

HITSP Clinical Research Requirements, Design and Standards Selection

HITSP/RDSS144



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Clinical Research Tiger Team



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Clinical Research Tiger Team	July 30, 2009



TABLE OF CONTENTS

1.0	INTRODUCTION	5
1.1	Interoperability Specification Overview	5
1.2	Copyright Permissions.....	5
1.3	Reference Documents.....	6
2.0	REQUIREMENTS	7
2.1	Synopsis of requirements	7
2.2	Protocol-driven sponsored research scenario.....	7
2.2.1	Protocol-Driven Sponsored Research Information Exchange requirements	8
2.3	Registry Reporting scenario	9
2.3.1	Registry Reporting Information Exchange Requirements	10
2.4	Research Network scenario	11
2.4.1	Research network Information Exchange Requirements.....	11
2.5	System Description.....	12
2.6	Exchange Content Descriptions	13
2.7	Data requirements	14
2.8	Information Exchange Requirements (IER) Descriptions.....	16
2.9	HITSP Capabilities Used	17
3.0	DESIGN.....	21
3.1	Capability Orchestration	21
3.1.1	Additional Constraints on Required Capabilities	22
3.1.2	Existing HITSP Constructs	23
3.1.3	New HITSP Constructs.....	28
4.0	STANDARDS SELECTION	29
4.1	Standards	29
4.1.1	Regulatory Guidance.....	29
4.1.2	Selected Standards	29
4.1.3	Informative Reference Standards.....	35
4.2	Gaps Where There Are No Standards	44
4.3	Standard Overlaps.....	45
5.0	APPENDIX	46
5.1	Use Case to Information Exchange and Data Requirements	46



FIGURES AND TABLES

Table 1-1 Reference Documents	6
Table 2-1 Description of Scenarios	7
Table 2-2 Protocol-driven Sponsored Research Information Exchange Requirements (IER)	8
Table 2-3 Registry Reporting Information Exchange Requirements	10
Table 2-4 Research Network Information Exchange Requirements (IER)	11
Table 2-5 System Names and Descriptions.....	12
Table 2-6 Exchange Content Descriptions	13
Table 2-7 Data Requirements	14
Table 2-8 Description of Information Exchange Requirements	17
Table 2-9 HITSP Capabilities.....	17
Table 2-10 Summary of Relationships between Capabilities and Information Exchange Requirements.....	19
Table 3-1 Capability Orchestration	21
Table 3-2 Conditions	22
Table 3-3 Additional Constraints on Capabilities	22
Table 3-4 Constructs and Required Modifications	23
Table 3-5 New Constructs.....	28
Table 4-1 Regulatory Guidance	29
Table 4-2 Selected Standards Linked to HITSP Constructs.....	29
Table 4-3 Informative Reference Standards	35
Table 4-4 Use Case Requirements and Associated Standards Gaps.....	45
Table 4-5 Use Case Requirements and Associated Standard Overlaps.....	45
Table 5-1 Mapping of Use Case Actions to Information Exchange Requirements.....	46
Figure 2-1 Protocol Driven Component Diagram.....	9
Figure 2-2 Registry Reporting Component Diagram	10
Figure 2-3 Research Network Component Diagram.....	12



1.0 INTRODUCTION

1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

The Use of Electronic Health Records in Clinical Research: Core Research Data Element Exchange Use Case focuses on ways in which electronic health record (EHR) data can support global clinical research activities. Specifically, the Use Case focuses on exchange of a core set of patient-level clinical information exchanges between EHRs and clinical research (CR) systems. The key interfaces in this Use Case are the research sponsors, investigative sites, and regulatory agencies. The goal of the Interoperability Specification is to identify appropriate standards for the exchange of information inclusive of all types of clinical research. The scope of this effort is on:

- The ability to communicate study parameters, eligibility information, results, and case report forms within the research community
- The ability to exchange a core dataset of de-identified or anonymized information from the EHR to a research system for use in clinical research

The Clinical Research Interoperability Specification follows the Use Case closely, and is informed by the prior work of HL7, CDISC, and IHE; testing and demonstrations of EHR and clinical research cooperation at four IHE Connectathons and three HIMSS Interoperability Showcase demonstrations, two real world implementations, and the functional profile developed by the EHR-CR collaborative of PhRMA and eClinical Forum. It also draws on existing HITSP constructs and addresses gaps with emerging standards and integration profiles. The Interoperability Specification draws upon the IHE profile Clinical Research Document (CRD) that relies in turn on the CDISC CDASH specification of data elements known to be of interest to clinical research studies. The CRD specification enables any EHR to export a well specified set of data elements, initially exchanged with the Continuity of Care Document that can be transformed for use in clinical research studies. In operation, this will be accomplished in a workflow in which any of these data elements will automatically populate a case report form that will then surface within the EHR for review and completion. No matter how complete the CRD might become research studies will typically require data elements in addition to those pulled from the EHR data base. It is this aspect of clinical research that suggests using a forms-based approach based on HITSP/T50 Retrieve Form for Data Capture rather than using a direct data extract. Only the forms approach can accommodate all the data elements required by a Case Report Form (CRF), including those not provided by Clinical Research Document (CRD). It is this aspect of clinical research that fundamentally differentiates it from the closely aligned Quality and Public Health Use Cases.

However, the forms approach brings with it serious challenges of privacy and confidentiality. In the case of Protocol-driven Sponsored Research Scenario, designated as Scenario 1, (see Section 2.2) it is not sufficient for EHRs to export a CRD to the research system without regard for the limitations of the sponsor's protocol. The workflow is complicated by the requirement that only those data required by the protocol be delivered to the sponsor's system, and the Interoperability Specification takes this requirement into account as one of the policy variants required.

The Registry Scenario, designated as Scenario 2, (see Section 2.3) has less restrictive requirements for privacy and confidentiality since the patient identity can usually be known to the registry database. This range of policy requirements around privacy and confidentiality will be met by articulating a taxonomy of policy configurations addressed by the HITSP Security and Privacy constructs.

1.2 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2009 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.



1.3 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material.

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

Table 1-1 Reference Documents

Reference Document	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents



2.0 REQUIREMENTS

2.1 SYNOPSIS OF REQUIREMENTS

The Clinical Research Value Case comprises three scenarios for the exchange of EHR data in support of research. In all three scenarios listed below, best practices and regulatory requirements of patient privacy and data security apply, but the scenarios have different privacy requirements. For example, Scenario 1 requires that all patient data are pseudonymized whereas Scenario 2 allows fully identified data.

Table 2-1 Description of Scenarios

Scenario Name	Scenario Description
Protocol-driven Sponsored Research	This scenario describes six processes that result in the submission of clinical data to a sponsoring agency as dictated by a sponsor's protocol. It contains most of the data elements of interest. (Scenario 1)
Registry Reporting	This scenario varies only slightly from the Sponsored Research Scenario, and describes the exchange of clinical data with a research registry or other related databases. (Scenario 2)
Research Network	This third scenario, in which data originate in a networked environment, merely changes the mode of origination. (Scenario 3)

2.2 PROTOCOL-DRIVEN SPONSORED RESEARCH SCENARIO

This scenario describes six processes that result in submission of data from an EHR to a clinical research sponsor for ultimate submission to regulatory, public health and other agencies. The data requirements are specified in the sponsor's research protocol. Note that since each protocol has unique data requirements, exact and complete specification of data cannot be accomplished. The best that can be done is to specify best practice data elements that are likely to be required by all protocols, and to provide for collection of ad hoc data that cannot be specified in advance. The processes are described below.

Enrollment: Notification of the Clinical Research Organization (CRO) or Sponsor should occur when a subject is enrolled in the study (i.e. deemed eligible per the research protocol). The subject should receive a study number linking the subject to the source health record, but providing a de-identification mechanism such that the CRO or Sponsor does not receive any information that could identify the subject (e.g., subject's name, social security number, address or any other identification information).

Data Collection: A case report form for a clinical protocol is pre-populated with data identified within the EHR. Core research data elements can be identified using triggers, case report form designs or trial designs from protocols. Following confirmation by the investigator or study coordinator that these data are correct and accurate, they can be exported from the EHR into the Clinical Data Management System (CDMS) which is housed by a research system vendor, CRO, or study sponsor via an Electronic Data Capture (EDC) system or other clinical research system. The transfer could occur at regular intervals or be performed in real-time in regions with advanced health information exchanges. The eSource data, including audit trails, are maintained in the EHR at the investigative site or in an appropriate archive format at the site or at a third party under contract to the site. Core dataset information present in the EHR would be available to the CDMS. Additional data specific to the clinical study may be collected and sent to the CDMS in addition to populating the EHR as appropriate (to retain the eSource record). It would also be possible to use existing EHR systems to capture study-specific data in a systematic fashion. Thus the information flow must be bidirectional for various purposes in the research process, such as Source Data Verification. This would streamline the workflow for the investigative site. Ideally, the associated terminology would be harmonized between the EHR and research systems.

Source Data Verification: Data source verification may take place initially at the site during the study and at the completion of the clinical trial. Queries about anomalous data can be sent by the Sponsor or CRO via the EDC system to the EHR system for verification.

Institutional Review Board (IRB) and Data Safety Management Boards (DSMB): Information may need to be exchanged between the clinical study and Data Safety Management Boards, Institutional



Review Boards, ethics committees, regulators or government funding agencies to ensure the safety of subjects in the study, as specified in the research protocol. Real-time access to the data also allows monitoring of event rate, compliance and adherence to study protocols, which may trigger the DSMB to conduct a safety review of the study before the protocol-specified DSMB assessment.

Data Re-use: Data collected in standard format from the EHR allows the information to be warehoused for future analyses. Rigorous data definitions facilitate pooling data from multiple studies. When a clinical research study is being planned, information is sent to a trial registry (see Scenario 2). At the conclusion of the trial, results should be published in a trial registry (e.g. clinicaltrials.gov) or peer-review journal.

Submission of Data to Regulatory Agency: Submission of data to a regulatory agency is primarily done with data from a combined set of clinical trials for a given therapy. A data warehouse is also useful for this purpose. For each study, statisticians within the Sponsor or CRO use trial data from the CDMS to produce reports, tables, figures and listings. In addition, an integrated safety database and an integrated efficacy database are created for the submission. All of these data would already be in the standardized format in which they were captured from the EHR; additional standards are used to transport and display the integrated data and statistical analyses for the regulatory reviewers.

2.2.1 PROTOCOL-DRIVEN SPONSORED RESEARCH INFORMATION EXCHANGE REQUIREMENTS

The following Information Exchange Requirements Table summarizes the relationship between the Exchange Action, Exchange Content, and the Initiating and Responding Systems.

