer	C [101]	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/T23	Patient Demographics Query	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set-b	R
	Content Creator	R	HITSP/C32	Creator-Registration Subset (see Section 3.2.3.1)	C[201]
				Creator-Registration-Coded Subset (see Section 3.2.3.2)	C[201]
				Creator-Medication and Immunization History Subset (see Section 3.2.3.3)	C[201]
				Creator-Medication and Immunization History - Coded Subset (see Section 3.2.3.4)	C[201]
				Creator-Conditions and Allergy Subset (see Section 3.2.3.5)	C[201]
				Creator-Conditions and Allergy -Coded Subset (see Section 3.2.3.6)	C[201]
				Creator-Laboratory Section Subset (see Section 3.2.3.7)	C[201]
				Creator-Laboratory Section -Coded Subset (see Section 3.2.3.8)	C[201]
			HITSP/C37	Laboratory Report Document Component	C[201]
			HITSP/TP30	Consent Document Component	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	C [103]	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Stored Query	R
	Consent Registry	O	HITSP/TP30	Provide and Register Document Set	R
				Register Document Set	R
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	User	R	HITSP/TP20	Access Control Request	O
	User Access Control Service (UACS)	R	HITSP/TP20	Access Control Request	O
Pharmacy Benefit Manager (PBM)/Pharmacy	Patient Identity Source	C [101]	HITSP/TP22	Patient Identity Feed	R
	PIX Consumer	C [101]	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/T23	Patient Demographics Query	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set-b	R
	Content Creator	R	HITSP/C32	Creator-Registration Subset (see Section 3.2.3.1)	C[201]
				Creator-Registration-Coded Subset (see Section 3.2.3.2)	C[201]
				Creator-Medication and Immunization History Subset (see Section 3.2.3.3)	C[201]
				Creator-Medication and Immunization History - Coded Subset (see Section 3.2.3.4)	C[201]
				Creator-Conditions and Allergy Subset (see Section 3.2.3.5)	C[201]
				Creator-Conditions and Allergy -Coded Subset (see Section 3.2.3.6)	C[201]
				Creator-Laboratory Section Subset (see Section 3.2.3.7)	C[201]
				Creator-Laboratory Section -Coded Subset (see Section 3.2.3.8)	C[201]
			HITSP/C37	Laboratory Report Document Component	C[201]
			HITSP/TP30	Consent Document Component	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	C [103]	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Repository	O	HITSP/TP30	Register Document Set	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Stored Query	R
	Consent Registry	O	HITSP/TP30	Provide and Register Document Set	R
				Register Document Set	R
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	User	R	HITSP/TP20	Access Control Request	O
	User Access Control Service (UACS)	R	HITSP/TP20	Access Control Request	O

*** NOTE:** Optionality **=** "R" for Required, or "O" for Optional, or "C" for Conditional. Conditional footnotes are further described below.

Actor Optionality Conditions

C [101] - Shall support (Patient Identity Source plus PIX Consumer) and/or Patient Demographics Consumer

C [102] - Required if Access Control Request transaction is not supported.

C [103] - Required when a Document Repository and/or a Document Registry is supported.

Transaction/Content (T/C) Optionality Conditions

C [201] - Shall support either at least one of the subsets of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) or the HITSP/C37 - Lab Report Document, or both.

3.2.3.1 C32 "Creator-Registration Subset"

This subset impacts the content of the HITSP/C32 - Summary Document Using HL7 Continuity of Care Document (CCD) document produced by a Content Creator Technical Actor. It requires the Content Creator to have the **ability to create the content** of the following content modules for the purpose of exchange, with variants as specified in the HITSP/C32 construct:

Table 3.2.3.1-1 Creator Registration Subset Content Modules

Content Modules	Optionality
Person Information	R
Language Spoken	R2
Support	R2
Healthcare Provider	R2
Insurance Provider	R2
Pregnancy	R2
Information Source	R2
Comments	R2
Advance Directive	R2

NOTE: Optionality **=** “R” for Required, “R2” for Required if known, “O” for Optional, or “C” for Conditional.

Additional HITSP/C32 Content Modules may be present, but are not required in this subset. Within the context of this subset, the Content Consumer is not required to recognize or process such "additional" Content Modules.

The type of payer and type of payer entries contain the concepts but without the HITSP/C32 specified code set.

3.2.3.2 C32 “Creator-Registration-Coded Subset”

This subset is identical to the Creator-Registration Subset but requires the creation of type of payer and type of payer entries with the HITSP/C32 specified code set.

3.2.3.3 C32 “Creator-Medication and Immunization History Subset”

This subset impacts the content of the HITSP/C32 - Summary Document Using HL7 Continuity of Care Document (CCD) document produced by a Content Creator Technical Actor. It requires the Content Creator to have the ability to create the content of the following content module for the purpose of exchange, with variants as specified in the HITSP/C32 construct:

Table 3.2.3.3-1 Creator Medication and Immunization History Subset Content Modules

Content Modules	Optionality
Person Information	R
Healthcare Provider	R2
Medications – Prescription and Non-Prescription	R2
Information Source	R2
Comments	R2
Immunization	R2

NOTE: Optionality **=** “R” for Required, “R2” for Required if known, “O” for Optional, or “C” for Conditional.

Additional HITSP/C32 content modules may be present, but are not required in this subset. Within the context of this subset, the content consumer is not required to recognize or process such "additional" content modules.

The Medication entry may contain the concepts but without an associated code.

3.2.3.4 C32 “Creator-Medication and Immunization History-Coded Subset”

This subset is identical to the Creator-Medication Subset but requires the creation of medication entries with the HITSP/C32 specified code sets.

