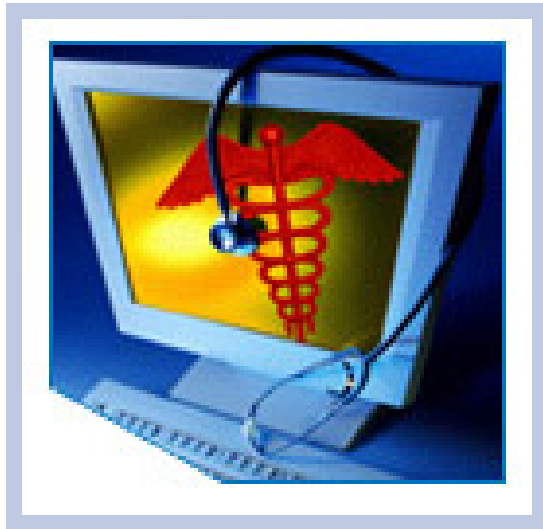


HITSP Remote Monitoring Interoperability Specification

HITSP/IS77



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Consumer Perspective Technical Committee



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
	Template Updated to V2.4	Project Team	July 31, 2008
0.0.1	Review Copy	Consumer Perspective Technical Committee	September 26, 2008
0.0.2	Review Copy	Consumer Perspective Technical Committee	December 10, 2008
1.0	Released for Implementation	Consumer Perspective Technical Committee	December 18, 2008



TABLE OF CONTENTS

1.0	INTRODUCTION	6
1.1	Interoperability Specification Overview	6
1.2	Interoperability Specification Document Map	7
1.2.1	List of Constructs	8
1.3	Copyright Permissions	11
1.4	Reference Documents	11
2.0	INTEROPERABILITY REQUIREMENTS	13
2.1	Use Case Synopsis	13
2.2	Use Case Requirements	15
2.2.1	Mapping of Use Case Actions to Information Exchange Requirements	16
2.2.2	Data and Information Exchange Requirements	16
2.2.3	Identification of Business Actors, and Scenarios	22
2.2.4	High-Level Business Sequence Diagram	24
3.0	DESIGN	27
3.1	Scope of Design	27
3.1.1	Assumptions	29
3.1.2	Constraints	30
3.1.3	Pre-conditions	30
3.1.4	Post-conditions	31
3.1.5	Process Triggers	31
3.2	Detailed Design	32
3.2.1	Technical Actor Role Descriptions	34
3.2.2	Construct Requirements	36
3.2.3	Mapping of Business Actors to Technical Actors and Constructs with Optionality	38
3.2.4	Construct Dependencies	45
3.2.5	Additional Constraints on Required Constructs	45
4.0	STANDARDS SELECTION	47
4.1	Standards	48
4.1.1	Regulatory Guidance	48
4.1.2	Selected Standards	49
4.1.3	Informative Reference Standards	54
4.2	Gaps Where There Are No Standards	58
4.3	Standard Overlaps	62
4.3.1	Strategy for HITSP/IS77 and Completing IER39 (HITSP/T73)	62



5.0	TECHNICAL IMPLEMENTATION	65
5.1	Conformance Criteria	65
5.2	Conformance Scoping, Subsetting and Options	65
5.3	Test Methods	66
6.0	APPENDIX	67
6.1	Description of Standards	67
6.2	Use Case to Information Exchange and Data Requirements	78
6.3	Use Case Sequence Diagrams	87
6.4	Mapping of Constructs to Information Exchange and Data Requirements	90
7.0	CHANGE HISTORY	92
7.1	December 10, 2008	92
7.2	December 18, 2008	92



FIGURES AND TABLES

Figure 1.2-1 Interoperability Specification Document Map	8
Figure 2.2.4-1 Business System Interfaces	25
Figure 2.2.4-2 Remote Monitoring Component Data Flow Diagram	26
Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1	37
Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2	38
Figure 6.3-1 Evaluate Patient and Order Remote Monitoring.....	87
Figure 6.3-2 Setup and Receive Remote Monitoring Summary	87
Figure 6.3-3 Evaluate/Manage Patient, and Modify Treatment Plan & Communicate with Patient	88
Figure 6.3-4 Initiate Remote Monitoring and Coordinate with Patient	88
Figure 6.3-5 Receive Remote Monitoring Data, and Utilize Device to Obtain Measurements.....	89
Figure 6.3-6 Receive Remote Monitoring Data, and Patient Modifies Meds, Dosage, Activities, Diet, etc.	89
Table 1.2.1-1 List of Constructs	8
Table 1.3.1-1 Reference Documents	12
Table 2.2.2-1 Data Element and Information Requirements	16
Table 2.2.2-2 Information Exchange Requirements (IER).....	20
Table 2.2.3-1 Business Actors	22
Table 3.1-1 Scoping Clarifications	27
Table 3.1.1-1 Assumptions	29
Table 3.1.2-1 Constraints.....	30
Table 3.1.3-1 Pre-conditions.....	30
Table 3.1.4-1 Post-conditions	31
Table 3.1.5-1 Process Triggers.....	31
Table 3.2.1-1 Technical Actor Role Descriptions.....	34
Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content	39
Table 3.2.3-2 Implementation Conditions/Constraints.....	44
Table 3.2.4-1 Construct Dependencies	45
Table 3.2.5-1 Additional Constraints on Required Constructs.....	46
Table 4.1.1-1 Regulatory and Guidance Standards	49
Table 4.1.2-1 Selected Standards Linked to HITSP Constructs.....	49
Table 4.1.3-1 Informative Reference Standards.....	54
Table 4.2-1 Use Case Events and Associated Gaps.....	58
Table 4.2-2 Remote Monitoring Roadmap.....	60
Table 4.3-1 Use Case Requirements and Associated Standards Overlaps.....	62
Table 4.3-2 Selected Nomenclature Standards for HITSP/T73.....	63
Table 6.2-1 Description of Standards	67
Table 6.2-1 Mapping of Use Case Actions to Information Exchange Requirements	78
Table 6.4-1 Mapping of Requirements to HITSP Constructs.....	90



1.0 INTRODUCTION

As an introduction to the Healthcare Information Technology Standards Panel (HITSP) Remote Monitoring Interoperability Specification, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for the Interoperability Specification, acknowledges the copyright protections that pertain, and provides a list of reference documents and background material.

1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

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

The HITSP Remote Monitoring Interoperability Specification addresses the data and information exchange requirements for the transfer of remote monitoring information from a device physically attached to or used by a patient in a location that is remote to the clinician.

The data to be transferred is directly related to the type of device that is sourcing the information. The data requirements will include both discrete measurements (e.g. physiological, diagnostic, medication tracking, and activities of daily living (ADL) measurements) as well as more descriptive information regarding the characteristics of the device itself, conditions regarding the monitoring activity, and/or commentary provided by the patient, a family care giver or a professional care coordinator. The objective of the information exchange is to provide a necessary and sufficient level of information to the clinician that has ordered this health monitoring activity to permit this individual to continue in the management of this patient's care from a remote location.