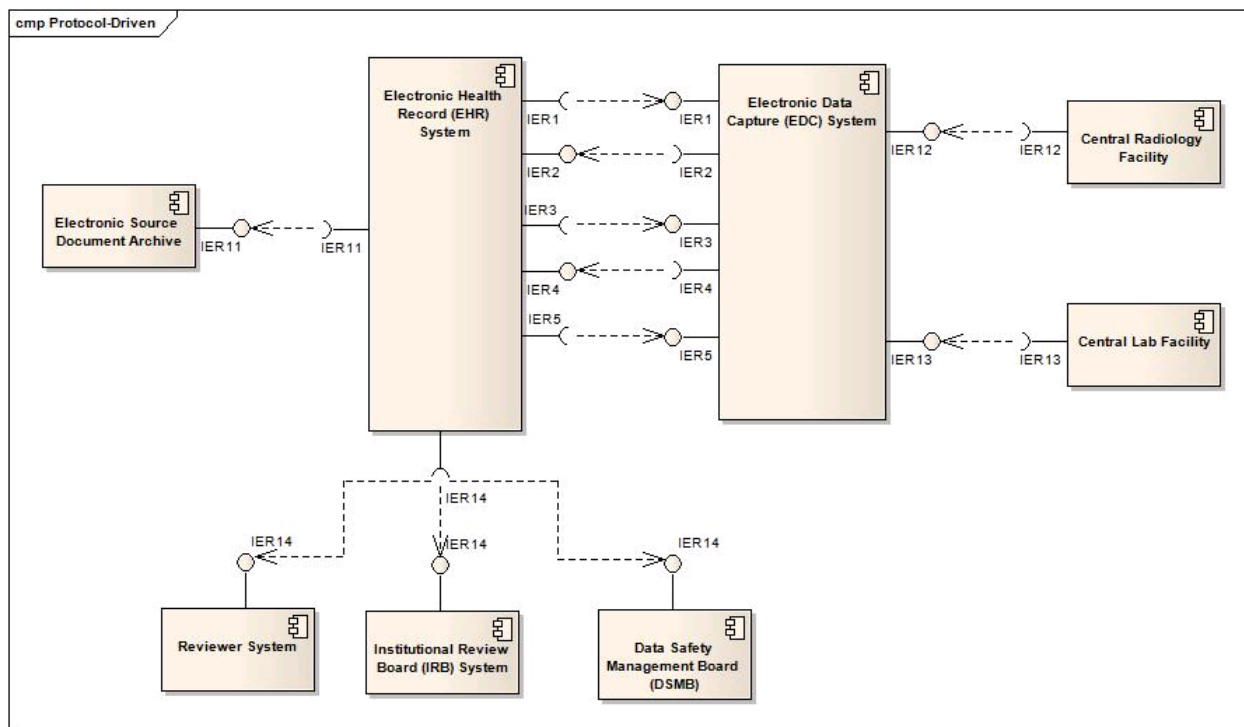
Table 2-2 Protocol-driven Sponsored Research Information Exchange Requirements (IER)

IER Number	Exchange Action	Exchange Content	Initiating System	Responding System(s)	Exchange Attribute
IER1	Send/receive	Redacted DR1, DR2, DR3, DR14	EHR	EDC	Site identifier, subject identifier, visit identifier, study identifier
IER2	Send/receive	DR2	EDC	EHR	Pseudonymous subject identifier
IER3	Send	DR2 + CRD	EHR	EDC	Site identifier, subject identifier, visit identifier, study identifier, redacted clinical research document
IER4	Response	Pre-populated CRF	EDC	EHR	CRF pre-populated with appropriate CRD data
IER5	Send/receive	Completed CRF	EHR	EDC	Includes data not provided by EHR but filled in by site personnel
IER11	Send/receive	Completed data form	EHR	Electronic Archive	Location determined by study site
IER12	Send/receive	HITSP/C37	Central Lab Facility	EDC	
IER13	Send/receive	HITSP/TP89	Central Radiology Facility	EDC	
IER14	Send/receive	EC4	EHR	EDC, IRB, DSMB, Reviewer	



Figure 2-1 is a Component Data Flow diagram that illustrates the information exchanges between the primary systems in a the Protocol-driven scenario. The information exchange numbers from Table 2-1 are annotated on the diagram to show how the requirements relate to the systems. Refer to the table for the exchange content associated with each IER.

Figure 2-1 Protocol Driven Component Diagram



2.3 REGISTRY REPORTING SCENARIO

The Registry Reporting Scenario differs from the Protocol-driven Sponsored Research Scenario in the regulatory environment and the requirements of confidentiality. Since registries are not part of the drug approval process, Food and Drug Administration (FDA) does not exercise regulatory oversight, and the requirement for source record archiving does not apply. In most cases, patient participation in a registry is entirely identified, eliminating the need for pseudonyms.

Database: The database or registry may be maintained at a single institution and enable aggregation and analysis of data collected by multiple EHR systems present within the institution. The database or registry may also be maintained by a third party, such as a patient advocacy organization, disease registry, or government agency (e.g. clinicaltrials.gov). Patients, with their physicians, submit core dataset information from the EHR directly into databases or disease registries for multiple purposes, including public health. This data transaction may include condition-specific data in addition to the core dataset information. Ideally, the submission would allow the database or registry data to be updated when changes are made in the EHR relevant to the core dataset.

Communication: The results of the clinical trial can be conveyed back to the individual and/or their care providers once the analysis is complete. In blinded studies, the longitudinal health record should be updated to indicate to which, if any, agent or intervention the individual was exposed and any long term follow up which may be required.



2.3.1 REGISTRY REPORTING INFORMATION EXCHANGE REQUIREMENTS

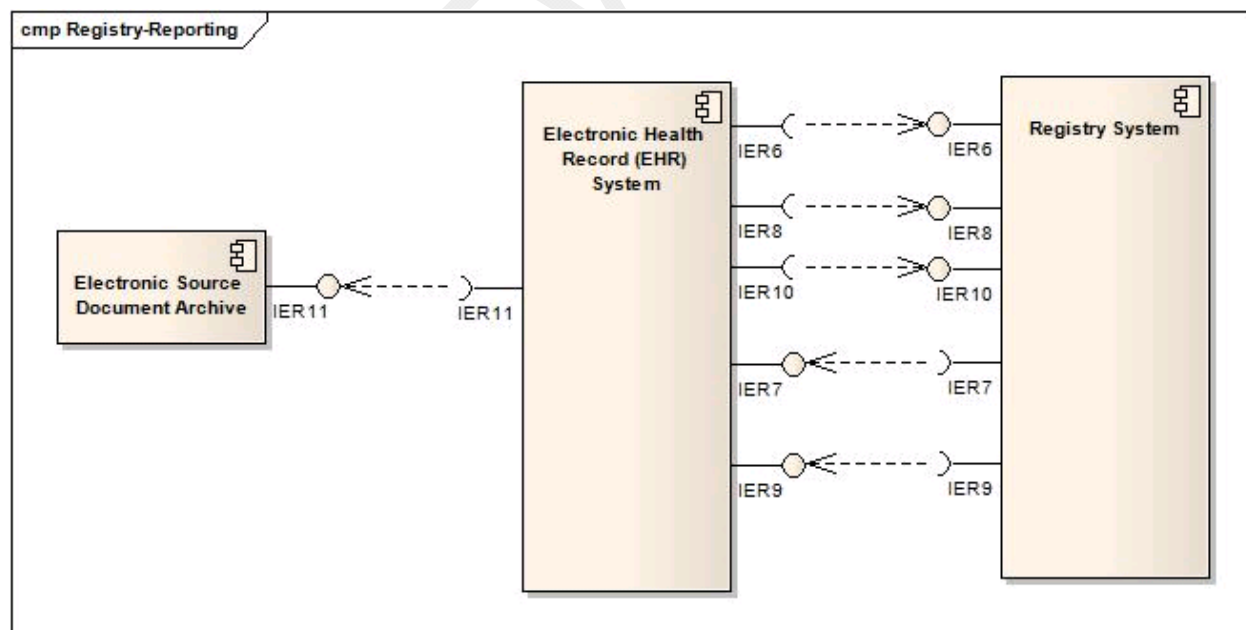
The following Information Exchange Requirements Table summarizes the relationship between the Exchange Action, Exchange Content, and the Initiating and Responding Systems.

Table 2-3 Registry Reporting Information Exchange Requirements

Information Exchange Requirement Number	Exchange Action	Exchange Content	Initiating System	Responding System(s)	Exchange Attribute
IER6	Send/receive	EC3	EHR	Registry System	Patient identifiers
IER7	Send/receive	DR2	Registry System	EHR	Subject identifier
IER8	Send	DR2 + HITSP/C32	EHR	Registry System	Patient id + HITSP/C32 complete
IER9	Response	Pre-populated registry form	Registry System	EHR	Pre-populated CRF with appropriate CCD data per CDASH and registry requirements
IER10	Send/receive	Completed Data Form	EHR	Registry System	Includes data not provided by EHR but filled in by site personnel
IER11	Send/receive	Completed Data Form	EHR	Electronic Archive	Location determined by study site

Figure 2-2 is a Component Data Flow diagram that illustrates the information exchanges between the primary systems in a the Protocol-driven scenario. The information exchange numbers from Table 2-3 are annotated on the diagram to show how the requirements relate to the systems. Refer to the table for the exchange content associated with the IER.

Figure 2-2 Registry Reporting Component Diagram



2.4 RESEARCH NETWORK SCENARIO

The Research Network Scenario positions a data aggregator, the research network system, between the participating healthcare sites and the research system, the EDC. This aggregator operates as a mega-site, and the relationship between the research network and the sponsor's system, the EDC, resembles the relationship of one site's EHR to the EDC.

Network: Data from a particular study can be aggregated from a single practice with multiple providers or from multiple sites within a network. Core data from the EHR is submitted regularly into the database and pseudonymized for aggregation with other data submissions. This allows for nearly real-time tracking of data across the network.

Data Queries. Data are maintained within a security firewall of an organization. Queries can be made of the data from outside the firewall under controlled access. Users of different types can be granted different levels of access to the data.

2.4.1 RESEARCH NETWORK INFORMATION EXCHANGE REQUIREMENTS

The following Information Exchange Requirements Table summarizes the relationship between the Exchange Action, Exchange Content, and the Initiating and Responding Systems.

Table 2-4 Research Network Information Exchange Requirements (IER)