3.2.3.5 C32 “Creator-Conditions and Allergy Subset”

This subset impacts the content of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) document produced by a Content Creator Technical Actor. It requires the Content Creator to have the ability to create the content for the purpose of exchange as specified in the HITSP/C32 construct:

Table 3.2.3.5-1 Creator Conditions and Allergy Subset Content Modules

Content Modules	Optionality
Person Information	R
Healthcare Provider	R2
Condition	R2
Allergies and Drug Sensitivity	R2
Information Source	R2
Comments	R2

NOTE: Optionality **=** “R” for Required, “R2” for Required if known, “O” for Optional, or “C” for Conditional.

Additional HITSP/C32 content modules may be present, but are not required in this subset. Within the context of this subset, the content consumer is not required to recognize or process such "additional" content modules.

The Condition and Allergy entries contain the concepts but without the HITSP/C32 specified code set.

3.2.3.6 C32 “Creator-Conditions and Allergy-Coded Subset”

This subset is identical to the Creator-Registration Subset but requires the creation of conditions and allergies entries with the HITSP/C32 specified code set.

3.2.3.7 C32 “Creator-Laboratory Section Subset”

This subset impacts the content of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) document produced by a Content Creator Technical Actor. It requires the Content Creator to have the ability to create the content for the purpose of exchange as specified in the HITSP/C32 construct:

Table 3.2.3.7-1 Creator Laboratory Subset Content Modules

Content Modules	Optionality
Person Information	R
Healthcare Provider	R2
Result	R2
Information Source	R2
Comments	R2

NOTE: Optionality **=** “R” for Required, “R2” for Required if known, “O” for Optional, or “C” for Conditional.

Additional HITSP/C32 Content Modules may be present, but are not required in this subset. Within the context of this subset, the Content Consumer is not required to recognize or process such "additional" Content Modules.

The Result entries contain the concepts but without the HITSP/C32 specified code set.

3.2.3.8 C32 “Creator-Laboratory Section-Coded Subset”

This subset is identical to the Creator-Laboratory Section Subset but requires the creation of laboratory results entries with the HITSP/C32 specified code set.

3.2.3.9 Consumer-Document Display Subset

This subset impacts the import of Documents processed by a Content Consumer Technical Actor. It requires the Document Consumer only to have the ability to display either document (e.g. HITSP/C32, HITSP/C37) as requested (it may not be able to locally import it in the patient record).

3.2.3.10 Consumer-Document Import Subset

This subset impacts the import of Documents processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import into the patient record either of the documents (e.g. HITSP/C32, HITSP/C37) as a whole and display it as requested.

3.2.3.11 C32 “Consumer-Registration Discrete Data Import Subset”

This subset impacts the import of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) document processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import the discrete data from one or more of the registration entries in a structured form into the patient record. Coded values shall be maintained

3.2.3.12 C32 “Consumer-Medication and Immunization History Discrete Data Import Subset”

This subset impacts the import of the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) document processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import the discrete data from one or more of the medication and immunization history entries in a structured form into the patient record. Coded values shall be maintained

3.2.3.13 C32 “Consumer-Conditions and Allergy Discrete Data Import Subset”

This subset impacts the import of the HITSP/C32 - Summary Documents using HL7 Continuity of Care Document (CCD) document processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import the discrete data from one or more of the conditions and allergy entries in a structured form into the patient record. Coded values shall be maintained.

3.2.3.14 C32 “Consumer-Laboratory Discrete Data Import Subset”

This subset impacts the import of the HITSP/C32 - Summary Documents using HL7 Continuity of Care Document (CCD) document processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import the discrete data from one or more of the laboratory entries in a structured form into the patient record. Coded values shall be maintained.

3.2.3.15 C37 “Consumer-Lab Report Discrete Data Import Subset”

This subset impacts the import of HITSP/C37 - Lab Report Document document processed by a Content Consumer Technical Actor. It requires the Document Consumer to have the ability to import the discrete data from one or more of the entries in a structured form into the patient record. Coded values shall be maintained.

3.2.4 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 construct. To support a dependent construct, a technical actor must implement all the required actions in the pre-requisite construct, or be grouped together with another construct as specified in the table below:

Table 3.2.4-1 Construct Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
HITSP/T15 - Collect and Communicate Audit Trail	HITSP/T16 - Consistent Time	Pre-condition	Pre-requisites for Use Cases
HITSP/TP13 - Manage Sharing of Documents	HITSP/T15 - Collect and Communicate Audit Trail	Pre-condition	Pre-requisites for Use Cases
HITSP/T17 - Secured Communication Channel	HITSP/T15 - Collect and Communicate Audit Trail	General	Identification and management of audit trigger events and audit event outputs
HITSP/TP30 - Manage Consent Directives	HITSP/T17 - Secured Communication Channel	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/T16 - Consistent Time	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/T15 - Collect and Communicate Audit Trail	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/C19 - Entity Identity Assertion	General	Pre-requisites for Use Cases

3.2.5 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

This section describes the constraints that further limit the constructs that are used by this Interoperability Specification.

Table 3.2.5-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
No applicable additional constraints				

4.0 STANDARDS SELECTION

This section presents the standards required to support each major Use Case event. Standards selection is based on the following process:

- Evaluation: The Technical Committee evaluates the standards using the HITSP Tier 2 Readiness Criteria
- Selection: Based on the Tier 2 evaluations, named standards are selected and listed in the table of selected standards below. 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
- Gap and Overlap Analysis and Recommendations: The Technical Committee also identifies and analyzes gaps and overlaps within the standards industry as they related to the specific Use Case. The Technical Committee provides a description of the gaps, including missing or incomplete standards, a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps

It is HITSP's policy to incorporate only standards that have been approved according to the formal policy of standards organization, as defined by HITSP, which publishes the standard. HITSP interprets approval to include Draft Standards for Trial Use. The objective is to incorporate only standards that are managed within a formal life cycle process as defined by the standards organization. In some cases, where we believe a standard that is not yet approved may best meet the requirements of an Interoperability Specification, HITSP may provide a roadmap of its future intent conditional on future actions by either or both the standards organizations and the HITSP Technical Committee. Thus there are four classes of HITSP-committed standards.