The information exchange requirements described in this specification document allow for the maximum segmentation of exchange steps to facilitate the maximum number of implementation variants. The main "business actor" systems specified as part of this exchange are: the monitoring device, a device intermediary system, a remote monitoring management system, and an EHR system. Although not specifically highlighted in the Use Case, this specification has also covered the implementation variants using a patient PHR system and/or a health information exchange resource as part of the exchange path. The overall remote monitoring information exchange is divided into a sequence of system exchanges between the business actor systems depending on the implementation variant. For example, implementations might be comprised of:

Variant 1. A transfer from the device to a device intermediary system (herein referred to as system data exchange #1), a transfer from a device intermediary to a remote monitoring management system (herein, system data exchange #2), and a transfer from the remote monitoring management system to the EHR (herein, system data exchange #4)



Variant 2. A transfer from the device to a device intermediary system (herein referred to as system data exchange #1), a transfer from a device intermediary to a remote monitoring management system (herein, system data exchange #2), a transfer from a remote monitoring management system to an HIE repository (herein, system data exchange #3), and a transfer from the HIE to the EHR (herein, system data exchange #5).

Per the Use Case, the transfer of the data from the device to the device intermediary has been indicated as out-of-scope at this time but may be re-visited at some time in the future. Despite this out-of-scope designation however, this Table recognizes the device as the originating source of the data and therefore has given full consideration to the IEEE industry specifications for this data at the device and to the harmonization of these data specifications with other related data terminology standards initiatives targeting its use in EHRs and PHRs.

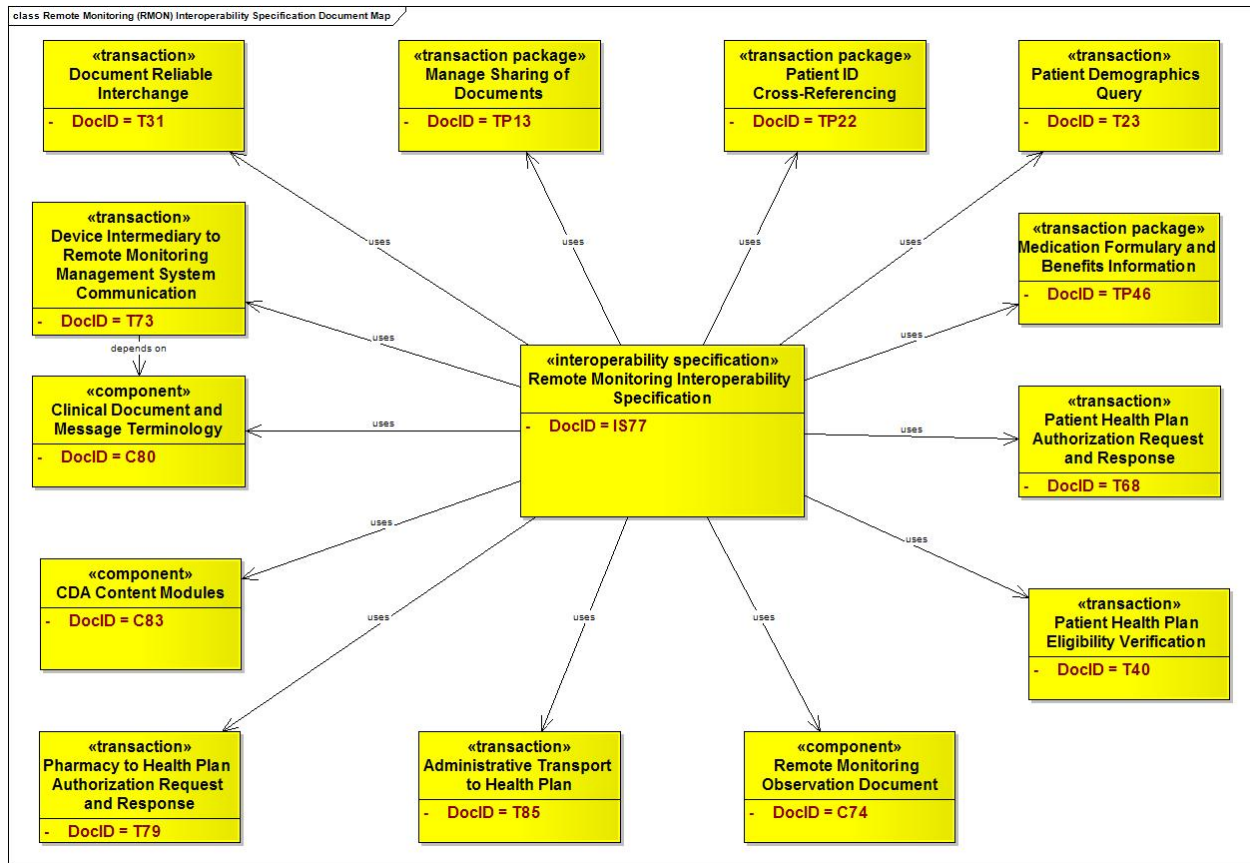
In addition to the transfer of the remote monitoring information itself, this Table also describes the pertinent administrative and finance transactions that need to be supported by the clinician's EHR system to satisfy the eligibility and authorization of the desired remote monitoring activities with a patient's health plan.

1.2 INTEROPERABILITY SPECIFICATION DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant context(s) for the use of HITSP constructs that further identify and constrain standards where necessary. In addition to ISs, there are three other types of HITSP constructs called Transaction Packages (TP), Transactions (T), and Components (C). The document map depicted in Figure 1.2-1 depicts how this IS integrates and constrains HITSP constructs to support the information exchange, within the defined context of the Use Case. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses. Note that the baseline Security and Privacy constructs are not shown in the diagram; however, they are described in Table 1.2.1-1.



Figure 1.2-1 Interoperability Specification Document Map



1.2.1 LIST OF CONSTRUCTS

The following table lists and describes the HITSP constructs that are used by the Interoperability Specification. All references to HITSP specifications are to the current, and Panel approved 'Released for Implementation' versions of the specifications retrieved from www.hitsp.org.

Table 1.2.1-1 List of Constructs

Construct	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



Construct	Description
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/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/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/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^K22, 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/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



Construct	Description
HITSP/T40 - Patient Health Plan Eligibility Verification	The Patient Health Plan Eligibility Verification Transaction is intended to provide the status of a health plan covering the individual, along with details regarding patient liability for deductible, co-pay and co-insurance amounts for a defined base set of generic benefits or services. The base set of benefits includes, but is not limited to, coverage status and patient liability for medical, chiropractic, dental, hospital inpatient, hospital outpatient, emergency, physician office visit, pharmacy and vision services that are included in the patient's generic health plan benefit
HITSP/T68 - Patient Health Plan Authorization Request and Response	The Patient Health Plan Authorization Request and Response Transaction provides a mechanism for a healthcare provider (other than a retail pharmacy) to request approval from a health plan to authorize certain healthcare services, when required by the patient's health plan contract. The information exchanged includes, but is not limited to, approval status for coverage, allowed service provider(s), and certification dates for services that are included in the patient's health plan benefits. The response from the health plan indicates that the health plan has determined that the particular service(s) will or will not be covered, and what is the level of coverage if that information is available from the health plan
HITSP/T73 - Aggregate Device Information Communication (planned June 2009 as per Section 4.3.1)	The Aggregate Device Information Communication Transaction allows a system serving as a device intermediary such as a home hub, a cell phone, a set top box, or a monitoring station to which one or more monitoring devices are connected to forward a set of observations through a local or remote connection to a remote monitoring management system where these device captured observations will be reviewed by a person managing the care of the patient under remote monitoring
HITSP/T79 - Pharmacy to Health Plan Authorization Request and Response Transaction	The Pharmacy to Health Plan Authorization Request and Response Transaction provides a mechanism for a pharmacy to request approval from a health plan to authorize certain healthcare products and services, as required by the patient's health plan contract. The health plan responds to the pharmacy's request for the approval of products and/or services. The information exchanged includes, but is not limited to, approval status for coverage of the products and/or services that are included in the patient's health plan benefits and/or authorization limitations
HITSP/T85 - Administrative Transport to Health Plan	The Administrative Transport to Health Plan Transaction will be used as the transport for administrative transactions between a provider and a health plan. Examples include a pharmacy obtaining health plan eligibility, and a physician requesting referral or authorization information from a health plan. This construct is based on the CAQH Phase II CORE #270 Connectivity Rule v2.0.0, which addresses the message envelope metadata, the message envelope standards, and the submitter authentication standards for administrative transactions, as well as communications-level errors, and acknowledgements
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