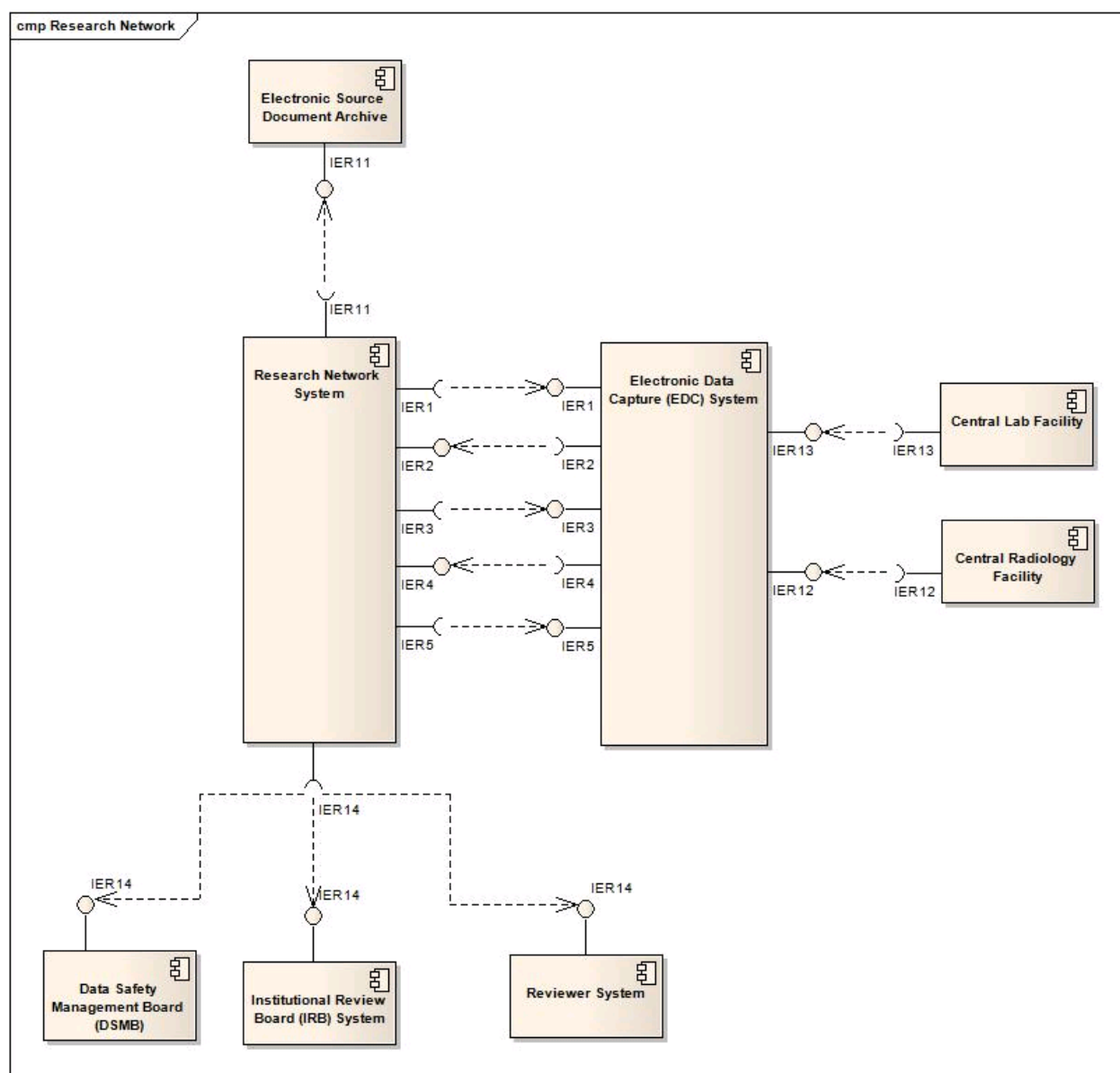
Information Exchange Requirement Number	Exchange Action	Exchange Content	Initiating System	Responding System(s)	Exchange Attribute
IER1	Request	EC3	Research network system	EDC	Some data elements may be redacted based on policy configuration
IER2	Respond	EC3	EDC	Research network system	Pseudonymous subject identifier
IER3	Send/receive	EC1	Research network system	EDC	Site identifier, subject identifier, visit identifier, study identifier, redacted clinical care document
IER4	Send/receive	EC1	EDC	Research network system	Pre-populated CRF with appropriate CCD data per CDASH
IER5	Send/receive	EC2	Research network system	EDC	Includes data not provided by EHR but filled in by site personnel. eSource document
IER11	Send/receive	EC1	Research network system	Electronic Archive	Location determined by study site or research network
IER12	Send/receive	EC5	Central Lab Facility	EDC	
IER13	Send/receive	EC6	Central Radiology Facility	EDC	
IER14	Send/receive	EC4	Research network system	EDC, IRB, DSMB, Reviewer	

Figure 2-3 is a Component Data Flow diagram that illustrates the information exchanges between the primary systems in a the Protocol-driven scenario. The information exchange numbers from Table 2-4 are



annotated on the diagram to show how the requirements relate to the systems. Refer to the table for the exchange content associated with the IER.

Figure 2-3 Research Network Component Diagram



2.5 SYSTEM DESCRIPTION

Table 2-5 System Names and Descriptions

System Name	System Description	Stakeholders
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 located at the healthcare site	Healthcare Delivery Organizations, Ancillary Entities, Clinicians, Care Delivery Interface



System Name	System Description	Stakeholders
Electronic Data Capture (EDC) System	Referred to as 'Site Study Data System' in Use Case Table 7.1. This system may handle data validation or it may be handled in a separate application	Sponsor
Clinical Data Management System (CDMS)	Clinical research repository where data are streamed for housing and cleansing. Out of scope; included for context only	Sponsor
Protocol Development System	System used to author protocols. Out of scope; included for context only	Sponsor
Electronic Source Document Archive	A system that embodies RFD Form Archiver interface, and stores electronic source information on behalf of the site. Can be an add-on to the EHR, a standalone application at the site, or an application hosted by a trusted third party to the site	Site
Data Safety Management Board (DSMB)	System to which adverse events are reported. Out of scope; included for context only	Site
Institutional Review Board (IRB) System	Committee whose primary responsibility is to protect the rights and welfare of human research subjects through appropriate review and approvals prior to beginning research. Out of scope; included for context only	Site
Reviewer System	Individuals or organizations that review the final tabulated dataset once the study is complete	Reviewer
Registry System	For retrospective studies, such as epidemiologic studies, the core dataset may be exchanged with the clinical system which houses the EHR and sent to various patient registries or research databases. Relevant to Scenario 2 only	Sponsor
Distributed Clinical Research Network System	An intermediate database or data repository that serves a network of healthcare and research sites. Relevant to Scenario 3 only	Site
Central Diagnostic System	A central laboratory or imaging diagnostic center to which research specific lab and image work is referred	Labs
Analysis and Reporting System	Sponsor-based system. Performs analysis on study data	Labs

2.6 EXCHANGE CONTENT DESCRIPTIONS

The exchange content descriptions answer one or more data requirements, and map to existing or planned HITSP constructs.

Table 2-6 Exchange Content Descriptions

Exchange Content Identifier	Exchange Content Name	Exchange Content Definition	Data Requirements
EC1	Clinical Research Document (CRD). (pending HITSP construct)	Continuity of Care Document (CCD) redacted to match the requirements of the protocol	DR4 DR5 DR6 DR7 DR8 DR9 DR10 DR12 DR14



Exchange Content Identifier	Exchange Content Name	Exchange Content Definition	Data Requirements
EC2	CRD	CRD expanded to include protocol and visit specific data not covered in the pre-population	DR4 DR5 DR6 DR7 DR8 DR9 DR10 DR12 DR13 DR14
EC3	CRD	Identifiers for patient, study, site, and investigator	DR1 DR2 DR3 DR14
EC4	HITSP/C76	Adverse Event Report	DR12
EC5	HITSP/C37	Lab Report Document	DR11
EC6	HITSP/TP89	Sharing Imaging Results	DR11

2.7 DATA REQUIREMENTS

The following data requirements support the exchange of data between electronic health records and clinical research systems.

Table 2-7 Data Requirements

Data Requirement Number (DR)	Description	Data
DR1	Planning and Reporting Requirements (Sources: CDISC Protocol Representation, CDISC Trial Design Model, HL7 Study Design)	Informed consents Eligibility verification Study design CRF template
DR2	Study Identifiers (data elements taken from CDISC Protocol Representation)	Study identifier - Unique Identifier for a study within a submission. Study Site identifier - The unique identification assigned to a study site by a study sponsor. StudyInvestigator.identifier The unique identification given to a study investigator by a study sponsor. StudyInvestigator.dateRange The date and time on which an investigator's participation in a specific study begins and ends. StudyInvestigator.signatureText The signed name of the investigator who is responsible for completing a form or report for a clinical trial. Investigator Name A non-unique textual identifier or moniker of a person. For example, proper names, nicknames, legal names of persons, etc. Study visit Study encounter - any participation by a participant



Data Requirement Number (DR)	Description	Data
DR3	Subject Demographics (HITSP/C83 Section 1)	Subject id@ Person id* Date of birth * Gender * Race (code list to be determined)* Ethnic/cultural background * Native language * Address * Phone* Patient Name* Marital status* Religious affiliation* Multiple birth indicator* Death indicator* Deceased date/time* Birth place* Date and time collected * Protected Health Information (Individually Identifiable Healthcare Information) can be used or not according to the privacy rules in play. Note that scenario 2, registry reporting, can be fully identified whereas scenario 1 is typically pseudonymized
DR4	Prior and Concomitant Medications (HITSP/C83 Section 2.1.2.8 Medication)	Medication Indication Dose Timing of medication Frequency Route Rate Length of time on medication Date and time collected
DR5	Medical History	Type of history Allergies Surgeries Family history Diet Exercise Concomitant therapies Date and time collected
DR6	Physical Examination	Body system examined Results Clinical comments Date and time collected
DR7	Substance Use	Type of substance Occurrence of use Frequency and duration Date and time collected
DR8	Vital Signs: (HITSP/C83 Section 15)	Result identifier Result date/time Result type Result status Result value Result interpretation Result reference range



Data Requirement Number (DR)	Description	Data
DR9	Family History (HITSP/C83 Section 18)	Pedigree Family Member Information Family Member Demographics Family Member Relationship Family Member Name Family Member Date of Birth Family Member Race Family Member Ethnicity Family Member Relationship Family Member Medical History Family Member Medical History Family Member Condition Family Member Age Family Member Cause of Death Family Member Age at Death Family Member Biological Sex Family Member Multiple Birth Status Family Member Age Family Member Genetic Test Code Family Member Genetic Test Name Family Member Genetic Test Result Family Member Genetic Test Date
DR10	List of Surgeries (HITSP/C83 Section 17)	Procedures Procedure Identifier Procedure Type Procedure Free Text Type Procedure Date/Time Procedure Provider
DR11	Diagnostic Data (HITSP/C83 Section 15)	Result Event Entry Result Identifier Result Date/Time Result Type Result Status Result Value Result Interpretation Result Reference Range
DR12	Adverse Clinical Events	Type of Event Severity Action Taken Outcome Date and Time Collected
DR13	Protocol-specific data not included in Clinical Research Document	Study Specific Data
DR14	Informed consent	Date and Time Consent Form was Executed

2.8 INFORMATION EXCHANGE REQUIREMENTS (IER) DESCRIPTIONS

The information exchange requirements specify the transactions among EHR, EDC, research network, archive systems, and central laboratories.



Table 2-8 Description of Information Exchange Requirements

Information Exchange Requirement Number (IER)	Description
IER1	Scenarios 1 and 3: EHR or research network system sends redacted patient header data (DR1, DR2, DR3, DR13) to EDC. Reference action 7.2.3.1. Confidentiality and consent policy configuration determines the specific data elements to be redacted
IER2	Scenario 1 and 3: EDC sends pseudonymous subject identifier to research network system or site EHR. Reference action 7.3.1.1
IER3	Scenarios 1 and 3: EHR or research network system sends redacted clinical research document to EDC. Reference action 7.2.5.1 part 1, 7.2.7.1, 7.3.6.1, IER8. Research protocol and confidentiality policy determines data elements to be redacted
IER4	Scenarios 1 and 3: EDC returns pre-populated CRF to EHR or Research Network system. Ref action 7.3.3.2 part 1, IER9
IER5	Scenarios 1 and 3: EHR or research network system sends completed case report form to EDC. Reference action 7.2.5.1 part 2, 7.3.3.2 part 2, IER10
IER6	Scenario 2: EHR sends patient information (DR1, DR2, DR3, DR13) to registry. Reference action 7.2.3.1, IER1
IER7	Scenario 2: Registry system sends subject identifier to EHR. Reference action 7.3.1.1, IER2
IER8	Scenario 2: EHR sends clinical research document to registry system. Reference action 7.2.6.1 part 1, IER3
IER9	Scenario 2: Registry system returns partially pre-populated registry form to EHR. Ref action 7.3.3.2 part 1, IER9
IER10	Scenario 2: EHR sends completed data form to Registry System. Reference 7.2.6.1 part 2, 7.3.3.2 part 2, IER5
IER11	Scenario 1 and 3: EHR or research network system sends document (CCD, CRD) to electronic source document archive. Ref. action 7.3.5.4
IER12	Scenario 1 and 3: Receive laboratory information from central diagnostic facilities. Ref action 7.3.4.1
IER13	Scenario 1 and 3: Receive image information from central diagnostic facilities. Ref action 7.3.4.1
IER14	Send/Receive adverse event report to IRB, DSMB, sponsor, reviewer

2.9 HITSP CAPABILITIES USED

The following Capabilities table summarizes the set of capabilities selected to support the Clinical Research Value Case scenarios. Capabilities work at the system level and use HITSP constructs (SC, TP, T, C) to realize information exchanges.