- Approved for Use – standards included for unconditional use within a HITSP construct
- Interim – standards included for use now within a HITSP construct but for a defined time period or conditional on future actions, e.g., "Intended for Use" standard is available
- Provisional - standards that are not yet but are expected to be approved by the Standards Organization by the time the Interoperability Specification is released by HITSP. A "Provisional" standard becomes an "Approved for Use" standard only if:
  - It is approved by the Standards Organization by the time that the Interoperability Specification is released by HITSP and
  - It is substantially the same as it was when it was provisionally used and
  - It requires no further action by the Technical Committee
- Intended for Use – proposed standards that are road mapped for future use pending actions by the Technical Committee and/or the standards organization. Therefore a standard is defined as "Intended for Use" because it will not be approved by the time that the HITSP construct is released but is sufficiently defined to enable detailed evaluation of how well it will meet technical and interoperability requirements

HITSP may continue to use “Provisional” or “Interim” standards as they existed when incorporated into the HITSP construct if the expected conditions are not satisfied until such time as HITSP can replace it with a more suitable standard. In this circumstance, the Standards Organization would have no responsibility to maintain or correct this artifact. If a standard “Intended for Use” is not developed and approved in terms of time frame or content as expected by the Technical Committee at the time of its initial selection, it may be replaced. All standards used by HITSP must meet the HITSP selection criteria. The use of “Interim” and “Intended for Use” standards will be weighed against the alternative of simply declaring a gap for HITSP and the Standards Organizations to resolve.

4.1 TABLE OF SELECTED 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 Interoperability 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 4.1.1)
- 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 4.1.2)
- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Interoperability Specification (see Section 4.1.3)

4.1.1 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 Interoperability Specification.

Table 4.1.1-1 Regulatory Guidance

Standard	Description
Clinical Laboratory Improvement Amendments (CLIA) of 1988	Establishes quality standards for all laboratory testing to ensure the accuracy, reliability, and timeliness of patient test results regardless of where the test is performed. The Centers for Medicare and Medicaid Services (CMS) regulates all laboratory testing (except research) performed on humans in the U.S. based on CLIA For more information visit http://www.fda.gov and http://www.cms.hhs.gov

4.1.2 SELECTED STANDARDS

The following table provides a list of standards that are used to meet information exchange requirements of the Interoperability Specification, and the HITSP constructs that use each standard. A detailed description of each standard is also provided in the appendix.

Table 4.1-1 Selected Standards Linked to HITSP Constructs

Standard Name	HITSP Construct	Remarks/ Minor Gaps
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	HITSP/C26 - Nonrepudiation of Origin	
CDC Race and Ethnicity Code Sets	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	Underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	HITSP/C26 - Nonrepudiation of Origin	
Federal Medication Terminologies	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	Underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)
Health Level Seven (HL7) Clinical Document Architecture Release 2 (CDA R2)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C37 - Lab Report Document	Re: HITSP/C32 - underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)
Health Level Seven (HL7) Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD), April 01, 2007	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/TP20 – Access Control	
Health Level Seven (HL7) Version 2.5[1]	HITSP/TP22 - Patient ID Cross-Referencing	Underlying standard referenced in Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0
Health Level Seven (HL7) Version 2.5.1	HITSP/C35 - Lab Result Terminology	
Health Level Seven (HL7) Version 2.5/2.5.1	HITSP/T23 - Patient Demographics Query	
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/TP30 - Manage Consent Directives	
Healthcare Provider Taxonomy	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	Underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)

[1] HITSP references HL7 2.5.1 messaging for lab results reporting and HL7 2.5 for other messages. Future maintenance work will move toward referencing a single HL7 version across HITSP documents.

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	HITSP/T15 - Collect and Communicate Security Audit Trail HITSP/T17 - Secured Communication Channel	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Consistent Time (CT) Integration Profile	HITSP/T16 - Consistent Time	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	HITSP/C19 - Entity Identity Assertion	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	HITSP/C26 - Nonrepudiation of Origin	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Demographics Query (PDQ) Integration Profile	HITSP/T23 - Patient Demographics Query	
Integrating the Healthcare Enterprise (IHE) Laboratory Technical Framework Volume 3 (LAB TF-3) Document-based Transactions, Revision 2.0 - For Trial Implementation, August 16, 2007	HITSP/C37 - Lab Report Document	

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C35 - Lab Result Terminology	Re: HITSP/C32 - underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF), The mailto URL (Uniform Resource Locators) scheme (RFC 2368) Proposed Standard	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Internet Engineering Task Force (IETF), The tel URI (Uniform Resource Identifier) for Telephone Numbers (RFC 3966) Proposed Standard	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Logical Observation Identifiers Names and Codes (LOINC®)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C35 - Lab Result Terminology	Re: HITSP/C32 - underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)
National Library of Medicine (NLM) Unified Medical Language System (UMLS) RxNorm	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/TP20 - Access Control	

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Unified Code for Units of Measure (UCUM)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C35 - Lab Result Terminology	Re: HITSP/C32 - underlying standard referenced in Health Level Seven (HL7) Version 3.0 Continuity of Care Document (CCD)

4.1.3 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 Interoperability Specification.