Construct	Description
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/TP46 - Medication Formulary and Benefits Information	The Medication Formulary and Benefits Information Transaction Package addresses two tasks. The first task is to perform an eligibility check for a specific patient's pharmacy benefits. The second task is to obtain the medication formulary and benefit information

Where HITSP has adopted HL7 V3.0 CDA/CCD for conveying information between Electronic Health Record (EHR) and Personal Health Record (PHR) applications and in other healthcare scenarios, it has consolidated common constraints applied against the Content Modules in HITSP/C83 CDA Content Modules. Likewise, HITSP/C80 Clinical Document and Message Terminology maintains commonly applied terminology constraints. Readers should refer to HITSP/TN901 Technical Note for Clinical Documents to better understand how HITSP/C83 and HITSP/C80 are used by other constructs that are based upon HL7 V3.0 CDA/CCD (e.g., HITSP/C32 Summary Documents Using HL7 Continuity of Care Document (CCD), HITSP/C48 Encounter Document Using IHE Medical Summary (XDS-MS) and HITSP/C84 Consult and History & Physical Note Document).

1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2008 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.

1.4 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0.

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 1.3.1-1 Reference Documents

Reference Document	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.
Remote Monitoring, March 21, 2008 Use Case	AHIC Use Case that is the basis of this HITSP Interoperability Specification
TN900 - Security and Privacy Technical Note	<p>Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following:</p> <ul style="list-style-type: none"> • The scope, reference policy background, and Security and Privacy principles used in the development of the constructs • A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs • A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases • A list of identified gaps and the recommended approaches to resolving those gaps • A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications • A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management • A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment <p>HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.</p>
TN901 - Technical Note for Clinical Documents	<p>Developed as a reference document to provide the overall context for use of the HITSP Care Management and Health Record constructs. It includes the following:</p> <ul style="list-style-type: none"> • The scope, background, and principles for use in the development of the CMHR constructs • A detailed description and schematics of the relationship between CMHR constructs • A conceptual framework for the construction of clinical documents • An overview of Clinical Document concepts • An overview of Vocabulary concepts



2.0 INTEROPERABILITY REQUIREMENTS

This section provides a high level description of the Remote Monitoring Use Case, as well as the specific information exchange and data requirements that are extracted from the Use Case. It includes the following information:

- Mapping from the Use Case actions and events, to the derived information exchange and data requirements – this table lists the requirements grouped by actor for each event and related action
- Data requirements – this table further describes the data requirements for each specified information exchange requirement
- Information exchange requirements – this table further describes the information exchange requirements for each applicable Use Case action
- Business Actors – this table defines the business actors that are included for the Interoperability Specification, and maps them to the applicable scenario, information exchange, and data requirements
- High Level Diagrams – these diagrams are used to describe the interaction between the business actors, and the data involved in each scenario that is documented

2.1 USE CASE SYNOPSIS

This section provides a synopsis of the Remote Monitoring Use Case, including any applicable scenarios that are part of the Use Case.

The Remote Monitoring Use Case addresses access to remote monitoring information within an Electronic Health Record (EHR) or a patient's Personal Health Record (PHR). The ability for a clinician to monitor patient information captured remotely in an ambulatory setting, such as physiological, diagnostic, medication tracking, and activities of daily living (ADL) measurements, will be a key enabler for the management of chronic health problems and initial management of new conditions. Remote monitoring will also be a component of maintaining wellness for the aging population. Measurement devices designed for use by the patient or a patient caregiver can communicate measurements to a clinician's ambulatory EHR and/or the patient's PHR.

The Use Case focuses on the communication of interoperable ambulatory remote monitoring information to the EHR and the PHR, and not on the communication and process by which data are captured and transmitted from the device itself. In specific terms:

- Patients and family caregivers benefit from the ability for the patient to gather and communicate remote monitoring information electronically from measurement devices in a home or other non-clinical setting to a clinician's ambulatory EHR system and/or to the patient's PHR. Remote monitoring could include, but is not limited to, communication of: physiologic measurements (e.g., weight, blood pressure, heart rate and rhythm, pulse oximetry, glucose), diagnostic measurements



(e.g., transthoracic impedance) medication tracking device information (e.g., medication pumps, infusion devices, electronic pillboxes), and activities of daily living measurements (e.g., ADL biosensors, pedometers, sleep actigraphy)

- Clinicians, care managers, and disease management programs can benefit by being able to better manage patients from the ability to receive patient remote monitoring information within an EHR

One of the goals of the AHIC is the establishment of a pathway, based on common data standards, to facilitate the incorporation of interoperable, clinically useful remote monitoring information into EHRs and PHRs to support clinical decision-making and management of patients with chronic conditions. This Use Case addresses areas for many stakeholders who are active in the development and implementation of EHRs, PHRs, and other remote monitoring tools including those engaged in activities related to standards, interoperability, harmonization, architecture, policy development, and certification.

Patients may utilize remote monitoring devices in their home, office, school, or other non-clinical setting using devices that are recommended by a clinician or obtained by patients themselves for self-management of chronic conditions. The remote monitoring information is transmitted to clinicians and care managers to assist them in monitoring and managing their patients. The information captured by remote monitoring devices can also be communicated to PHRs for access by patients or family caregivers. In order for remote monitoring data to be captured from a patient's device and made available within a PHR or EHR, remote monitoring information needs to be available in an interoperable manner.

There are a variety of mechanisms by which the remote monitoring information can be communicated to EHRs or PHRs. A common mechanism is via information exchange capabilities provided by a device data intermediary. The device data intermediary serves as the direct interface to extract and store remote monitoring information from the device. A second information exchange between the device intermediary and a remote monitoring management resource provides a mechanism for clinicians and care coordinators (such as case managers, clinician office support personnel, clinical call centers, etc.) to access and review remote monitoring information and determine the information to be communicated to the clinician's EHR. Additional information exchanges may also provide a mechanism for clinicians, care coordinators, patients, and family caregivers to access data from many individual devices and transmit them to different EHRs and PHRs. Remote monitoring information may also be communicated to an EHR or PHR via a Health Information Exchange (HIE) resource or health record bank. Lastly, a remote monitoring device may connect directly to an EHR or PHR via a direct point-to-point device interface, although this method is less prevalent in the market today. The Remote Monitoring Use Case focuses on information needs to communicate information to the EHR or PHR specifically, not the communication from the device itself to an information intermediary.