Table 2-9 HITSP Capabilities

Capability ID	Capability Name	Capability Description	IER
CAP119	Communicate Structured Document	This capability addresses interoperability requirements that support the communication of structured health data related to a patient in a context set by the source of the document who is attesting to its content. Several document content subsets, structured according to the HL7 CDA standard, are supported by this capability. The following are examples of the type of structured data that may be used: Continuity of Care Document (CCD) Emergency Department Encounter Summary Discharge Summary (In-patient encounter and/or episodes of care) Referral Summary Ambulatory encounter and/or episodes of care Consultation Notes History and Physical Personal Health Device Monitoring Document Healthcare Associated Infection (HAI) Report Document Document creators shall support a number of the HITSP specified coded terminologies as defined by specific content subsets specified in this capability	IER3, IER8, IER14
CAP120	Communicate Unstructured Document	This capability addresses interoperability requirements that support the communication of a set of unstructured health data related to a patient in a context set by the source of the document who is attesting to its content.	IER5, IER10



Capability ID	Capability Name	Capability Description	IER
		Two types of specific unstructured content are supported, both with a structured CDA header: PDF-A supporting long-term archival UTF-8 text	
CAP123	Retrieve Existing Data	This capability supports queries for clinical data (e.g., common observations, vital signs, problems, medications, allergies, immunizations, diagnostic results, professional services, procedures and visit history)	IER3, IER8
CAP124	Establish Secure Web Access	This capability is focused on providing a secured method to access information available from document repositories (e.g., Laboratory Report) in order to view them locally on a system. The chosen method for viewing the document content is through a web browser	IER1, IER2, IER3, IER4, IER5, IER6, IER7, IER8, IER9, IER10, IER11, IER12, IER13, IER14
CAP126	Communicate Lab Results Message	This capability addresses interoperability requirements that support the sending of a set of laboratory test results. Ordering Providers of Care receive results as a laboratory results message. The communication of the order is out of scope for this capability. The content of these test results may be either or both: General Laboratory Test Results; Microbiology Test Results This capability may use content anonymization	IER12
CAP127	Communicate Lab Results Document	This capability addresses interoperability requirements that support the communication of a set of structured laboratory results related to a patient in a context set by the source of the document who is attesting to its content. Non-ordering Providers of Care access historical laboratory results as documents and "copy-to" Providers of Care may receive document availability notifications to retrieve such lab report documents. Lab Report content creators shall support HITSP specified coded terminologies as defined by specific content subsets specified in this Capability for: General Laboratory Test Results; Microbiology Test Results. This capability may use content anonymization	IER12
CAP128	Communicate Imaging Information	This capability addresses interoperability requirements that support the communication of a set of imaging results (i.e., reports, image series from imaging studies) related to a patient in a context set. This is done by an Imaging System acting as the information source attesting to its content. This capability may use content anonymization	IER13
CAP135	Retrieve and Populate Form	This capability addresses interoperability requirements to support the upload of specific captured data (e.g. public health surveillance reportable conditions, healthcare associated infection reporting) to Public Health Monitoring Systems and Quality Organizations Systems and Clinical Research Systems. The forms presented may be pre-populated by information provided by the clinical or laboratory information systems to avoid manual re-entry. A number of supplemental information variables may be captured from within the user's clinical information system to improve the workflow and	IER3, IER8



Capability ID	Capability Name	Capability Description	IER
		timeliness of required reporting. One or more types of form content may be supported: Pre-population for Public Health Case Reports from Structured Documents using CDA Pre-population for Quality Data from Structured Documents using CDA Pre-population of Clinical Research Reports from structured documents. No pre-population content Systems may optionally support the means to retrieve request for clarifications	
CAP137	Communicate Encounter Information Message	This capability addresses interoperability requirements to send specific clinical encounter data among multiple systems. The content may be either or both: Encounter Data Message Radiology Results Message It may be used in conjunction with other capabilities such as those related to the communication of laboratory data. This capability includes optional anonymization of content	IER3, IER8
CAP138	Retrieve Pseudonym	This capability addresses interoperability requirements to support a particular type of anonymization that both removes the association with a data subject, and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. This enables a process of supplying an alternative identifier, which permits a patient to be referred to by a key that suppresses his/her actual identification information. The purpose of this capability is to offer a pseudonymization framework for situations that require the use of specific data without disclosing the specific identity of patients or providers. Pseudo-identifiers are intended to allow accessibility to clinical information, while safeguarding any information that may compromise the privacy of the individual patient or provider. However, unlike anonymization, the alternative identifier key can be used to re-identify the individuals whose data was used	IER2, IER6
CAP143	Manage Consumer Preference and Consents	This capability addresses management of consumer preferences and consents as an acknowledgement of a privacy policy. This capability is used to capture a patient or consumer agreement to one or more privacy policies; where examples of a privacy policy may represent a consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial. This capability also supports the recording of changes to prior privacy policies such as when a patient changes their mind on participation or requests that data no-longer be made available because they have left the region	IER1, IER2, IER3, IER4, IER5, IER6, IER7, IER8, IER9, IER10

Table 2-10 Summary of Relationships between Capabilities and Information Exchange Requirements¹

Capability	IERs Satisfied
CAP119 Communicate Structured Document	IER3, IER8, IER14
CAP120 Communicate Unstructured Document	IER5, IER10
CAP123 Retrieve Existing Data	IER3, IER8

¹ It is assumed that HITSP will update the capabilities selected for clinical research to include the appropriate entities in the list of interacting systems



Capability	IERs Satisfied
CAP124 Establish Secure Web Access	IER1, IER2, IER3, IER4, IER5, IER6, IER7, IER8, IER9, IER10, IER11, IER12, IER13, IER14
CAP126 Communicate Lab Results Message	IER12
CAP127 Communicate Lab Results Document	IER12
CAP128 Communicate Imaging Information	IER13
CAP135 Retrieve and Populate Form	IER3, IER8
CAP137 Communicate Encounter Information Message	IER3, IER8
CAP138 Retrieve Pseudonym	IER2, IER6
CAP143 Manage Consumer Preference and Consents	IER1, IER2, IER3, IER4, IER5, IER6, IER7, IER8, IER9, IER10



3.0 DESIGN

3.1 CAPABILITY ORCHESTRATION

The table and below illustrates the data flow and information exchanges between the primary Systems engaged in the support of the requirements described in Section 2.0. Subsets of these Systems perform information exchanges according to one or more of the HITSP Capabilities identified in this Specification. The in-scope requirements are supported by Capabilities previously specified by HITSP.

Table 3-1 Capability Orchestration

System	Capability	Optionality ²
Electronic Health Record (EHR) System	HITSP/CAP119 Communicate Structured Document	R
	HITSP/CAP123 Retrieve Existing Data	O
	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP135 Retrieve and Populate Form	R
	HITSP/CAP138 Retrieve Pseudonym	C(101)
	HITSP/CAP143 Manage Consumer Preference and Consents	R
Electronic Data Capture System	HITSP/CAP119 Communicate Structured Document	R
	HITSP/CAP123 Retrieve Existing Data	O
	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP 127 Communicate Lab Results Document	O
	HITSP/CAP135 Retrieve and Populate Form	R
	HITSP/CAP138 Retrieve Pseudonym	C(101)
	HITSP/CAP143 Manage Consumer Preference and Consents	R
Clinical Data Management System (CDMS)		Out of scope
Protocol Development System		Out of scope
Electronic Source Document Archive	HITSP/CAP135 Retrieve and Populate form	C(101)
Data Safety Management Board (DSMB)	HITSP/CAP119 Communicate Structured Document	O
	HITSP/CAP123 Retrieve Existing Data	O
	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP 127 Communicate Lab Results Document	O
	HITSP/CAP 128 Communicate Imaging Information	O
	HITSP/CAP135 Retrieve and Populate Form	R
	HITSP/CAP143 Manage Consumer Preference and Consents	R
Institutional Review Board (IRB) System	HITSP/CAP119 Communicate Structured Document	O
	HITSP/CAP123 Retrieve Existing Data	O
	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP 127 Communicate Lab Results Document	O
	HITSP/CAP 128 Communicate Imaging Information	O
	HITSP/CAP135 Retrieve and Populate Form	R
	HITSP/CAP143 Manage Consumer Preference and Consents	R
Distributed Clinical Research Network System	HITSP/CAP119 Communicate Structured Document	R
	HITSP/CAP123 Retrieve Existing Data	O

² Optionality = "R" for Required, "R2" for Required if Known or "O" for Optional, or "C" for Conditional



System	Capability	Optionality ²
	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP 127 Communicate Lab Results Document	O
	HITSP/CAP 128 Communicate Imaging Information	O
	HITSP/CAP135 Retrieve and Populate Form	R
	HITSP/CAP138 Retrieve Pseudonym	R
	HITSP/CAP143 Manage Consumer Preference and Consents	R
Central Diagnostic system	HITSP/CAP124 Establish Secure Web Access	R
	HITSP/CAP 127 Communicate Lab Results Document	R
	HITSP/CAP 128 Communicate Imaging Information	R
Analysis and Reporting System		Out of scope

Table 3-2 Conditions

Condition Code	Condition Description
C(101)	Optional for Scenario 2; Required for Scenarios 1 and 3.

3.1.1 ADDITIONAL CONSTRAINTS ON REQUIRED CAPABILITIES

This section describes the constraints that further limit the capabilities that are used.

Table 3-3 Additional Constraints on Capabilities

Capability	Constraint	Constraint Type	Purpose (Reason for this constraint)
HITSP/CAP123 Retrieve Existing Data	Data sent to the EDC, IRB, and DSMB must be pseudonymized or anonymized unless otherwise permitted through legal and out-of-band arrangements	Pre-condition	Required to protect the confidentiality of the study participant whose personal health information is sent for analysis
HITSP/CAP135 Retrieve and Populate Form	Data sent to the EDC, IRB, and DSMB must be pseudonymized or anonymized unless otherwise permitted through legal and out-of-band arrangements	Pre-condition	Required to protect the confidentiality of the study participant whose personal health information is sent for analysis
HITSP/CAP119 Communicate Structured Document	Data sent to the EDC, IRB, and DSMB must be pseudonymized or anonymized unless otherwise permitted through legal and out-of-band arrangements	Pre-condition	Required to protect the confidentiality of the study participant whose personal health information is sent for analysis
HITSP/CAP123 Retrieve Existing Data	Data sent to the EDC, IRB, or DSMB must be redacted to match the requirements of the research protocol	Pre-condition	Required to comply with regulations limiting the confidentiality of subjects in clinical studies
HITSP/CAP135 Retrieve and Populate Form	Data sent to the EDC, IRB, or DSMB must be redacted to match the requirements of the research protocol	Pre-condition	Required to comply with regulations limiting the confidentiality of subjects in clinical studies



Capability	Constraint	Constraint Type	Purpose (Reason for this constraint)
HITSP/CAP119- Communicate Structured Document	Data sent to the EDC, IRB, or DSMB must be redacted to match the requirements of the research protocol	Pre-condition	Required to comply with regulations limiting the confidentiality of subjects in clinical studies

3.1.2 EXISTING HITSP CONSTRUCTS

The table below provides a description of the existing HITSP constructs that will be used for this Value Case solution. It also specifies whether the construct will require modification based on the new sets of requirements that are being satisfied by the construct.