Table 4.1.3-1 Informative Reference Standards

Standard Name	Description/Reason for Use
American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), #359-2004	This standard describes RBAC features that have achieved acceptance in the commercial marketplace. It includes a reference model and functional specifications for the RBAC features defined in the reference model. It is intended for (1) software engineers and product development managers who design products incorporating access control features; and (2) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional. For more information visit http://www.ansi.org
American Society for Testing and Materials (ASTM) Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management. The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards. Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org

Standard Name	Description/Reason for Use
American Society for Testing and Materials (ASTM) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1)." For more information visit www.astm.org
Council for Affordable Quality Health Care (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase I Operating Rules	Provide agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.caqh.org
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
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
Health Level Seven (HL7) Version 3.0	The HL7 Version 3.0 Messaging Standard is an application protocol for electronic data exchange in healthcare. Version 3.0 is based on a Reference Information Model (RIM); which is used to instantiate various message formats. Value sets / code tables are contained in the standard. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	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 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

Standard Name	Description/Reason for Use
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Revision 1.0	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross-Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross-Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
International Organization for Standardization (ISO) Health informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992	Establishes user requirements for the service definition needed to support the security alarm reporting function, defines the service provided by the security alarm reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics -- Information technology -- Text and office systems - Office Document Architecture (ODA) and interchange format, Technical Report on ISO 8613 implementation testing, Technical Specification # ISO/IEC CD 10183 -- Part 3: Testing procedure.	Specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system. For more information visit www.iso.org

Standard Name	Description/Reason for Use
International Organization for Standardization (ISO) Health informatics -- Privilege management and access control(PMAC), Technical Specification #22600 -- Part 1: Overview and policy management, July 2006	Supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics – Functional and Structural Roles (ISO SF Roles), Technical Specification #21298 , Draft May, 2007	This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed. Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare actors. Directory services: structural roles are usefully recorded within directories of health care providers (see for example, ISO TS 21091 Health Informatics – Directory services for security, communications, and identification of professionals and patients). Audit trails: functional roles are usefully recorded within audit trails for health information applications. Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary. For more information visit www.iso.org
National Cancer Institute (NCI) Thesaurus: Route of Administration	Route of Administration is the path by which a particular drug product is introduced on or into the body. The medication terminology is maintained by the NCI Thesaurus, a reference terminology and biomedical ontology used in a growing number of NCI and other systems. It covers vocabulary for clinical care, translational and basic research, and public information and administrative activities. The NCI Thesaurus provides definitions, synonyms, and other information on nearly 10,000 cancers and related diseases, 8,000 single agents and combination therapies, and a wide range of other topics related to cancer and biomedical research. It is part of the Federal Medication Terminologies. For more information, visit www.cancer.gov
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org

Standard Name	Description/Reason for Use
Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security SOAP Message Security Version 1.0	Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e.. support multiple security token formats. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Simple Object Access Protocol (SOAP) Version 1.1	SOAP is a protocol specification for invoking methods on servers, services, components and objects. SOAP codifies the existing practice of using XML and HTTP as a method invocation mechanism. The SOAP specification mandates a small number of HTTP headers that facilitate firewall/proxy filtering plus an XML vocabulary that is used for representing method parameters, return values, and exceptions." {DevelopMentor} SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. For more information visit www.oasis-open.org
Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity	This classification provides a minimum standard for maintaining, collecting, and presenting data on race and ethnicity for all Federal-reporting purposes. The categories in this classification are social-political constructs and should not be interpreted as being scientific or anthropological in nature. The standards have been developed to provide a common language for uniformity and comparability in the collection and use of data on race and ethnicity by Federal agencies. For more information visit www.census.gov

4.2 GAPS WHERE THERE ARE NO STANDARDS

This section describes gaps in standards. Gaps occur in the following two cases, where HITSP has:

- Identified requirements derived from the context that have no standards that meet all tiers of HITSP criteria to merit selection for that context
- Identified a single standard that encompasses and singly fulfills a set of tightly-coupled standards from the given context, yet is lacking in fulfilling one or more of the tightly-coupled requirements

The gap is only relative to the specific Consumer Empowerment and the Consumer Access to Clinical Information Use Case events. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross team validation of the gap, provisional recommendations and peer review by the team.

The table below identifies the Use Case events and known associated gaps, along with the recommended resolutions.

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Event Description	Identified Gaps	Recommended Resolution
2.1.5.0	Modify registration/medication data	The Use Case states: Consumers may have the following options for modifying, updating, and correcting various data elements: (1) some data fields will permit unrestricted modifications. (2) some data fields may not permit consumers to edit data, but could allow annotations to be made by the consumer. (3) some data fields will not permit changes and consumers would need to submit requests for modifications and corrections directly to the Providers of PHR Services and/or the Data Systems and Networks that are the original source of the data. Requirements (1) and (2) are met by preventing all fields from any information modules for the registration/medication history not authored by the document creator to be modified, but allowing any author to create new modules in the documents it makes available. Requirement (3) is a pre-condition for the Use Case, but is a gap that would eventually need to be addressed.	Consider a future extension to the Use Case to explicitly include a means for the consumer to submit an electronic request for modifications and corrections directly to the original source of data.
2.1.5.0	Modify registration/medication data	A robust terminology that allows consumers to qualify the role of their healthcare providers in their registration summary is lacking. The Use Case was addressed without such a terminology, but further extensions will likely require its definition.	A consumer oriented terminology for healthcare provider type role (e.g., primary care physician, ob/gyn, pharmacy, cardiologist). Consider use of X12 and consider leaving roles as an uncoded entry because consumer use does not fit existing coding systems.
2.1.5.0	Modify registration/medication data	There is no recognized standard or vocabulary in the industry regarding how the dose calculation is to be explicitly expressed.	The medication history needs to include an entry for dose calculation including weight dosing. We should monitor and encourage standards progress in both NCPDP and HL7 in this regard.

Considering the relationship to previous constructs, known gaps, potential activities by SDOs, and other initiatives that are either in-progress or pending results that might impact the Interoperability Specification development, the Use Case was broken down in high-level Work Items to one of two Work Sets.

- Addressed by this update to this Interoperability Specification (HITSP/IS03) and the new HITSP/IS05 Consumer Empowerment and Access to Clinical Information via Media shown in Table 3.1-1
- Gaps or results of works-in-progress initiatives to be addressed during next year's HITSP cycle are shown below

A detailed analysis of work items marked as "2008 Cycle" has not been conducted by the HITSP Technical Committees. They are included here as a reflection that the required standards to satisfy them are not available or that a more in-depth review is required to make this determination definitively.