Remote monitoring information can support needs for care coordinators or other clinical support personnel who monitor trends in data. Care coordination includes a variety of tasks. Some care coordination may be clinical in nature and support the clinician. Other care coordination may be more patient-oriented and provided by caregivers, call centers, and health plan case managers. Remote monitoring information needs can vary from detailed measurements to summarized or selected data.



“Care Coordinators” serve roles to support clinicians and are likely to need access to detailed measurements. Clinician preferences may range from comprehensive raw data to summarized datasets, which may be inclusive of comments and interpretations provided by the care coordinator. Clinicians may also serve as the care coordinator and perform the functions described in this Use Case in both the clinician and care coordinator perspectives.

This Use Case assumes the presence of electronic systems such as EHRs, PHRs, information intermediaries, and other local or web-based solutions supporting patients and clinicians, while recognizing the issues and obstacles associated with these assumptions.

2.2 USE CASE REQUIREMENTS

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

The requirements of the Use Case are described in a single scenario entitled Communication of Remote Monitoring Information to EHR or PHR.

In this scenario, the patient or caregiver prepares the device for use and communication. This may involve registering the device with the manufacturer and/or setting up the communications capabilities of the device. The patient or caregiver uses the remote monitoring device to gather patient measurements. Measurements could be communicated each time the device gathers the data or the accumulated measurements could be communicated periodically (e.g., hourly, daily). Measurements could be communicated to an information exchange, such as a device intermediary, or directly to the patient’s PHR or clinician’s EHR. The mechanisms to obtain device connectivity and transmit data from the device itself can vary greatly based upon clinical goals and objectives, device types, communication protocols, and manufacturer design. Therefore, direct device connectivity between the information intermediary and the device is not a focus of this Use Case.

With appropriate safeguards for patient security and privacy, a care coordinator may review the measurement information received via a portal provided by an information intermediary, such as a device data intermediary provided by the device manufacturer or a third party, or within an EHR. Care coordinators may interact directly with the patient or caregivers to verify the information received and gather additional information about the patient’s situation.

If a clinician review, analysis, or intervention is needed, remote monitoring information and relevant additional information about the patient’s situation is communicated to the clinician’s EHR. The clinician reviews the remote monitoring information received and determines if a patient evaluation or change in treatment plan is necessary. Upon completion of the patient evaluation and modified treatment plan, the appropriate information may be communicated to the care coordinator and the patient’s PHR.



2.2.1 MAPPING OF USE CASE ACTIONS TO INFORMATION EXCHANGE REQUIREMENTS

Section 6.2 contains the perspectives, scenarios, and events from the Use Case. This section maps these events and actions to extracted Information Exchange Requirements (IER), and Data Requirements (DR) that are described in Section 2.2.2. An Information Exchange Requirements (IER) describes a requirement for information exchange between HITSP Business Actors. Data Requirements (DR) define requirements for part, or all, of the data exchanged by one or more IERs. The DR's are defined as a set of information attributes with specific details for each attribute. IER's and DR's form the basis for the construct requirements of the Interoperability Specification that are described in Section 3.0.

2.2.2 DATA AND INFORMATION EXCHANGE REQUIREMENTS

This section contains an extraction of data and information requirements (Table 2.2.2-1) and information exchange requirements (Table 2.2.2-2).

Table 2.2.2-1 provides the data requirement numbers, requirement descriptions, and a listing of the actual data elements and information that meet the data requirements. These requirements are referenced from the Data Requirements column of the Use Case Mapping Table 6.2-1 provided in Section 6.2.

Table 2.2.2-1 Data Element and Information Requirements

Data Requirement Number (DR)	Description	
DR06	Health Plan Eligibility Information	Including (but not limited to): <ul style="list-style-type: none">• Health Plan related patient demographics (First name, last name, date of birth, health plan member ID)• Co-pay• Deductibles• Limits, and exclusions• Procedure or services coded values• Effective date of health insurance coverage actually in operation and in force
DR30	Identification/Remote Monitoring Registration Data	Data is provided, including (but not limited to) <ul style="list-style-type: none">• Patient ID• Provider ID• Device ID (Device Type, Brand, Serial Number)• Other Identifying Information – Case Manager• Other Identifying Information – Device Intermediary Manufacturer• Data Recipient(s) ID Note: all device and device intermediary components in the data transfer need to be identified in the message set
DR35	Free Text Notes (e.g., patient-entered or patient-authorized care-giver-entered measurement instance specific details)	Data elements/attributes needed: <ul style="list-style-type: none">• Free text,• Language,• Max length Note: There may be constraints that need to be considered with different base specifications, e.g. CDA, V2 Message, V3 XML Message



Data Requirement Number (DR)	Description	
DR36	Care Coordination Notes	<p>Data elements/attributes needed:</p> <ul style="list-style-type: none"> • Clinical Document (e.g., Care Coordinator Reason for Referral/Summary, Care Management Program Notification, Care Manager to Clinician Summary) • Free Text Notes section must also be available in addition to device data and formal clinical documents • There may be Clinical and Non-clinical notes • Clinical notes would likely require additional support for persistence and nonrepudiation.
DR37	Alerts, Alarms and Notices	<p>Data elements/attributes needed:</p> <ul style="list-style-type: none"> • Normal Range, • Normal Range for Patient, • Alert (Low Value, High Value, Change in Trend); • including evidentiary numeric, waveform and annotation data to validate alarm
DR38	Health plan authorization	<p>Including (but not limited to):</p> <ul style="list-style-type: none"> • Healthcare Provider – to provide the service • Procedure or service or medication coded values • Authorization scope, such as timing, quantity, limits, effective dates • Diagnosis • Health Plan related patient demographics • Authorization/certification number – not always required for pharmacy transactions
DR39	Remote Monitoring Services Order	Remote Monitoring Services Order information
DR40	Structured Treatment Plan	Structured Treatment Plan information
DR74	Access control lists	<p>Including (but not limited to):</p> <ul style="list-style-type: none"> • Identification of entity being authorized • Identification of entity granting authorization/test results, etc. • Type of authorization (read/no-read, write/no-write, etc) • Criteria defining the application of the authorization (e.g., document type, procedure)
DR80	Physiological measurement data - Blood Glucose Meter [see IEEE P11073-10417™ Dev specialization – Glucose meter or similar]	<p>Physiological measurement data – blood glucose meter, including (but not limited to) [see IEEE P11073-10417™ Dev specialization – Glucose meter or similar]</p> <ul style="list-style-type: none"> • Glucose Level • Blood Glucose Level • Glucose Control Measurement • Interstitial Fluid Glucose Level • Sample Location • Measurement Condition • Tester • Meter event