Table 3-4 Constructs and Required Modifications

HITSP Construct	Modification Required	Description
HITSP/C19 Entity Identity Assertion		The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system
HITSP/C25 Anonymize	Modify to accommodate clinical research anonymization.	The Anonymize Component provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. This construct defines the Component specification that provides the ability to anonymize patient identifiable information
HITSP/C26 Nonrepudiation of Origin		The Nonrepudiation of Origin Component provides the mechanisms to support Nonrepudiation of Origin, which refers to both the proof of the integrity and origin of documents in a high-assurance manner, which can be verified by any party. This Component does not provide Nonrepudiation of Receipt
HITSP/C32 Summary Documents Using HL7 Continuity of Care Document (CCD)		The Summary Documents Using HL7 Continuity of Care Document (CCD) Component describes the document content summarizing a consumer's medical status for the purpose of information exchange. The content may include administrative (e.g., registration, demographics, insurance, etc.) and clinical (problem list, medication list, allergies, test results, etc) information. This Component defines content in order to promote interoperability between participating systems such as Personal Health Record Systems (PHRs), Electronic Health Record Systems (EHRs), Practice Management Applications and others
HITSP/C35 Lab Result Terminology		The Lab Result Terminology Component defines the vocabulary for either message-based or document-based laboratory results reporting
HITSP/C37 Lab Report Document		The Lab Report Document Component prescribes the use of the standard Clinical Document Architecture Release 2 (CDA R2), as in the HL7 V3 2006 normative edition profiled by IHE LAB TF-3 for: transmission of complete, preliminary, final and updated laboratory results to the EHR system (local or remote) of the ordering clinician; transmission of complete, preliminary, final and updated (or notification) to the EHR system (local or remote) or other clinical data system of designated providers of care (with respect to a specific patient); transmission of laboratory result data from electronically enabled healthcare delivery and public health systems in standardized and anonymized format to authorized Public Health Agencies with less than one day lag time
HITSP/C39 Encounter Message		The Encounter Message Component supports the process of sending patient encounter data (excluding laboratory, radiology)



HITSP Construct	Modification Required	Description
		from a Biosurveillance Message Sender to a Biosurveillance Message Receiver
HITSP/C44 Secure Web Connection		The Secure Web Connection Component provides the capability to access documents through a secure web browser
HITSP/C48 Encounter Document Using IHE Medical Summary (XDS-MS)		The Encounter Document Using IHE Medical Summary (XDS-MS) Component supports the process of sending patient encounter data (excluding laboratory and radiology) in a document sharing functional flow scenario. Patient encounter data are captured as part of the normal process of care performed by healthcare providers, such as hospitals, emergency departments and outpatient clinics
HITSP/C62 Unstructured Document		The Emergency Message Distribution Element Transaction selects the Emergency Data Exchange Language (EDXL) Distribution Element (DE) v1.0 standard, and is a multicast notification message sent to an identified population (assume this is not to the general public, but to specifically identified populations, such as emergency departments)
HITSP/C74 Remote Monitoring Observation Document		The Remote Monitoring Observation Document Component describes the document content to convey medical information collected by remote monitoring management systems from monitoring devices and/or device intermediaries for the purpose of information exchange. The content may include administrative (e.g., registration, demographics, insurance, etc.) and clinical (results, vital signs, etc) information. This specification defines content in order to promote interoperability between participating systems. Such systems may include Remote Monitoring Management Systems, Personal Health Record Systems (PHRs), Electronic Health Record Systems (EHRs), Health Information Exchange infrastructure services and other persons and systems as identified and permitted
HITSP/C75 Healthcare Associated Infection (HAI) Report		The Healthcare Associated Infection (HAI) Report Component specifies a standard for electronic submission of Healthcare Associated Infection (HAI) Reports to the National Healthcare Safety Network (NHSN) of the Centers for Disease Control and Prevention (CDC). HITSP has adopted the HL7 Implementation Guide for CDA Release 2: NHSN Healthcare Associated Infection (HAI) Reports, Release 1 for this construct
HITSP/C76 Case Report Pre-Populate		The Case Report Pre-Populate Component supports the Data Mapping needed for Public Health Case Reports. Initially the Component supports only those data attributes that are universal or pertain to Drug Safety reporting. For those attributes that are universal in case reporting, this component may be used in support of pre-populating the remaining report types. However, other public health specific attributes will be addressed in subsequent releases
HITSP/C80 Clinical Document and Message Terminology		The Clinical Document and Message Terminology Component defines the vocabularies and terminologies utilized by HITSP specifications for Clinical Documents and Messages used to support the interoperable transmission of information
HITSP/C83 CDA Content Modules		The CDA Content Modules Component defines the content modules for document based HITSP constructs utilizing clinical information. These Content modules are based on IHE PCC Technical Framework Volume II, Release 4. That technical framework contains specifications for document sections that are consistent with all implementation guides for clinical documents currently selected for HITSP constructs
HITSP/C84 Consult and History & Physical Note		The Consult and History & Physical Note Component supports two types of commonly used clinical notes, a consult note, and a history and physical note. It is intended for use to support the



HITSP Construct	Modification Required	Description
		exchange of information from a consulting provider to a referring provider; and may also be used to provide background information from a referring provider to a consulting provider (e.g., prior reports)
HITSP/SC108 Access Control		The Access Control service provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives
HITSP/SC109 Security Audit		The Security Audit Service Collaboration describes the mechanism to record security relevant events in support of policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/SC111 Knowledge and Vocabulary		The Knowledge and Vocabulary Service Collaboration provides the ability to retrieve medical knowledge and terminology
HITSP/SC112 Healthcare Document Management		The Healthcare Document Management Service Collaboration provides the ability to share healthcare documents using a set of topologies, such as Media, e-Mail, Point-to-Point, Shared within a Health Information Exchange, and Shared within a larger community (made up of potentially diverse Health Information Exchanges)
HITSP/SC113 Query for Existing Data		The Query for Existing Data service collaboration provides the capability to query and retrieve data from another clinical system, and the capability to respond to same queries. It applies the necessary Security and Privacy constructs and supports all the queries found in TP21
HITSP/SC115 HL7 Messaging		The HL7 Messaging service collaboration provides the capability to send and receive HL7 messages. The Service Collaboration applies the necessary Security and Privacy constructs
HITSP/T15 Collect and Communicate Security Audit Trail		The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/T16 Consistent Time		The Consistent Time Transaction provides a mechanism to ensure that all of the entities that are communicating within the network have synchronized system clocks
HITSP/T17 Secured Communication Channel		The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing: mutual node authentication to assure each node of the others' identity; transmission integrity to guard against improper information modification or destruction while in transit; and transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes
HITSP/T18 View Laboratory Results from a Web Application		The View Laboratory Results from a Web Application Transaction allows a user to view a laboratory report through a secure browser. This Transaction uses the HITSP/C44 Secure Web Connection Component. It may not define all functions, constructs and standards necessary to implement a conforming system in a real world environment. In particular, an implementer must provide the technical infrastructure and security framework necessary to support operations in accordance with law, regulation, best practices and business agreements



HITSP Construct	Modification Required	Description
HITSP/T23 Patient Demographics Query		The Patient Demographics Query Transaction is intended to provide a 'list patients and their demographics' query/patient(s) and their demographics identified' response message pair (QBP^Q22, RSP^K22) for use wherever such needs exist. This Transaction document extracts the Health Level Seven (HL7) version 2.5 Query and Response data mapping. The underlying basis for this extraction can be found in the Integrating the Healthcare Enterprise IT Infrastructure Technical Framework, Patient Demographics Query integration profile
HITSP/T24 Pseudonymize	Modify to accommodate clinical research pseudonymization. Modify to include generalization and modification	The Pseudonymize Transaction describes a framework for including Pseudonymization Services where the use of "dummy" or pseudo references to specific patients or providers is required. Pseudo-identifiers are intended to allow accessibility to clinical information, while safeguarding any information that may compromise the privacy of the individual patient or provider. Using pseudo-identifiers can assist in compliance with HIPAA regulations regarding suppression of patient identification information
HITSP/T29 Notification of Document Availability		The Notification of Document Availability Transaction is based on the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement - Notification of Document Availability (NAV). The Notification of Document Availability Transaction defines a mechanism for a healthcare stakeholder (e.g. provider, public health, etc) to notify providers or the patient about information that is available for retrieval pertaining to an identified patient. This Transaction defines the format, content, encoding and transmission of notification messages and acknowledgements between IHE NAV Actors and a known recipient (either a person or system) that participate in the same XDS Affinity Domain
HITSP/T31 Document Reliable Interchange		The Document Reliable Interchange Transaction provides a standards-based mechanism for conveying a set of medical documents in a point-to-point network-based communication. This Transaction uses the IHE Cross-Enterprise Document Reliable Interchange (XDR) Integration Profile, a companion to the IHE Cross-Enterprise Document Sharing (XDS) Integration Profile. Cross-Enterprise Document Reliable Interchange (XDR) uses the XDS defined metadata formats in a simpler environment in which the communicating parties have agreed to a point-to-point interchange rather than communicating via document sharing
HITSP/T33 Transfer Documents on Media		The Transfer of Documents on Media Transaction describes both the type of media (CD-ROM, USB Memory, and e-Mail) that may be used to write the documents and provides a directory structure that must be followed in order for the contents to be successfully accessed and processed by systems. An example might be to transport data from one healthcare provider to another healthcare provider, or a healthcare consumer may wish to move the contents of a Personal Health Record (PHR) using physical media or e-Mail. This Transaction uses the IHE Cross-Enterprise Document Media Interchange Integration Profile developed by Integrating the Healthcare Enterprise (IHE), a companion to the IHE Cross-Enterprise Document Sharing (XDS) Integration Profile
HITSP/T64 Identify Communications Recipients		The Identify Communication Recipients Transaction is intended to serve the purpose of identification of communication recipients and the subsequent purpose of delivery of alerts and bi-directional communications (e.g., public health agencies notifying a specific group of service providers about an event). The method and criteria by which individuals are added to a directory is a policy decision, which is out of scope for this construct. It uses the Integrating the Healthcare Enterprise (IHE) Personnel White Pages



HITSP Construct	Modification Required	Description
		profile which provides access to basic directory information for identifying one or more recipients
HITSP/T66 Retrieve Value Set		The Retrieve Value Set Transaction is used to transform human or computer vocabularies. For example, it can be used to convert the initial capture of a human-readable concept into a computer vocabulary captured in a document or message that will be communicated. It may also be used in the reverse, to take computer vocabulary and convert to human-readable form
HITSP/T81 Retrieval of Medical Knowledge		The Retrieval of Medical Knowledge Transaction enables the request and receipt of additional knowledge about a medical concept based on specific context parameters. This transaction does not prescribe the knowledge content of the message returned but provides the specifications for the query for and receipt of additional knowledge. It uses the Health Level 7 (HL7) Context-Aware Information Retrieval (Infobutton) Specification: URL Implementation Guide as the base standard for implementation
HITSP/TP13 Manage Sharing of Documents		The Manage Sharing of Documents Transaction Package supports the sharing of patient records in the form of source attested objects called documents. A healthcare document is a composite of structured and coded health information, both narrative and tabular, that describes acts, observations and services for the purpose of exchange. No assumption is made by this construct in terms of the format and structure of the content of documents shared
HITSP/TP20 Access Control		The Access Control Transaction Package provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control; entity based access control; context based access control; and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents
HITSP/TP21 Query for Existing Data		The Query for Existing Data Transaction Package is based on the IHE Query for Existing Data Integration Profile (QED) which supports dynamic queries for clinical data, including vital signs, problems, medications, immunizations, diagnostic results, procedures and visit history. A wide variety of systems often needs access to dynamic clinical information stored and maintained in an EMR system or other clinical data repository. The construct makes the information widely available to other systems within and across enterprises to support provision of better clinical care
HITSP/TP22 Patient ID Cross-Referencing		The Patient ID Cross-Referencing Transaction Package is used for identifying and cross-referencing different attributes for the same patient. It contains a query for cross-reference and patient identity feed transactions. These transactions are used to identify patients from a list of potentials, and/or to communicate patient demographic data
HITSP/TP30 Manage Consent Directives		The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 Manage Sharing of Documents
HITSP/TP50 Retrieve Form for Data Capture	Modify to accommodate data redaction	The Retrieve Form for Data Capture Transaction Package enables capture of supplemental data variables not typically maintained in



HITSP Construct	Modification Required	Description
		an electronic health record or laboratory information system through a more seamless integration with the local information system. This allows for the local system to retrieve a form specific to the identified potential public health threat. In the context of quality, it allows for the local system to capture supplemental data elements required for quality reporting that may not be available to the electronic health record
HITSP/TP89 Sharing Imaging Results		The Sharing Imaging Results Transaction Package supports the process of sharing medical imaging results data. Imaging results data are captured as part of the normal process of care performed by healthcare providers. This data can be made available through document sharing for both clinical care and public health purposes

3.1.3 NEW HITSP CONSTRUCTS

The table below provides a description of the new HITSP constructs that will be created for this Value Case.