Work Items	Work Set	Reason for Classification Result
Advance Directives (AD)	2008 cycle	May need additional vocabulary re. types of AD, location of it, currency of it, as well as nonrepudiation issue specification work. The AD is packaged with the rest of the HITSP/C32 message Encourage State Health Alliance work to address this topic Acknowledge the gap that exists in the industry to do something better in this regard, however, this is not work that is currently requested in the current Use Case. Since we're modifying HITSP/C32 we will add this to the Gap table. Awaiting HISPC to address the X-State disjointed solution in terms of policy as a prerequisite
Med / Labs Info in Consumer-friendly Manner	2008 cycle	American College of Physicians has worked with HL7 regarding its Context-aware Information retrieval activity which can likely be leveraged to query for "consumer friendly" knowledge. Standard expected to be approved by HL7 in 2008
PHR Portability – via a data network-based exchange	2008 cycle	Scope issue. It is critical that the "payload" specification be independent of the transport/packaging utilized and that consistency be ensured for information continuity with the current Interoperability Specification IS03. It is logical that current documents described in HITSP/C32, the additional lab documents (see candidate above), and other documents (HITSP defined or not), be supported Want to do a "copy" function w/o any implication of why this is being accomplished. The management of intent is a pre-condition. Be content agnostic, multi-document capable, adequate wrapper and select transport to affect interoperability [Wrapper/Transport Standard Selection options: X12 plan-to-plan PHR transfer, IHE XDR (reuse of existing of TP13 transaction), EDIFACT (e.g. for NCPDP Medication content only transfer), other transport standards
Permission Lists for PHR Portability	2008 cycle	HL7 is currently balloting a "permissions catalogue." Need definition of provider roles (static & dynamic)…some of this may be available but may vary State-to-State The Use Case includes the access to pharmacy information at PBMs by providers (7.2.1) It needs to be determined if this mandates different query/response solutions for different types of information (e.g. NCPDP-based message exchange)
Distributed Management of Access Control	2008 cycle	To be handled by HITSP Security, Privacy and Infrastructure Domain Technical Committee (SPI-DTC) in its entirety. The HIE is described as enforcing the permissions/access controls from the consumer (9.2). We might need to consider two tiers of access control: 1. High-level access control to a consumer's PHR location (a consumer may have different PHRs for different purposes and may desire that different sets of users have different access controls to one or more of them) 2. Data level access controls to the elements within a PHR Leverage and extend HITSP SPI-DTC work regarding the definition of an HIE-level access control technical actor

Work Items	Work Set	Reason for Classification Result
Provider List(s)	2008 cycle	Major gap in the specification of a provider registry (if using the HIE variant); its content, privacy issues, organization-provider relationship(s), and organization-organization relationship(s). Also, if this is related to addressing the permissions issue then are there other. organizations/individuals that we need to cover as well. This provider list is required for inclusion in /association to the permissions/access control entries 1. Need to do query/retrieve access with a provider registry (assumes that one exists and is maintained) or do pt-to-pt request (in-person, phone) to a healthcare entity. The entity pushes this info to the consumer (using HITSP/C32). 2. Consumer creates and is capable of communicating this list to others (method for building the relationship to permissions?) Consider payor-provided portals to provider lists for its members as a source of provider list content
Audit Logs / Disclosure Logs	2008 cycle	There is existing work re audit logs (EHRSFM IN 2.2, RFC 3881, IHE ATNA,), and some use of the term “disclosure logs” exists in HIPAA (Section 164.528), but nothing standards-based regarding Disclosure Logs as described in the Use Case. The definition of a standard format and the content for an interoperable disclosure log is to be addressed by the HITSP SPI-DTC If the PHR contains a pointer to information, how does this get reflected in the audit/disclosure logs?
PHR Location	2008 cycle	There is no known standard for expressing the “address” for information destined for someone’s PHR. Need to identify if there is an element in the HITSP/C32 currently for retaining this info, also how do we specify this content to be used for the different types of info exchange? [Also noted in the Access Controls entry] The HIE is described as enforcing the permissions / access controls from the consumer (9.2). We might need to consider two tiers of access control: 1. High-level access control to a consumer’s PHR location (a consumer may have different PHRs for different purposes and may desire that different sets of users have different access controls to one or more of them) 2. Data level access controls to the elements within a PHR (better managed by the PHR itself when the query is received) Is there any work regarding the definition of an HIE-level access control technical actor (e.g. from HITSP SPI-DTC)?

4.3 STANDARD OVERLAPS

This section describes the instances where there are overlaps among standards for the Use Case. The overlap is only relative to the specific Use Case event. Overlaps refer to instances wherein some of the requirements are met by multiple standards. The overlap is only relative to the specific Consumer Empowerment and the Consumer Access to Clinical Information Use Case events. Recommended resolutions were developed through a series of steps including the Technical Committee’s initial recommendations, cross Technical Committee validation of the overlap, provisional recommendations and peer review by the Technical Committees.

The table below presents the identified overlaps and the respective resolution plans.