Data Requirement Number (DR)	Description	
DR81	Physiological measurement data - Blood Pressure Monitor [see IEEE P11073-10407™ Dev specialization – Blood pressure monitor or similar]	Physiological measurement data - blood pressure monitor, including (but not limited to): <ul style="list-style-type: none"> • Systolic Pressure • Diastolic Pressure • Mean Aerial Pressure • Pulse
DR82	Physiological measurement data - Brain Activity	Physiological measurement data – brain activity, including (but not limited to): <ul style="list-style-type: none"> • Ambulatory EEG
DR83	Physiological measurement data - Cholesterol	Physiological measurement data - cholesterol, including (but not limited to): <ul style="list-style-type: none"> • <Not yet defined – to be determined>
DR84	Physiological measurement data - Esophageal pH	Physiological measurement data – esophageal pH, including (but not limited to): <ul style="list-style-type: none"> • <Not yet defined – to be determined>
DR85	Physiological measurement data - Heart Rate	Physiological measurement data – heart rate, including (but not limited to): <ul style="list-style-type: none"> • <Not yet defined – to be determined>
DR86	Physiological measurement data - Heart Rhythm	Physiological measurement data – hearth rhythm, including (but not limited to): <ul style="list-style-type: none"> • AECG • Holter Monitor • Cardiac Implants
DR87	Physiological measurement data - Implantable Cardioverter Defibrillator (ICD) Monitoring	Physiological measurement data – Implantable Cardioverter Defibrillator (ICD), including (but not limited to): <ul style="list-style-type: none"> • Monitoring Intercardiac Pressure • Intrathoracic Fluid • EGM Waveforms
DR88	Physiological measurement data - Lung Function	Physiological measurement data – lung function, including (but not limited to): <ul style="list-style-type: none"> • FEV1 • FVC • PEV



Data Requirement Number (DR)	Description	
DR89	Physiological measurement data - Oxygen Saturation (Pulse Oximeter) [see IEEE P11073-10404™ Dev specialization – Pulse oximeter]	Physiological measurement data – oxygen saturation (pulse oximeter), including (but not limited to): <ul style="list-style-type: none"> • SpO2 • SpO2 fast response • SpO2 slow response • SpO2 spot check • Pulse Rate • Pulse amplitude • Plethysmographic waveform • Pulse events • Physiological threshold conditions • Device and sensor annunciation conditions
DR90	Physiological measurement data - Respiration Rhythm	Physiological measurement data – respiration rhythm, including (but not limited to): <ul style="list-style-type: none"> • <Not yet defined – to be determined>
DR91	Physiological measurement data - Temperature (Thermometer) [see IEEE P11073-10408™ Dev specialization – Thermometer]	Physiological measurement data - temperature, including (but not limited to): <ul style="list-style-type: none"> • Temperature
DR92	Physiological measurement data - Weight (Weighing Scale) [see IEEE P11073-10415™ Dev specialization – Weighing scale]	Physiological measurement data - weight, including (but not limited to): <ul style="list-style-type: none"> • Body Weight • Body Height • Body Mass Index
DR93	Measurement Management and Administration data – Electronic Pillbox	Medication Administration Tracking Measurement management and administration data – electronic pillbox patient alerts, including (but not limited to): <ul style="list-style-type: none"> • Patient Alerts and Medication Administration Tracking
DR94	Measurement Management and Administration data – Medication Pumps	Measurement management and administration data – medication pumps, including (but not limited to): <ul style="list-style-type: none"> • Medication Administration
DR95	Measurement Management and Administration data – Medication Infusion Devices	Measurement management and administration data – medication infusion devices, including (but not limited to): <ul style="list-style-type: none"> • Medication Administration
DR96	Patient Sensor Monitoring Data	Data elements/attributes needed: <ul style="list-style-type: none"> • Activities of Daily Living Biosensors and Detection Devices • Emergency Alerting [with Global Positioning System (GPS)] • Fall Detection • Pedometer (Steps Moved) • Sleep Actigraphy



Data Requirement Number (DR)	Description	
DR97	Device and measurement descriptive data – Generic Device Data [See IEEE P11073-20601™ Optimized exchange protocol]	Device and measurement descriptive data – generic device, including (but not limited to): [See IEEE P11073-20601™ Optimized exchange protocol] <ul style="list-style-type: none"> • Manufacturer • Device ID • Serial # • Type • Model # • FW Version # • HW Version # • Time Accuracy • Measurement • Accuracy • Regulatory Info
DR98	Device and measurement descriptive data – Measurement Descriptive Data	Device and measurement descriptive data – measurement descriptive, including (but not limited to): <ul style="list-style-type: none"> • Device Setting Information • Date/Time of Measurement • Data Source (Device or Patient entered) • Measurement Characteristics (raw vs. summary data) • Measurement Scale/Units • Device Calibration/Programming Data
DR99	Device and measurement descriptive data – Measurement Error Data	Device and measurement descriptive data – measurement error, including (but not limited to): <ul style="list-style-type: none"> • Measurement Error Data Device Malfunction • User Error During Measurement • Measurement Cancelled by Patient (Stopped measurement process or marked measurement as invalid)

Table 2.2.2-2 below contains an extraction of the Information Exchange Requirements from the Use Case. Information Exchange Requirements map to the Information Exchange Requirements column in the Use Case Mapping Table 6.2-1 provided in Section 6.2.

Table 2.2.2-2 Information Exchange Requirements (IER)

Information Exchange Requirement Number (IER)	Description
IER01	Provide authorization and consent: Consumers authorize clinicians and other individuals (e.g., family members) to access/view PHR information (a.k.a., proxy access)
IER02	Send data over secured communication channel: A session oriented, synchronous, point-to-point communication channel establishing a secure path through which data can be transmitted



Information Exchange Requirement Number (IER)	Description
IER03	Create audit log entry: The secure message system will log that the message was sent, received or viewed. Provides assurance that security policies are being followed or enforced and that risks are being mitigated
IER04	Synchronize system time: Ensures that all of the entities that are communicating within the network have synchronized system clocks
IER05	Verify Entity Identity: Secure message system authenticates user. Entities are asserted to assure that the entity is the person or application that claims the identity
IER10	Identify patient: Support for identifying, cross referencing, and query of patients
IER14	Send/receive health plan eligibility: Identify and verify eligibility from Health Plan Note: for remote monitoring services and equipment
IER15	Send/receive health plan authorization: Obtain authorization for service from Health Plan Note: for remote monitoring equipment and services
IER18	Send/receive clinical document: Supports the sharing of patient records in the form of source attested objects called documents, using physical media and email to transport clinical document information from a source to a destination, or communicate a clinical document to a recipient through direct communication conveying a set of medical documents in a point-to-point network-based communication. IS77: The options for communication is constrained to use a point-to-point network-based communication solution
IER24	Send/receive structured treatment plan: Communication of a Structured Treatment Plan and Revision Thereof. Treatment plan information communicated between the clinician and the patient Note The communication of structured treatment plans in a standardized format requires further standards development
IER36	Send/receive remote monitoring service order: Note: The communication of remote monitoring services orders in a standardized format requires further standards development
IER38	Query/retrieve document set: The system queries and retrieves a patient's clinical/health data including health records, documents etc. Standardized information (direct reuse of HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) and HITSP/C37 - Lab Report Document, HITSP/C35 - Lab Result Terminology
IER39	Send/receive device observation data: Note that this System Data Exchange has been specified to meet the following requirements: 1) Shall support conventional networks (e.g., POTS, Cable, DSL, GPRS, CDMA). 2) Must support "always on" (e.g., Internet) and "intermittent" connections (e.g., POTS) 3) Shall support conventional Device Intermediaries (e.g., Cell Phone, PC, Set Top Boxes, PDA) 4) Device data values shall not be modified. There needs to be a sufficient data integrity (i.e., must not be altered or destroyed either by attack or accident while in transmission) 5) A tamper-resistant audit log file should record security-relevant actions 6) A mechanism must be provided to synchronize clocks with the Remote Monitoring Mgmt System 7) Sufficient Security/Privacy based on a reasonable level of risk 8) Transport sessions must be initiated from within the home or from the patient-side device 9) Message size should be reasonable (but not minimized more than lossless compression) due to bandwidth limitation and/or transmission cost
IER61	Provide and register document set: A global unique document ID must be included. Must be able to update a previously submitted record. A unique patient ID must be associated with the summary data