Table 3-5 New Constructs

New Construct	Construct Description	IER
HITSP/CXX Clinical Research Document	Defines the HITSP constraints applied to the IHE Quality, Research and Public Health (QRPH) Technical Framework Supplement 10 - Clinical Research Data Capture (CRD). The purpose of this IHE profile is to support a standard set of data in CCD format which the Form Filler provides for use in Clinical Research. In addition this profile references the ability to convert this output into a standard case report form, a Clinical Research Document	IER3, IER4, IER5, IER8, IER9, IER10
HITSP/CXX CDASH	Defines the subset of data within HITSP/C32 that is of consistent interest to researchers. Instrumental in the conversion of a Continuity of Care Document into a Clinical Research Document	IER3, IER4, IER5, IER8, IER9, IER10
HITSP/CXX	Anonymization specific to clinical research	



4.0 STANDARDS SELECTION

4.1 STANDARDS

4.1.1 REGULATORY GUIDANCE

Table 4-1 Regulatory Guidance

Regulation	Explanation
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
Health Insurance Portability and Accountability Act (HIPAA) -- Administrative Simplification	A listing of national standards plus rules adopted by federal regulation for electronically communicating specified administrative and financial healthcare transactions, and protecting the security and privacy of healthcare information, as applied to the three types of defined covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct any of the specified healthcare transactions. See the Code of Federal Regulations, Title 45, Parts 160, et. seq. for more information
Health Insurance Portability and Accountability Act (HIPAA) Code of Federal Regulations (CFR) Title 45, Part 164, Section 502(d) (CFR§164.502(d)) Uses and disclosures of protected health information: general rules	This is a specific reference to 45 CFR 164.502(d) which specifies the general rules for uses and disclosures of de-identified protected health information
21 CFR 11	This regulation states several requirements for electronic systems that may be used in clinical research settings
45 CFR 46	This regulation covers confidentiality and the role of IRBs for clinical research

4.1.2 SELECTED STANDARDS

Table 4-2 Selected Standards Linked to HITSP Constructs

Standard	Remarks
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 www.ansi.org



Standard	Remarks
American Society for Testing and Materials ASTM #E1986 -98 (2005) Standard Guide for Information Access Privileges to Health Information	The guide covers the process of granting and maintaining access privileges to health information. In particular, Table 2 Healthcare Personnel that Warrant Differing Levels of Access Control provides the necessary content for structural roles per ASTM E2595 and for user-based access controls enforcing patient consent directives
ASTM International 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
Digital Imaging and Communications in Medicine (DICOM) Attribute Level Confidentiality Supplement: #55	Adds a mechanism for selective protection of individual attributes within arbitrary DICOM service-object pair (SOP) instances. It may be used to achieve protection of identifying information, e.g. a reversible anonymization or pseudonymization of DICOM SOP instances while continuing to use unmodified lower level message and protocol services for network transfer, storage, and media exchange of composite image information objects. For more information visit medical.nema.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) HL7 Version 3 Standard: Clinical Document Architecture (CDA), Release 2	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. 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



Standard	Remarks
Health Level Seven (HL7) Version 2.5 ³	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
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. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication Profile (ATNA)	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 interface specific requirements. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Volume 2 Transactions, Appendix M Using Patient Demographics Query in a Multi-Domain Environment	Appendix M - Using Patient Data Query (PDQ) in a Multi-Domain Environment, provides an architectural discussion of how Query Parameter Definition, QPD-8 is processed
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later	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, Final Text, specifies the IHE transactions defined and implemented as of October 10, 2008. The latest version of the IHE Technical Framework is available at www.ihe.net

³ 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	Remarks
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Revision 4.0	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 Content Transactions (PCC-5) enables sharing of immunization information between immunization registries and clinical data consumers. 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 4.0, 2008 - 2009, Emergency Department Referral Integration Profile	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 Emergency Department Referral (EDR) Integration Profile enables the emergency department to provide information including the nature of the current problem, past medical history and medications with the person who will ultimately care for the patient. 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
International Organization for Standardization (ISO) Health informatics -- Directory services for security, communications and identification of professionals and patients, Technical Specification #21091	Defines minimal specifications for directory services for healthcare using the X.500 framework. This Technical Specification provides the common directory information and services needed to support the secure exchange of healthcare information over public networks. It addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction and international healthcare communications. ISO/TS 21091:2005 also supports directory services aiming to support identification of health professionals and organizations and the patients/consumers. The latter services include aspects sometimes referred to as master patient indices. The healthcare directory will only support standard LDAP Client searches. Specific implementation guidance, search criteria and support are out of scope of this document. For more information visit www.iso.org
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



Standard	Remarks
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
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
Internet Engineering Task Force (IETF) Tags for the Identification of Languages, "Request for Comment" (RFC) #3066, January, 2001	Describes a language tag for use in cases where it is desired to indicate the language used in an information object, how to register values for use in this language tag, and a construct for matching such language tags. For more information visit www.ietf.org
Internet Engineering Task Force (IETF) The application/pdf Media Type (RFC 3778)	PDF, the 'Portable Document Format', is a general document representation language that has been in use for document exchange on the Internet since 1993. This document provides an overview of the PDF format, explains the mechanisms for digital signatures and encryption within PDF files, and updates the media type registration of 'application/pdf'. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), HTTP HyperText Transfer Protocol HTTP/1.1 (RFC 2616)	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol, which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers [47]. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), MIME Multipurpose Internet Message Extensions (RFC 2045 to RFC 2049)	The first and second documents in this set define MIME header fields and the initial set of MIME media types. The third document describes extensions to RFC 822 formats to allow for character sets other than US-ASCII. The fourth document describes what portions of MIME must be supported by a conformant MIME implementation. It also describes various pitfalls of contemporary messaging systems as well as the canonical encoding model MIME is based on. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), SMTP Simple Mail Transfer Protocol (RFC 2821)	The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. While this document specifically discusses transport over TCP, other transports are possible. For more information visit www.ietf.org



Standard	Remarks
Internet Engineering Task Force (IETF), The MIME Multipart/Related Content-type (RFC 2387)	The Multipart/Related content-type provides a common mechanism for representing objects that are aggregates of related MIME body parts. This document defines the Multipart/Related content-type and provides examples of its use. For more information visit www.ietf.org
Organization for the Advancement of Structured Information Standards (OASIS) - ebMS OASIS/ebXML Messaging Services Specifications v2.1	Defines a Message Service protocol for reliable Business-to-Business data interchange. ebMS v2.1 adds quality of service features on top of transfer protocols such as HTTP and SMTP. Key qualities of service features include guaranteed delivery and nonrepudiation of receipt. ebMS v2.1 can reliably transfer any data type including XML, X12, EDIFACT, or binary data between two parties over the Internet. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) - ebRIM OASIS – ebXML Registry Information Model v2.1	The Registry Information Model provides a blueprint or high-level schema for the ebXML Registry. Its primary value is for implementers of ebXML Registries. It provides these implementers with information on the type of metadata that is stored in the Registry as well as the relationships among metadata Classes. The Registry information model: a) Defines what types of objects are stored in the Registry; b) Defines how stored objects are organized in the Registry. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) – ebXML Registry Information Model (3.0)	The Registry Information Model provides a blueprint or high-level schema for the ebXML Registry. Its primary value is for implementers of ebXML Registries. It provides these implementers with information on the type of metadata that is stored in the Registry as well as the relationships among metadata Classes. The Registry information model: a) Defines what types of objects are stored in the Registry; b) Defines how stored objects are organized in the Registry. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) – ebXML Registry Services Specification (3.0)	The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services defined in this document. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of eXtensible Access Control Markup Language (XACML) for Healthcare, Committee Draft, 14 October 2008	The XSPA XACML profile provides the necessary content for evaluating principal access control information against established security policy and making access control decisions enforcing established security policy. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare, Committee Draft, 14 October 2008	The XSPA WS-Trust profile provides the necessary content for exchange interoperable access control information facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.oasis-open.org



Standard	Remarks
Organization for the Advancement of Structured Information Standards (OASIS) -ebRS OASIS – ebXML Registry Services Specifications v2.1	The ebXML Registry provides a set of services that enable sharing of information between interested parties for the purpose of enabling business process integration between such parties based on the ebXML specifications. The shared information is maintained as objects in a repository and managed by the ebXML Registry Services defined in this document. For more information visit www.oasis-open.org
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
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
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.2 Committee Draft 01 June 23, 2008	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
World Wide Web Consortium (W3C) Web Services Description Language (WSDL) v1.1	WSDL is an XML-based language that provides a model for describing Web services. It is also an XML-based service description on how to communicate using web services. The WSDL defines services as collections of network endpoints, or ports. WSDL specification provides an XML format for documents for this purpose. For more information visit www.w3.org

4.1.3 INFORMATIVE REFERENCE STANDARDS

Table 4-3 Informative Reference Standards

Standard	Explanation
American Medical Association (AMA) Current Procedural Terminology (CPT®) Fourth Edition (CPT-4)	A uniform coding system used primarily to identify medical services and procedures furnished by physicians and other healthcare professionals. For more information visit www.ama-assn.org



Standard	Explanation
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
Digital Imaging and Communications in Medicine (DICOM) Part 3.12: Media Formats and Physical Media for Media Interchange	This DICOM Standard describes the services and the data necessary for the interchange of information between digital imaging computer systems found in health care settings. PS 3.12 of the DICOM Standard articulates the structure between the Media Storage Model and specific media. Media physical characteristics are also covered. For more information visit medical.nema.org
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 nonrepudiation 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 Information Processing Standards (FIPS) Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas Publication # 5-2, May, 1987	A set of two-digit numeric codes and a set of two-letter alphabetic codes for representing the 50 states, the District of Columbia and the outlying areas of the United States, and associated areas. The standard covers all land areas under the sovereignty of the United States, the freely associated states of Federated States of Micronesia and Marshall Islands, and the trust territory of Palau. For more information visit www.itl.nist.gov . NOTE: ASC X12 transactions and ASC X12N Implementation Guides do not allow use of this standard; instead they require use of the U.S. Postal Service's National Zip Code and Post Office Directory -- which provides similar alphabetic code values
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