Table 4.3-1 Standard Overlaps

Event Code	Event Description	Standard Duplication/ Overlap	Recommended Resolution
	View registration/medication data	Standard terminology used to describe providers used in the U.S. are almost all driven by, based on, or have been source material for the HIPAA Healthcare Provider Taxonomy, which leads to a large number of overlaps. Since the HIPAA provider taxonomy is the logical successor to many of these standards, this overlap is not hard to understand. However, harmonization of the HIPAA provider taxonomy with other working going on in ISO, should be undertaken. The HIPAA provider taxonomy is used to describe providers by their specialty, and is often related to licensure, accreditation, and/or certification, a "structural role," based on who they are and what they know. However, what is needed from a Consumer Empowerment perspective is a way to describe providers by their function role according to the consumer, not provider viewpoint. Consumers think in terms of Cardiologist, Gynecologist, et cetera. Often the consumer "functional role" and the provider "structural role" will match, but this is not always the case.	The HITSP Consumer Perspective Technical Committee recommends that a standardized terminology be developed that might be used in future releases of this Component. The HL7 Security Technical Committee is presently working with the VHA Role Based Access Control Task Force (RBAC-TF) to develop materials describing the roles of providers, for the purposes of supporting access controls. The present work nearly met the needs of the HITSP Consumer Perspective Technical Committee lacking only coded terms to describe the roles
	View registration/medication data	For the Registration Summary and Medication History Document, two base standards may be used: HL7 CDA Rel 2 and ASTM CCR. For PHR information exchange “on the wire”, this specification selected the use of the CCD implementation guide resulting from the harmonization work performed by ASTM and HL7.	See Section 4.3.1

4.3.1 STANDARDS OVERLAP RECOMMENDED RESOLUTION

The Consumer Perspective Technical Committee has been charged with introducing the consumer, and the PHR, as an integral partner of the healthcare information flow representing a new paradigm in healthcare interoperability. This paradigm establishes the consumer as the active participant in health information exchange that touches all segments of the industry; providers/care facilities, health plans, pharmacies/prescription benefit managers, and others. This challenge is exacerbated by the current information technology situation wherein providers, health plans, and pharmacies, and pharmacy benefit managers (PBMs) industry segments each have created different standards based on differing business needs and timing, with shared and overlapping data elements via three different standards developers: HL7, ASC X12, and NCPDP.

In addition to these aforementioned standards, a fourth standard initiative from ASTM targeting the provider-provider and provider-consumer interoperability space, entitled the Continuity of Care (CCR), passed favorable ballot in October 2005. In the latter phase of the successful CCR balloting process, ASTM and HL7 initiated a formal harmonization effort regarding their respective efforts addressing the same interoperability space. This harmonization initiative resulted in the joint development of the Continuity of Care Document (CCD) which was approved by HL7 ballot in January 2007.

The Consumer Perspective Technical Committee has determined that it is in the best interest of HITSP harmonization efforts to wholeheartedly support this HL7-ASTM harmonization initiative and leverage its deliverables to the highest degree possible. To this end, the approach taken by HITSP is to align its Interoperability Specification to the harmonized HL7-ASTM CCD and require its sole use for provider-consumer information exchange. This Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification is therefore intended to facilitate the transition from the current disparate standards environment to a harmonized state.

As noted in the initial paragraph, the Consumer Perspective Technical Committee also recognizes the need to ensure consistency of its specified data elements across all the standards deployed by the business actors of the Use Cases which are potential sources of data in the PHR. For example, ASC X12 is used to describe health plan information that is relevant for updating a consumer's PHR. To this end, the Summary Documents Using HL7 Continuity of Care Document (CCD) Component includes appendices for informative data element cross-mapping tables between the CCD elements and the ASTM CCR, ASC X12, and NCPDP SCRIPT data elements for all common content areas. These element mapping tables will serve as guidance to the standards organizations and/or application system vendors using these base standards as to how to adapt these standards and their implementations to the HITSP Interoperability Specification. Table 4.3.1-1 shows the resolution plan.

Table 4.3.1-1 Resolution Plan

Date	Task to be Accomplished/Who is involved
January 2007	HL7 and ASTM have released and achieved a successful ballot of the HL7 CCD standard and implementation guide

5.0 TECHNICAL IMPLEMENTATION

5.1 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.

5.1.1 CONFORMANCE CRITERIA

In order to claim conformance to the specification, an implementation must satisfy all the requirements and mandatory statements listed in the HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must be constrained as specified in Table 3.1.2-1, and implement all of the required actors from Table 3.2.3-1, within the scope, subset or implementation option that is selected from Section 5.1.2 below.

Claims of conformance to this specification must be made using the following language:
This product conforms to HITSP's Consumer Empowerment and Access to Clinical Information via Networks Interoperability Specification, available at www.hitsp.org.

5.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification can be implemented for individual business actors defined in the Interoperability Specification. An implementation claiming conformance to a specific business actor from the Interoperability Specification shall support all of the requirements associated to that business actor as described in table 3.2.3-1.

This means that **for each implemented business actor**:

1. All Required or Conditionally Required technical actors listed for the business actor shall be supported as specified in the associated construct
2. Optional technical actors listed for the business actor may be supported as specified in the associated construct
3. All Required or Conditionally Required transactions and content subsets listed for each implemented technical actor assigned to the business actor shall be supported as specified in the associated construct
4. Optional transactions and content subsets listed for each implemented technical actor assigned to the business actor may be supported as specified in the associated construct

Implementers of this Interoperability Specification who follow the principles listed above are being provided a level of implementation flexibility, while maintaining interoperability.

5.1.3 TEST METHODS

HITSP relies on the conformance test methods, test tools and other test-related material produced by, or under the auspices, of standards developers, profiling organizations and implementation guide producers as part of its collaborative implementation testing effort. Efforts to produce conformance test methods, tools, etc. may be internal to the organization or provided by an external organization.

An HIT Implementation Testing Web Site has been developed in collaboration with HITSP, NIST, CCHIT, and ONC to advance conformance and interoperability testing capabilities. This Web Site provides HIT implementers with the necessary resources to support and test their implementation of standards-based health systems. A link to the Web Site can be found on www.hitsp.org.