2.2.3 IDENTIFICATION OF BUSINESS ACTORS, AND SCENARIOS

This section describes the Business Actors that impact information exchange requirements for each scenario. A Business Actor is an abstraction that is instantiated as an IT system application that a Stakeholder uses in the exchange of data needed to complete Use Case action(s); a Business Actor is not a Stakeholder. A HITSP Stakeholder is a person, organization or “personified system” that performs actions in a Use Case. Only Business Actors as an IT system are directly engaged and benefit from the real world information exchange defined within a business Use Case action. Only Business Actors are associated with Technical Actors, which support the data exchanges of the Business Actors (see Section 3.2 for Technical Actors). The table below identifies the significant Use Case Business Actors, their descriptions, the Stakeholders they support, the Use Case scenarios, and the information exchange or data requirements for which they are used. Refer to the Use Case for a more detailed description of the listed stakeholders.

Table 2.2.3-1 Business Actors

Business Actor	Description	Supported Stakeholders	Use Case Scenario	Information Exchange Requirement Numbers (IER)	Data Requirement Numbers (DR)
Device Intermediary	A system that enables one or more measurement devices (devices that provide measurements from a patient under remote monitoring) to feed, in a secure manner, captured measurements to a care management system	Patient	1	IER39	DR30 , DR80 , DR81, DR82, DR83, DR84, DR85, DR86, DR87, DR88, DR89, DR90, DR91, DR92, DR93, DR94, DR95, DR96, DR97, DR98, DR99, DR35 , DR37
Remote Monitoring Management System	A system that supports health professionals supporting the patient under remote monitoring and analyzes the captured measurements over the period of planned remote monitoring. The care coordinator works with this tool to fulfill care oversight	Care Coordinator	1	IER61 , IER38 , IER10 , IER2 , IER3 , IER5 , IER39 , IER15 , IER14 , IER18	DR30 , DR80 , DR81, DR82, DR83, DR84, DR85, DR86, DR87, DR88, DR89, DR90, DR91, DR92, DR93, DR94, DR95, DR96, DR97, DR98, DR99, DR35 , DR36 , DR37
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	Clinician	1	IER61 , IER38 , IER10 , IER18 , IER2 , IER3 , IER5	DR06 , DR30 , DR80 , DR81, DR82, DR83, DR84, DR85, DR86, DR87, DR88, DR89, DR90, DR91, DR92, DR93, DR94, DR95, DR96, DR97, DR98, DR99, DR35 , DR36 , DR37 , DR38



Business Actor	Description	Supported Stakeholders	Use Case Scenario	Information Exchange Requirement Numbers (IER)	Data Requirement Numbers (DR)
Personal Health Record (PHR) System	A healthcare record system used to create, review, annotate and maintain records by the patient or the caregiver for a patient. The PHR may include any aspect(s) of the health condition, medications, medical problems, allergies, vaccination history, visit history or communications with healthcare providers	Patient	1	IER61 , IER38 , IER10 , IER2 , IER3 , IER5	DR30 , DR80 , DR81, DR82, DR83, DR84, DR85, DR86, DR87, DR88, DR89, DR90, DR91, DR92, DR93, DR94, DR95, DR96, DR97, DR98, DR99, DR35 , DR36 , DR37
Infrastructure Service	Infrastructure Service is a multi-stakeholder system that enables the exchange and use of health information, in a secure manner, for the purpose of promoting the improvement of health quality, safety and efficiency	Health Information Exchange	1	IER61 , IER38 , IER10 , IER2 , IER3 , IER5	DR30 , DR80 , DR81, DR82, DR83, DR84, DR85, DR86, DR87, DR88, DR89, DR90, DR91, DR92, DR93, DR94, DR95, DR96, DR97, DR98, DR99, DR35 , DR36 , DR37
Provider Administrative and Financial System	Systems used by healthcare provider that include administrative and financial functions associated with the delivery of healthcare. These functions support the delivery and optimization of care, but generally do not impact the direct care of an individual patient	Clinician	1	IER15 , IER14	DR06 , DR38



Business Actor	Description	Supported Stakeholders	Use Case Scenario	Information Exchange Requirement Numbers (IER)	Data Requirement Numbers (DR)
Health Plan System	Systems used by health plans that include administrative and financial functions associated with the coverage and financing of healthcare for the health plan's enrolled members. These functions include information regarding the individual's enrollment, eligibility, coverage and benefits, authorizations, claims, care coordination and other information related to the member	Health Plan	1	IER15, IER14	DR06, DR38

2.2.4 HIGH-LEVEL BUSINESS SEQUENCE DIAGRAM

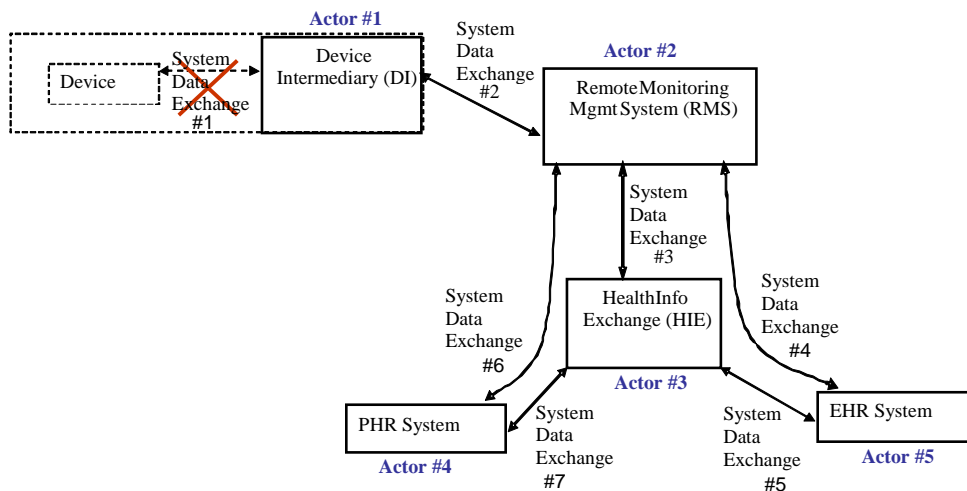
This section contains an explanation of the relationship between the business actors and data interactions between the primary actors and alternative actors for each Use Case scenario. The Unified Modeling Language (UML) diagrams that follow illustrate each scenario with a representation of a normal sequence of exchange between the primary actors. The interactions are to be supported by the various constructs which will be introduced in Section 3.0 of this Interoperability Specification. The event codes from the AHIC Use Case are annotated on the diagrams to show how the interactions relate to the Use Case.

Section 6.3 provides High Level Sequence Diagrams to illustrate each scenario with a representation of a normal sequence of exchange between the primary actors

Figure 2.2.4-1 below identifies the Business Actors that support this Use Case and illustrates the major interactions between these business actors. This figure is a simplified diagram that will be expanded in a High Level UML diagram.