Standard	Explanation
Health Level Seven (HL7) Common Terminology Services (CTS) Release 1	The HL7 Common Terminology Services (HL7 CTS) defines an Application Programming Interface (API) that can be used when accessing terminological content. The CTS specification was developed as an alternative to a common data structure. Instead of specifying what an external terminology must look like, HL7 has chosen to identify the common functional characteristics that an external terminology must be able to provide. As an example, an HL7 compliant terminology service will need to be able to determine whether a given concept code is valid within the particular resource. Instead of describing a table keyed by the resource identifier and concept code, the CTS specification describes an Application Programming Interface (API) call that takes a resource identifier and concept code as input and returns a true/false value. Each terminology developer is free to implement this API call in whatever way is most appropriate or them. It describes a set of API calls that represent the core functionality that will be needed by basic HL7 Version 3 applications. For more information visit www.hl7.org
Health Level Seven (HL7) Implementation Guide for CDA Release 2.0 Personal Health Monitoring Report (PHMR) DSTU Release 1	This HL7 profile on the use of CDA R2 has been developed within the HL7 community to define an exchange document in support of the remote health monitoring Use Case. The profile is provisionally selected pending a successful balloting within the HL7 community. The PHMR is a document that carries personal healthcare monitoring data. The data is transmitted either in the form of a summary or as raw data. The summary may be a result of analysis by a disease management service provider. For more information visit www.hl7.org
Health Level Seven (HL7) Implementation Guide for CDA Release 2: NHSN Healthcare Associated Infection (HAI) Reports, Release1	The Healthcare Associated Infection Report Implementation Guide describes a standard for electronic submission of Healthcare Associated Infection (HAI) Reports to the National Healthcare Safety Network (NHSN) of the Centers for Disease Control and Prevention (CDC). It defines the overall approach and method of electronic submission and prescribes constraints defining specific HAI report types. Further information can be retrieved from 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. 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 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration	The HL7 Version 2.3.1 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 are contained in the standard. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 - Query	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. For more information visit www.hl7.org



Standard	Explanation
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
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
Health Level Seven (HL7) Version 3.0 Context-Aware Information Retrieval Specification: URL Implementation Guide	Informative implementation guide for URL-based implementations of the context-aware information retrieval ("Infobutton") The goal of this infobutton implementation guide is to recommend a URL-based implementation of the context-aware information retrieval ("infobutton") domain. The intent is to provide a simple way to implement infobuttons that is compatible with the current state of the market in this area. Most infobutton implementations to date, especially on the side of on-line information resources, rely on URL-based APIs. For more information visit www.hl7.org
Health Level Seven (HL7) Version 3.0 Infrastructure Management - Query Infrastructure, Release 2 DSTU Ballot 1 - September 2008	Query Infrastructure domain specifies the formation of information queries and the responses to these queries to meet the needs of healthcare applications using the HL7 version 3 messaging standard. 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
Health Level Seven (HL7) Version 3.0 Standard: Transport Specification - Web Services Profile, Release 2 Committee Ballot 1 - May 2008	The Web Services Profile for HL7 promotes the use of Web Services to exchange HL7 messages and to ease interoperability between implementations. The profile focuses on basic Web services protocols and technologies like SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language), which lay the groundwork for more complex interactions based on higher-level Web services specifications. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) Exchange of Personal Health Record Content (XPHR)	The Exchange of Personal Health Record Content (XPHR) integration profile describes the content and format of summary information extracted from a PHR system used by a patient for import into healthcare provider information systems, and visa versa. The purpose of this profile is to support interoperability between PHR systems used by patients and the information systems used by healthcare providers. This profile does not address all the data exchange requirements of PHR systems. For more information visit www.ihe.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) 2007-2008 Trial Implementation Supplement Cross-enterprise Document Reliable Interchange (XDR) Release 3	This Supplement to the IHE IT Infrastructure Technical Framework provides a generic, standards based mechanism for conveying a set of medical documents in a point-to-point networked based communication. The current version of the XDR is specified in the XDR Trial Implementation Supplement to the ITI-TF, rev. 5.0, which is consistent with IHE XDS.b Supplement in term of document entry metadata. For more information visit www.ihe.net/technical_framework . NOTE: off-line mode transaction expected to be updated once standards are available for Web Services Off-line



Standard	Explanation
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	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.3.0 for Final Text, specifies the IHE transactions defined and implemented as of December 9, 2006. 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 - 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. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, 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 Final Text, specifies the IHE CT Integration Profile, and other transactions defined and implemented as of October 10, 2008. 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 or later, 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 interfaces, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single interface, 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. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, 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. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 - 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 5.0 or later, Cross Enterprise Sharing of Scanned Documents (XDS-SD) Integration Profile	This Integration Profile defines how to store healthcare metadata in clinical documents, including patient identifiers, demographics, encounter, order or service information, represented within a structured HL7 CDA R2 header, with a PDF or plaintext formatted document containing clinical information within a nonXMLBody. For more information visit www.ihe.net to retrieve Volume 1, and Volume 2 of the Framework



Standard	Explanation
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Cross-Enterprise Document Media Interchange (XDM) Integration Profile	Provides document interchange using a common file and directory structure over several standard media types. This permits the patient to use physical media to carry medical documents. This also permits the use of person-to-person email to convey medical documents. XDM supports the transfer of data about multiple patients within one data exchange. Visit www.ihe.net for more information
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, 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. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 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 5.0 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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0, Basic Patient Privacy Consents (BPPC) Profile	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 Interfaces (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* Interfaces 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) Revision 5.0, 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) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	The experience of immunization registries and other public health population databases has shown that matching and linking patient records from different sources for the same individual person in environments with large proportions of pediatric records requires additional demographic data. Pediatric Demographics makes use of the following six additional demographic fields to aid record matching in databases with many pediatric records. 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 2008-2009 Sharing Value Sets (SVS) Integration Profile	The Sharing Value Sets (SVS) Integration Profile provides a means through which healthcare systems producing clinical or administrative data, such as diagnostic imaging equipment, laboratory reporting systems, primary care physician office EMR systems, or national healthcare record systems, can receive a common, uniform nomenclature managed centrally. Shared nomenclatures are essential to achieving semantic interoperability. For more information visit www.ihe.net



Standard	Explanation
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008-2009, Cross-Community Access (XCA), Trial Implementation, October 10, 2008	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-Technical Framework, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. For more information visit 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 2007 – 2008, Notification of Document Availability Integration Profile, Draft for Trial Implementation, October 10, 2008	The Notification of Document Availability Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems within a Cross-Enterprise Document Sharing affinity domain (See IHE IT Infrastructure XDS Integration Profile), eliminating the need for manual steps or polling mechanisms for a Document Consumer to be aware that documents that may be of interest have been registered with an XDS Document Registry Interface. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement, Retrieve Form for Data Capture (RFD), Draft for Trial Implementation, October 10 2008	The Retrieve Form for Data Capture Profile (RFD) provides a method for gathering data within a user's current application to meet the requirements of an external system. RFD supports the retrieval of forms from a form source, display and completion of a form, and return of instance data from the display application to the source application. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework, Revision 4.0 or later, Personnel White Pages profile	The Personnel White Pages (PWP) Profile provides access to basic directory information on human workforce members to other workforce members within the enterprise. This information has broad use among many clinical and non-clinical applications across the healthcare enterprise. This Personnel White Pages Profile specifies a method of finding directory information on the User Identities (user@realm) supplied by the Enterprise User Authentication (EUA) Integration Profile. For more information visit 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) - Emergency Department Encounter Summary (EDES), Technical Framework Supplement, Volume I, 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 Emergency Department Encounter Summary (EDES) enables the sharing of emergency department summary 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 .



Standard	Explanation
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Supplement 2008 – 2009, Draft for Trial Implementation, August 22, 2008	The Query for Existing Data Profile (QED) supports dynamic queries for clinical data, including vital signs, problems, medications, immunizations, diagnostic results, procedures and visit history. This profile makes the information widely available to other systems within and across enterprises to support provision of better clinical care. The QED profile leverages the existing content modeling defined previously in other IHE document profiles and the HL7 CCD Implementation Guide to deliver information that is semantically equivalent as a web service using the IHE ITI web services and HL7 web services guidelines. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Supplement 2008-2009, Immunization Content (IC), Trial Implementation Version 1.0	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementation (called Integration Profiles) of established standards to deal with integration issues the cross providers, patient problems or time. The Immunization Content (IC) Supplement enables sharing of a standard document to exchange immunization data. It is intended to facilitate the exchange of immunization data among multiple systems belonging to a single or to multiple organizations. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 4.0, 2008 - 2009, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	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) Quality, Research and Public Health (QRPH) Technical Framework Supplement 2008 – 2009, Drug Safety Content (DSC) Profile, Public Comment, Version 10	Describes the content and format to be used within the Pre-population Data transaction described within the RFD Integration Profile. The purpose of this profile is to support a standard set of data in CCD format which the Form Filler provides for use in reporting adverse events as it relates to Drug Safety. In addition this profile will reference the ability to convert this output into the ICH E2B (R3) standard. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Radiology Technical Framework Revision 8.0	The IHE Radiology Technical Framework specifies the Cross-Enterprise Document Sharing for Imaging (XDS-I) Integration Profile which enables sharing of imaging documents such as radiology images and reports across healthcare enterprises. XDS-I extends XDS by sharing, locating and accessing DICOM Instances from its original local sources, e.g., for radiologists or oncologists. For more information visit www.ihe.net
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	The International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS), describes the classification of inpatient procedures for statistical purposes and for the indexing of healthcare records by procedures. ICD-10-PCS is a procedural coding system managed by the Centers for Medicare and Medicaid Services (CMS). For more information visit www.cms.hhs.gov . Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Classification of Diseases, 10th Revision, Related Health Problems (ICD-10-CM)	The International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM), describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases. The National Center for Health Statistics (NCHS), the Federal agency responsible for use of the International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) in the United States, developed a clinical modification of the classification for morbidity purposes. For more information visit www.cdc.gov/nchs . Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Classification of Diseases, 9th Revision, Clinical Modifications (ICD-9-CM)	The International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), Volumes I, II (diagnoses) and III (procedures) describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases and procedures. For more information visit www.cdc.gov/nchs



Standard	Explanation
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
International Organization for Standardization (ISO) Health informatics - 9660 Level 1	Defines a common logical format for files and directories so discs written to ISO 9660 specifications can be read by a wide array of computer operating systems. For more information visit www.iso.org
International Organization for Standardization (ISO) Health Informatics -- Pseudonymisation, Unpublished Technical Specification # 25237	Health Informatics – Pseudonymisation. Approved as a Technical Specification March, 2007. For more information visit www.iso.org
International Organization for Standardization (ISO) PDF/A ISO 19005-1b. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF (PDF/A)	Specifies how to use the Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster and vector data. For more information visit www.iso.org
Internet Engineering Task Force (IETF) Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) (RFC) #2818, May 2000	Describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. For more information visit www.ietf.org
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
ISO/IEEE 11073-10101 Health informatics - Point-of-care Medical Device Communication – Nomenclature	Within the context of the ISO/IEEE 11073 family of standards for point-of-care (POC) medical device communication (MCD), this standard provides the nomenclature that supports both the domain information model and service model components of the standards family, as well as the semantic content exchanged with medical devices. The nomenclature is specialized for patient vital signs information representation and medical device informatics, with major areas including concepts for electrocardiograph (ECG), haemodynamics, respiration, blood gas, urine, fluid-related metrics, and neurology, as well as specialized units of measurement, general device events, alarms, and body sites. The standard defines both the architecture and major components of the nomenclature, along with extensive definitions for each conceptual area. Device specific information is defined in: · IEEE 11073-10404 - Health Informatics Personal Health Device Communication Device Specialization Pulse Oximeter · IEEE 11073-10407 - Health Informatics Personal Health Device Communication Device Specialization Blood Pressure Monitor · IEEE 11073-10408 - Health Informatics Personal Health Device Communication Device Specialization Thermometer · IEEE 11073-10415 - Health Informatics Personal Health Device Communication Device Specialization Weighing Scale · IEEE 11073-10417 - Health Informatics Personal Health Device Communication Device Specialization Glucose Meter. For more information visit standards.ieee.org



Standard	Explanation
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 Uniform Billing Committee (NUBC) Uniform Bill Version 1992 (UB-92) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	A code set identifying status of patient discharge on an institutional claim (e.g., inpatient, outpatient, hospice, home care). For more information visit www.nubc.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 XACML 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
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
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 Token Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. 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
USB Removable Device Type 2.0 (USB Implementers Forum)	The USB-IF was formed to provide a support organization and forum for the advancement and adoption of Universal Serial Bus technology. The Forum facilitates the development of high-quality compatible USB peripherals (devices), and promotes the benefits of USB and the quality of products that have passed compliance testing. For more information visit www.usb.org

4.2 GAPS WHERE THERE ARE NO STANDARDS

The table below identifies the Scenario requirements and known associated gaps, along with the recommended resolutions.