6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF STANDARDS

The following table contains descriptions of the standards that are referenced by this Interoperability Specification:

Table 6.1-1 Description of Standards

Standard	Description
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Defines a document structure for use by electronic signature mechanisms, describes the characteristics of an electronic signature process. Defines minimum requirements for different electronic signature mechanisms, defines signature attributes for use with electronic signature mechanisms, describes acceptable electronic signature mechanisms and technologies, defines minimum requirements for user identification, access control, and other security requirements for electronic signatures, and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism. For more information visit www.astm.org
CDC Race and Ethnicity Code Sets	The U.S. Centers for Disease Control and Prevention (CDC) has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards. For more information visit www.cdc.gov
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	Extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European Directive. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with this document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. For more information, visit www.etsi.org
Federal Medication Terminologies	A set of controlled terminologies and code sets developed and maintained as part of a collaboration between the Food and Drug Administration, National Library of Medicine, Veterans Health Administration, National Cancer Institute and Agency for Healthcare Research and Quality related to medications, including medication proprietary and nonproprietary names, clinical drug code (RxNorm); ingredient names and Unique Ingredient Identifiers (UNII); routes of administration, dosage forms, and units of presentation from the NCI Thesaurus (NCIt); and certain pharmacological drug classes from the National Drug File Reference Terminology (NDF-RT) . The Federal Medication Terminology leverages medication models maintained by the Food and Drug Administration (ex. UNII, NDC Codes), National Library of Medicine (RxNorm), the Veterans Health Administration (NDF-RT), and the National Cancer Institute (NCIt). Information on the Federal Medication Terminologies may be found and downloaded from the NCI Web portal terminology resources page at www.cancer.gov/cancertopics

Standard	Description
Health Care Provider Taxonomy	The Health Care Provider Taxonomy code set is a collection of unique alphanumeric codes, ten characters in length. The Health Care Provider Taxonomy code set includes specialty categories for individuals, groups of individuals, and non-individuals. The National Uniform Claims Committee maintains this code set. The complete code set is available from the Washington Publishing Company at www.wpc-edi.com
Health Level Seven (HL7) Clinical Document Architecture Release 2 (CDA R2)	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit www.hl7.org
Health Level Seven (HL7) Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD), April 01, 2007	The Continuity of Care Document implementation guide describes constraints on the HL7 Clinical Document Architecture, Release 2 (CDA) specification in accordance with requirements set forward in ASTM E2369-05 Standard Specification for Continuity of Care Record (CCR). The resulting specification, known as the Continuity of Care Document (CCD), is developed as a collaborative effort between ASTM and HL7. It is intended as an alternate implementation to the one specified in ASTM ADJE2369 for those institutions or organizations committed to implementation of the HL7 Clinical Document Architecture
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
Health Level Seven (HL7) Version 2.5[2]	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5.1	The HL7 Version 2.5.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 4, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. They are also used in HL7 order messages. For more information visit www.hl7.org

[2] HITSP references HL7 V2.5.1 messaging for lab results reporting and HL7 V2.5 for other messages. Future maintenance work will move toward referencing a single HL7 version across HITSP documents.

Standard	Description
Health Level Seven (HL7) Version 2.5/2.5.1	The HL7 Version 2.5 and 2.5.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 4, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. They are also used in HL7 order messages. For more information visit www.hl7.org
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) 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
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

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	The Patient Identifier Cross-referencing Integration Profile (PIX) is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1)The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification. By specifying the above transactions among specific actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise.. 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) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. 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) Revision 4.0, Consistent Time (CT) Integration Profile	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. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE CT Integration Profile, and other 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) 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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the user 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 user in a way that the receiver can make access decisions and 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 entities, and others that may have chosen to use a third party to perform the authentication. The latest version of the IHE framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. The latest version of the IHE Technical Framework is available at www.ihe.net

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Demographics Query (PDQ) Integration Profile	Provides ways for multiple distributed applications to query a central patient information server for a list of patients, based on user-defined search criteria, and retrieve a patient's demographic (and, optionally, visit or visit-related) information directly into the application. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) Laboratory Technical Framework Volume 3 (LAB TF-3) Document-based Transactions, Revision 2.0 - For Trial Implementation, August 16, 2007	The IHE Laboratory Technical Framework introduces a content Integration Profile Sharing Laboratory Reports (LAB TF-3) that describes a clinical laboratory report as a human-readable electronic document. This document, which may also contain data in a machine-readable format and contains the complete set of final results produced by a clinical laboratory in fulfillment of one or more test orders for a patient. This document is focused on the sharing of sets of laboratory results in the form of a laboratory report structured document, and is not intended to address ordering or return of laboratory results to the ordering provider. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross-Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
International Health Terminology Standards Development Organisation (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
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. For more information visit www.ietf.org
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), The mailto URL (Uniform Resource Locators) scheme (RFC 2368) Proposed Standard	This document defines the format of Uniform Resource Locators (URL) for designating electronic mail addresses. It is one of a suite of documents which replace RFC 1738, 'Uniform Resource Locators', and RFC 1808, 'Relative Uniform Resource Locators'. The syntax of 'mailto' URLs from RFC 1738 is extended to allow creation of more RFC 822 messages by allowing the URL to express additional header and body fields. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), The tel URI (Uniform Resource Identifier) for Telephone Numbers (RFC 3966) Proposed Standard	This document specifies the URI (Uniform Resource Identifier) scheme "tel". The "tel" URI describes resources identified by telephone numbers. This document obsoletes RFC 2806. For more information visit www.ietf.org

Standard	Description
Logical Observation Identifiers Names and Codes (LOINC®)	A database of universal identifiers for laboratory and other clinical observations. The laboratory portion of the LOINC database contains the usual categories of chemistry, hematology, serology, microbiology (including parasitology and virology), and toxicology; as well as categories for drugs and the cell counts typically reported on a complete blood count or a cerebrospinal fluid cell count. Antibiotic susceptibilities are a separate category. The clinical portion of the LOINC database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments, and other clinical observations. For more information visit www.loinc.org
National Library of Medicine (NLM) Unified Medical Language System (UMLS) RxNorm	Provides standard names for (1) clinical drugs and (2) drug dose forms as administered to a patient. Also provides links from clinical drugs, both branded and generic, to their active ingredients, drug components (active ingredient + strength), and related brand names. Food and Drug Administration (FDA) National Drug Codes (NDCs) for specific drug products and many of the drug vocabularies commonly used in pharmacy management and drug interaction software are additionally linked to RxNorm. RxNorm is a part of the Federal Medication Terminologies. For more information visit www.nlm.nih.gov
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	SA SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Toke Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XCML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit www.oasis-open.org
Unified Code for Units of Measure (UCUM)	A code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. For more information visit aurora.regenstrief.org

7.0 CHANGE HISTORY

The following sections provide the history of changes made to this document.