Figure 2.2.4-1 Business System Interfaces



Alternate Business Actor Combinations

- PHR integrated into the RMS (Combine Actors #2 & #4; Eliminate SDE #6)
- EHR integrated into the RMS (Combine Actors #2 & #5; Eliminate SDE #4)
- PHR integrated into the HIE (Combine Actors #3 & #4; Eliminate SDE #6 & #7)

Special Note Regarding a Media based Data Exchange: Although not explicitly denoted in the Use Case, a low end solution deploying a physical media to transfer the remote monitoring data from the patient device intermediary system to the EHR / patient PHR is also possible and should be considered as an extension of the RMON Use Case. For this implementation variant, the above SDE #2 through #5 would be replaced by a single media-based interchange between the business actors of the Device Intermediary and the EHR System (SDE #8) and/or the PHR system (SDE #9)

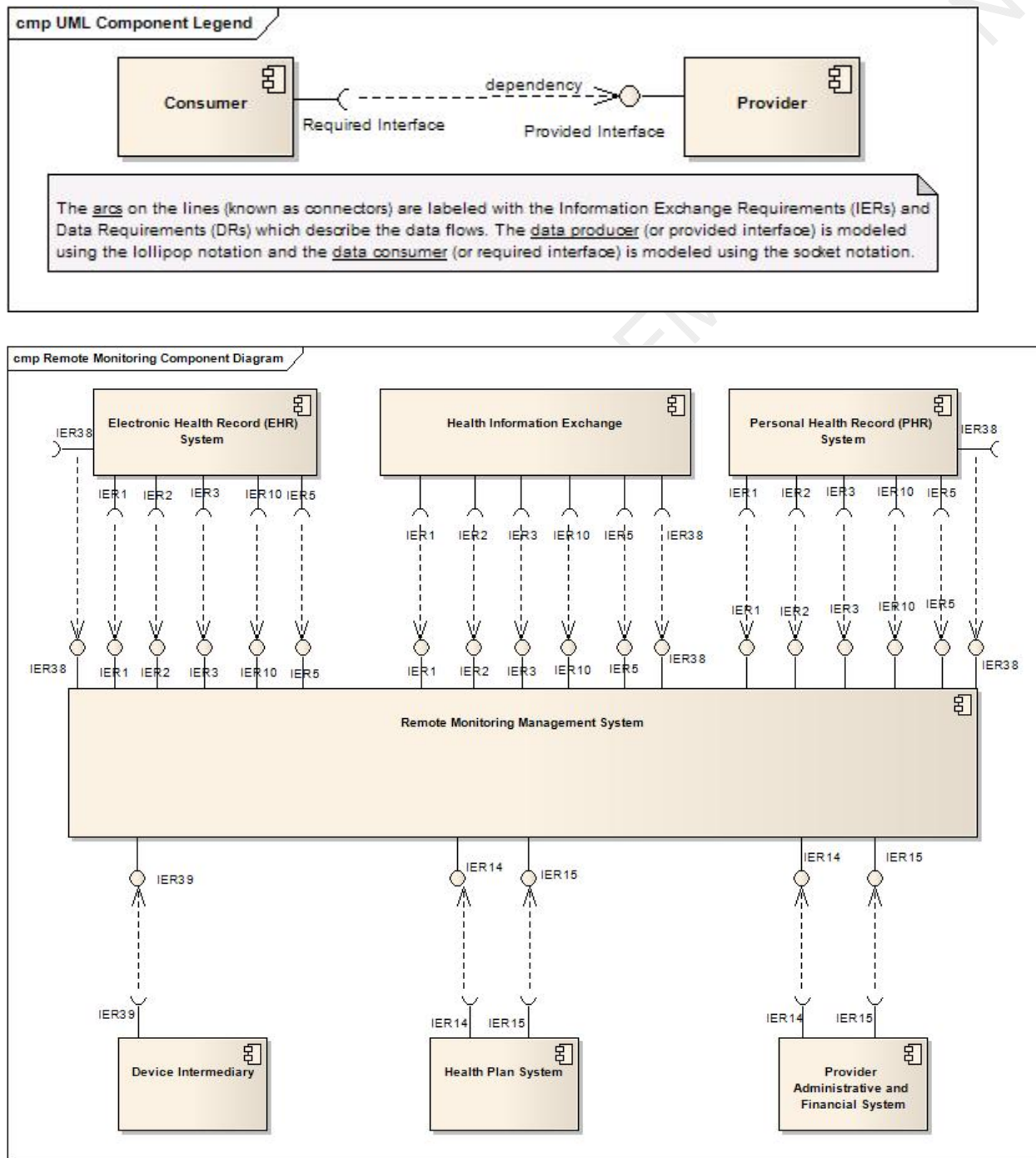
Legend:

- System Data Exchange #1 is placed out of scope in this specification on the basis of the remote monitoring requirements of the Use Case. The Device Intermediary Business Actor is therefore assumed to include the device
- System Data Exchanges #3, #4, and #6 are expected to be identical. System Data Exchanges #5 and #7 are expected to be identical. These two sets may however require different metadata or behavior for the interchange. They are identified to be within scope of the Use Case



Figure 2.2.4-2 is a Component Data Flow diagram that illustrates the data flow and information exchanges between the primary actors. The information exchange and data requirement numbers from tables in Section 2.2.2 are annotated on the diagrams to show how the requirements relate to the primary actors. The in-scope requirements are supported by constructs which will be introduced in Section 3.0 of this Interoperability Specification.

Figure 2.2.4-2 Remote Monitoring Component Data Flow Diagram



3.0 DESIGN

The design for the Interoperability Specification is the result of the requirements analysis and iterative standards selection process. This section describes the design based on the specified Business Actors and their Information Exchange and Data Requirements. It provides a detailed mapping of the specified requirements to HITSP constructs and their Technical Actors, groupings of specific Technical Actors which support Business Actors are specified to further describe the relevant interactions from existing or new HITSP constructs required for interoperability.

3.1 SCOPE OF DESIGN

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

Table 3.1-1 provides explanations as to why specific Use Case requirements are considered out-of-scope or not being addressed in this document production cycle including a recommended resolution as to how and when these requirements are to be addressed in the future.

Table 3.1-1 Scoping Clarifications

Scope Item	Event	Scoping Action	Recommended Resolution
#1	7.1.1 Evaluate patient and order remote monitoring 7.1.3 Receive remote monitoring summary 7.2.1 Initiate remote monitoring and coordinate with patient	<p>Based on initial due diligence regarding frequency of a given remote monitoring device being deployed and for what medical conditions (informed in part by the work done by the Continua initiative), it has been determined to scope this cycle's work for remote monitoring for the following conditions: Diabetes, Obesity, COPD, CHF and Hypertension.</p> <p>The specific devices typically deployed for remote monitoring for these medical conditions which are proposed as required for 2008 include:</p> <ul style="list-style-type: none">• Blood Pressure Monitor• Weighing Scale• Glucose Meter• Thermometer• Pulse Oximeter <p>This reduces the content of Data Requirements Table 2.2.2-1 for this cycle to the following subset:</p> <p>DR31 Identification/Remote Monitoring Registration Data</p> <p>DR80 Blood Glucose Meter [see IEEE P11073-10417™ Dev specialization – Glucose meter]</p> <p>DR81 Blood Pressure Monitor</p> <p>[see IEEE P11073-10407™ Dev specialization – Blood</p>	None required. This is a clarifying statement highlighting that a specific subset of the device requirements described in the RMON Use Case are to be addressed in the 2008 release of HITSP/IS77. Additional device requirements are to be addressed in 2009 in accordance with the CPTC Roadmap noted in Table 4.2.2-2