Table 4-4 Use Case Requirements and Associated Standards Gaps

Requirement Number	Summary Description	Identified Gaps	Recommended Resolution
IER3	The data sent from the EHR to the EDC must conform to the protocol. Currently there is a gap in the ability to redact the CCD to conform to the protocol required data as specified in the case report form	<p>CCD provides a snapshot of the patient's record at that time. The case report form requires a subset of data elements that conform to the research protocol. CRD has the capability to redact the CCD, but RFD does not have the transactions needed to allow the redaction to take place</p> <p>CRD takes the policy agreement of the two parties, EHR and EDC, and creates the definition of what data elements to pull from the CCD</p>	<p>July 2009: Discussions among RFD implementers and developers at IHE propose extensions to RFD. Sept 2009: Draft change proposal to RFD. Fall 2009: Submit same to IHE ITI for approval.</p> <p>Include the change proposal to CRD</p>

4.3 STANDARD OVERLAPS

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

Table 4-5 Use Case Requirements and Associated Standard Overlaps

Requirement Number	Summary Description	Standard Overlap	Recommended Resolution
Not applicable			



5.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

5.1 USE CASE TO INFORMATION EXCHANGE AND DATA REQUIREMENTS

This section contains an extraction of systems, required interactions and conditions/scenarios from the Use Case into a matrix/table.

Note the following:

- Actions and numbering are not intended to be sequential and can be iterative and should not be interpreted as a sequence diagram. Actions may not occur sequentially

Table 5-1 Mapping of Use Case Actions to Information Exchange Requirements

Event	Action	IER	Initiating System	Responding System	Information Exchange	Comments
7.1.1 Event: Complete and communicate study design	7.1.1.1 Action: Develop study design and protocol	N/A	Protocol Development System	N/A	DR1	Out of scope. Action Included in scenario for context only
	7.1.1.2 Action: Working with the Principal Investigator	N/A	Protocol Development System	EHR	DR1	Out of scope. Action Included in scenario for context only
	7.1.1.3 Action: Sponsor sends design and protocol to investigative site and Reviewer(s)	N/A	Protocol Development System	Reviewer's system, CRO, EDC, EHR	DR1	Out of scope. Action Included in scenario for context only
7.1.2 Event: Send case reporting form (CRF Template) from centrally hosted server	7.1.2.1 Action: Sponsor sends CRF to the Investigative Site data manager	N/A	Protocol Development System	EDC, EHR	DR1	Out of scope. Action Included in scenario for context only
7.1.3 Event: Receive, validate and tabulate CRF study data	7.1.3.1 Action: Study data is received from the Investigative Site	N/A	EHR	EDC	DR2 – DR9	Out of scope. Action Included in scenario for context only
	7.1.3.2 Action: Study data is validated	N/A	Clinical Data Management System (CDMS)	N/A	DR2 – DR9	Out of scope. Action is internal to one system
	7.1.3.3 Action: Study data is tabulated	N/A	CDMS	N/A	DR2 – DR9	Out of scope. Action is internal to one system
7.1.4 Event: Monitor site as necessary	7.1.4.1 Action: Sponsor monitors investigative site	N/A	CDMS, EDC	EHR	DR2 – DR9	Out of scope. Beyond boundaries of data exchange.
7.1.5 Event: Transmit interim data	7.1.5.1 Action: Interim data is transmitted to a Reviewer	N/A	CDMS	Reviewer	DR2 – DR9	Out of scope. Beyond boundaries of data exchange
7.1.6 Event: Transmit final data	7.1.6.1 Action: Final data and application for approval is sent to the Reviewer	N/A	CDMS, Analysis and Reporting system	Reviewer	DR1 – DR9	Out of scope. Beyond boundaries of data exchange
7.2.1 Event: Receive study design including CRF	7.2.1.1 Action: Site receives study design	N/A	EDC	EHR	DR1	Out of scope. Action Included in scenario for context only



Event	Action	IER	Initiating System	Responding System	Information Exchange	Comments
parameters into EHR system	7.2.1.2 Action: Study sent to Institutional Review Board (IRB) for approval	N/A	EDC	IRB	DR1	Out of scope. Action Included in scenario for context only
7.2.2 Event: Identify/select eligible study subjects*	7.2.2.1 Action: Study subjects are selected for the study according to the eligibility criteria set in the study protocol and design	N/A	EHR	N/A	Application specific	Out of scope. Action is internal to one system
7.2.3 Event: Register study subject in EHR clinical system	7.2.3.1 Action: Study subject is enrolled in the EHR clinical system	IER1	EHR	EDC	DR1 - 3	In scope. EHR identifies patient as a candidate subject for the study and requests subject identifier from the study data system. Patient may receive a temporary screening number before the permanent enrollment number is assigned. Certificate of Confidentiality may prevent EHR from identifying a patient as an enrolled subject or it may limit such identification to certain 'need to know' EHR users
7.2.4 Event: Perform clinical activities	7.2.4.1 Action: Perform all patient activities related to the clinical study	N/A	EHR	N/A		Out of scope. Action is internal to one system
	7.2.4.2 Action: Record all study related information to form the source document	N/A	EHR	N/A	DR2 – DR9	Out of scope. Action is internal to one system
7.2.5 Event: Send information to study data system	7.2.5.1 Action: Source document is sent to the study data system	IER3, IER5	EHR	EDC	DR2 – DR9	In scope. Must ensure that only protocol-specified data are sent from the EHR. This action takes place in two parts: 1. Send EHR extract and request form; 2. send completed CRF. IER3 and IER5
7.2.6 Event: Extract core dataset from EHR and send information to registry or database	7.2.6.1 Action: Information is sent to registries or other databases (Scenario 2 only)	IER8, IER10	EHR	Registry system	DR2 – DR9	In scope, Scenario 2. This action takes place in two parts: 1. Send DHR extract and request form; 2. send complete CRF return. IER8 and IER10
7.2.7 Event: Periodically exchange data from EHR in a distributed network	7.2.7.1 Action: Data is exchanged with the clinical system (EHR) and sent to an intermediate database	IER3	EHR	Distributed Clinical Research Network system	DR2 – DR9	In scope for Scenario 3



Event	Action	IER	Initiating System	Responding System	Information Exchange	Comments
7.3.1 Event: Enroll subject in study	7.3.1.1 Action: Patient is enrolled in study	IER2	EDC	N/A	DR2	In scope. Subject identifier is returned to EHR ('Enrolled' means to be randomized into trial) IER2
	7.3.1.2 Alternative Action	N/A	EDC	N/A	N/A	Out of scope. Null case where patient does not meet criteria. Sponsor may still have interest in the subject information
7.3.2 Event: Retrieve case reporting form (CRF Template)	7.3.2.1 Action: Data manager obtains a CRF template from a server managed by the study sponsor	N/A	Protocol Development System	EDC, EHR	DR1	Out of scope. Action included in scenario for context only
7.3.3 Event: Receive data from clinical personnel or EHR	7.3.3.1 Action: Data Manager receives the data from the clinical study coordinator and enters the data into a study database	N/A		EDC	DR2 – DR9	Out of scope. Action included in scenario for context only
	7.3.3.2 Alternative Action: Data from the EHR is pre-populated on an electronic form with study specific information entered electronically	IER4, IER5, IER9, IER10	EDC	EHR	DR2 – DR9	In scope. Action takes place two steps: 1. Pre-population data received and mapped to form and returned to EHR (IER4, IER9); 2. Final completed data form received from EHR (IER5, IER10)
7.3.4 Event: Receive and incorporate results from Central Diagnostics into study database	7.3.4.1 Action: Diagnostic information is received and incorporated into the study database	IER12, IER13	Central Diagnostic System	EDC or EHR	DR11	In scope. IER12, IER13
7.3.5 Event: Complete, validate and transmit CRF to Sponsor and e-Source Document Archive.	7.3.5.1 Action: Data is completed and validated	N/A	EDC	EHR, Source archive	DR2 – DR9	Out of scope. Action Included in scenario for context only
	7.3.5.2 Action: Various safety boards' monitor the study	N/A	EDC, CDMS	DSMB, IRB	DR2 – DR9	Out of scope. Action Included in scenario for context only
	7.3.5.3 Action: CRF data is transmitted to sponsor	N/A	EDC	CDMS	DR2 – DR9	Out of scope. Action Included in scenario for context only
	7.3.5.3a Alternative Action: Additional clarification of transmitted CRF data	N/A	EDC, EHR	CDMS		Out of scope. Action Included in scenario for context only
	7.3.5.4 Action: CRF data is transmitted to Electronic Source Document Archive	IER11	EHR	Source Archive	DR2 – DR9	In scope. Data are archived at the same time that data are received at the EDC system



Event	Action	IER	Initiating System	Responding System	Information Exchange	Comments
7.3.6 Event: Exchange aggregated longitudinal data from distributed network with organizational database	7.3.6.1 Action: Longitudinal information is aggregated and sent to an organizational database	IER3	EHR	Distributed Clinical Research Network System	DR2 – DR9	Scenario 3. IER3
7.4.1 Event: Receive study design including CRF parameters	7.4.1.1 Action: Reviewer receives a version of the study design and CRF parameters	N/A	Protocol Development System	Reviewer System	DR1	Out of scope. Action Included in scenario for context only
7.4.2 Event: Register study	7.4.2.1 Action: Clinical study is registered with the reviewer	N/A	Protocol Development System	Reviewer System	DR1	Out of scope. Action Included in scenario for context only
7.4.3 Event: Receive interim data and/or audits	7.4.3.1 Action: Sponsor sends interim data reports and/or audits to the reviewer	N/A	CDMS	Reviewer System	DR2 – DR9	Out of scope. Action Included in scenario for context only
	7.4.3.2 Action: Sponsor and reviewer may exchange information regarding the ongoing study	N/A	CDMS, Reviewer System	Reviewer System, CDMS	DR2 – DR9	Out of scope. Action Included in scenario for context only
7.4.4 Event: Receive final data	7.4.4.1 Action: Sponsor sends final data at the end of the clinical study	N/A	CDMS	Reviewer System	DR2 – DR9	Out of scope. Action Included in scenario for context only
7.5.1 Event: Receive aggregated data from distributed network	7.5.1.1 Action: Aggregated data is received by the organizational database	N/A	CDMS	Distributed Clinical Research Network System	DR2 – DR9	Out of scope. Action Included in scenario for context only