7.1 MAY 11, 2007

This document is now Released for Implementation.

7.2 SEPTEMBER 18, 2007

1. Updated Foreword to account for the CACI Use Case description
2. Updated Interoperability Roadmap
3. Rename IS to Consumer Sharing of Health Information via Networks
4. Updated HITSP/C32 - Registration and Medication History Document Content Component to include: list of allergies for the consumer, encounters, identified conditions and problems diagnosed, the current list of immunizations received by the consumer, as well as some key laboratory test results indicative of the patient health status
5. Updated HITSP/TP13 with provisional selection of XDS.b to support Entity Identity Assertion (SAML) support
6. Added HITSP/C37 and HITSP/C35 constructs for laboratory reports
7. Added reference to Security and Privacy constructs: HITSP T15, T16, T17, TP20, TP30, C19, C26
8. Add in Section 4.0 reference to SNOMED, CLIA, LOINC, UCUM
9. Add in 3.1 the CACI resolution plan with 2008 work items
10. Add to overview of the CACI Use Case description
11. Rescope Scenario 3.2.2.1
12. Remove security pre-conditions now explicitly addressed
13. Extend technical actors with Content Creator (to leave Doc Source and Media Creator for infrastructure interchange) and Content Consumer
14. Add Security and Privacy technical actors
15. Add Results – Laboratory, Immunizations, Encounters, Vital Signs in HITSP/C32 summary
16. Add Lab Report Doc description
17. Rescope Scenario 3.2.2.2
18. Rescope Scenario 3.2.2.3
19. Extend list of Transaction, Transaction Package and Components
20. Update list of dependencies
21. Remove Overview figure
22. Add for each business actor the extended list of technical actors
23. Extend the mapping from technical actor to Transaction Requirements
24. Add CACI to supporting documents
25. Add Subsetting to the conformance section

7.3 DECEMBER 5, 2007

The changes in this cycle address the following comments:

2424, 2444, 2445, 2446, 2456, 246, 2424, 2444, 2445, 2446, 2456, 2461

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

1. The Consumer Empowerment IS deliverables represent the joint analysis of both of the Consumer Empowerment (CE) Use Cases (Consumer Empowerment and Clinical Access to Clinical Information). The IS's are differentiated solely by the transport by which the consumer has access to and shares clinical information – via Networks (IS03) and using Media (IS05). As such, Section 2 for each of these IS's is identical. Section 2 Tables and their associated UML's have been completely redone to reflect a concatenation, where appropriate, of the events/actions from both of both CE Use Cases. This integration of the events/actions resulted in scenario one being fully merged into a single scenario entitled "Consumer creates account to host and Access Registration Summary and Clinical Information." Scenario 2 and 3 of the Consumer Empowerment Use Case were likewise edited to include operationally equivalent events/actions from the Consumer Access Use Case. Scenario 2 and 3 of the Consumer Access Use Case remained intact as originally presented.
2. Section 3 has been revised to reflect the new template (effective 11/29/07) which was the result of a cross-TC and project management assessment of the IS readability and usability for implementation and certification purposes. The following changes were made to the document in this regard:
   - Table 3.2.1-1 was revised to only list the technical actor names and their descriptions
   - The UML's in section 3.2.2 were completely redesigned to improve the segmentation of business actor-to- business actor interactions and technical actor-to technical actor transactions
   - Table 3.2.3-1 was completely redesigned to improve the clarity of the requirements (and optionality) for a business actor in terms of what technical actors need to be supported AND what specific transactions for those technical actors are required, optional, or conditional
   - The conformance subsets previously included in Section 5.1.2 were relocated to Section 3.2.3 as paragraphs 3.2.3.x, where x = the subset number. These subsets were also included in table 3.2.3-1 accordingly
   - The Conformance Section 5.1 was revised to direct the reader to section 3.2.3 for the mandatory requirements to claim conformance to this specification
3. Transactions and Content were differentiated in table 3.2.3-1 to clarify how specific technical actors (e.g. Document Source) needed to support both Content Technical Actors (Content Creator and Content Consumer), specified with the detailed subsets of clinical information, and the transaction to transport that information (e.g. TP13).
4. All relevant Security and Privacy constructs, including their applicable transactions, have been included in Section 3, with particular specificity regarding their association to business actors requirements highlighted via table 3.2.3-1.

5. The results of TC dispositions of public comments received against this IS have been appropriately reflected in the text, tables, and UML diagrams of the IS. Specifically, comment dispositions for the following comment topic categories have been effectively included:
   - PHR Data Entry/Quality/Integrity – comments #2424, 2425, 2426, 2427, 2428, 2443, 2450
   - Data Content Specifics – comments #2444, 2446, 2454, 2455, 2456, 2489
   - Data Transport Logistics & Controls – comments #2445, 2453, 2461
   - CFH Initiative General Comments – comment #2495

7.4 DECEMBER 13, 2007

Upon approval by the HITSP Panel on December 13, 2007, this document is now Released for Implementation.

7.5 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. Please refer to the underlying constructs for specific changes to standards.

7.6 AUGUST 27, 2008

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