Scope Item	Event	Scoping Action	Recommended Resolution
		<p>pressure monitor]</p> <p>DR89 Oxygen Saturation (Pulse Oximeter) [see IEEE P11073-10404™ Dev specialization – Pulse oximeter]</p> <p>DR91 Temperature (Thermometer) [see IEEE P11073-10408™ Dev specialization – Thermometer]</p> <p>DR92 Weight (Weighing Scale) [see IEEE P11073-10415™ Dev specialization – Weighing scale]</p> <p>DR97 Generic Device Data [see IEEE P11073-20601™ Optimized exchange protocol]</p> <p>DR35 Free Text Notes (e.g., Patient-entered Measurement Instance Specific Details)</p> <p>DR36 Care Coordination Notes</p> <p>In addition, there are two distinct levels of timeliness of the data transfer. Namely,</p> <ol style="list-style-type: none"> 1. store and forward processing 2. real-time streaming data <p>For the 2008 cycle, it is recommended that only specific remote monitoring measurements using the store and forward data exchange level are addressed.</p> <ul style="list-style-type: none"> • As identified in the Description column of table 2.2.1-1, this data interchange must support store and forward transfer of the data content of all types of data content 	
#2	<p>7.1.1 Evaluate patient and order remote monitoring</p> <p>7.1.3 Receive remote monitoring summary</p> <p>7.2.1 Initiate remote monitoring and coordinate with patient</p>	<p>The corollary of scoping statement #1 is that the following Data Requirements Table 2.2.2-1 entries are excluded from consideration for the 2008 cycle:</p> <p>DR82 through DR88, and DR90, DR93, DR94, DR95, DR96, and DR99</p> <p>At this point, it is recommended that for this cycle, real-time streaming data exchange is not included but will retained as part of the requirements in future cycles</p>	<p>Based on the ongoing standards development work underway in the industry in regards to Remote Monitoring, the projected set of devices and their related measurements/information to be addressed by the CPTC is depicted in the Roadmap Matrix shown in Table 4.2.2-2. Data and device requirements included in this Use Case which are not addressed in 2009 will remain on the CPTC roadmap for attention in subsequent years</p>
#3	7.1.1.3a	<p>Patient enrollment is unclear. Need to better understand the enrollment process and what entity does the remote monitoring/disease mgmt program have? More than just the patient inquiry will be needed; it needs to be determined exactly what construct to use to send patient enrollment information?</p>	<p>Reach out to the appropriate SDO or standards development groups regarding activities for this interface requirement and add this to the CPTC roadmap accordingly</p>
#4	7.1.1 Evaluate patient and order remote monitoring	<p>Action 7.1.1.3 [Identified as IER36] The process for electronic ordering of remote monitoring may require standards and procedure designations that are not currently available and are therefore recommended to not be included in 2008 version of</p>	<p>Reach out to the appropriate SDO or standards development groups regarding activities for this interface requirement and</p>



Scope Item	Event	Scoping Action	Recommended Resolution
		the IS	add this to the CPTC roadmap accordingly
#5	7.1.5 Modify treatment plan and communicate with patient	Action 7.1.5.2 [Identified as IER24] The communication of structured treatment plans in a standardized format requires further standards development. The requirements in this regard are likely to be included in the Consultation and Transfer of Care Use Case	Review the requirements related to Treatment Plans and their administration in the Consultation and Transfer of Care Use Case with the Provider PTC. Ensure the Remote Monitoring activity is appropriately reflected in the options of treatment plan oversight and data collection
#6	7.3.4 Receive remote monitoring data	The Remote Monitoring Management System to PHR interactions (System Data Exchange #6 in Figure 2.2.4-1) may require standards that are not currently available and therefore are recommended to not be included in 2008 version of this IS	Reach out to the appropriate SDO or standards development groups regarding activities for this interface and add this to the CPTC roadmap accordingly
#7	7.3.5.1 Patient self-manages chronic disease or wellness care based upon measurement values 7.3.5.2 The patient may be contacted by a coordinator to review or modify care management activities 7.3.6.1 Patient discusses treatment or management with their clinician 7.3.6.3 Patient implements modified treatment plan and continues remote monitoring participation as directed	These actions are considered to be out of scope due to the absence of electronic data interchange. Out-of-band communication is expected to accomplish these actions but electronic communications are not yet defined	Reach out to the appropriate SDO or standards development groups regarding activities for this "patient self-managing" variant and add this to the CPTC roadmap accordingly

3.1.1 ASSUMPTIONS

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

Table 3.1.1-1 Assumptions

Assumption	Use Case Scenario
It is assumed that there is a developing presence of electronic systems such as EHRs, PHRs, information intermediaries, and other local or web-based solutions supporting patients and clinicians, while recognizing the issues and obstacles associated with these assumptions	1



Assumption	Use Case Scenario
It is assumed that the data to be interchanged between the Remote Monitoring Management System (RMMS) and the PHR System is the same content and format as that being exchanged with the EHR System. As such, only one HITSP component is being identified at this time for both of these data exchanges, namely, the Remote Monitoring Observation Document	1

3.1.2 CONSTRAINTS

This section describes the constraints that limit the context in which the Interoperability Specification may be used. A constraint describes a rule that limits the use of the actors, actions or data within the given context, or to which the interactions must conform to be used within the described context. It is a description of the limits and scope of the interactions and can describe actions or events that are not part of the initial definition for the context.

Table 3.1.2-1 Constraints

Constraint	Use Case Scenario
No applicable constraints	

3.1.3 PRE-CONDITIONS

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

Table 3.1.3-1 Pre-conditions

Pre-condition	Use Case Scenario
Support the technical measures to ensure security and privacy of consumer/patient health information	1
Authentication service to authenticate requestors and/or data submissions from various locations	1
Security and privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient security and privacy	1
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	1
Support the following HITSP Security and Privacy constructs: HITSP/C19 Entity Identity Assertion HITSP/T16 Consistent Time HITSP/T17 Secure Communication Channel HITSP/T15 Collect and Communicate Security Audit Trail HITSP/TP30 Manage Consent Directive HITSP/TP20 Access Control	1
All pre-conditions from the lower level constructs are incorporated	1



Pre-condition	Use Case Scenario
When needed, the patient is uniquely registered with the Patient Identity Cross-Referencing service. The patient ID must be unique for all interface transactions but can be cross-referenced to another patient ID used internally by one of the business actor systems. A local id that is unique for the transactional moment is sufficient	1
Patient Identities (name, demographics etc.) are known and are consistent with policies. In this regard, it is expected that the Health Plan's Patient Id is known and related to the Provider's Finance & Admin System patient accordingly	1
Patient enrollment is expected to be completed prior to the remote monitoring service commencing. [Note: A better understanding of the enrollment process and what entity does this for the remote monitoring/disease mgmt program is needed before selecting a construct to send patient enrollment information.]	1
All devices and systems involved have been cleared of prior patient data, prior alarms, critical values and other related information, so that the device may be safely used on the current patient	1

3.1.4 POST-CONDITIONS

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

Table 3.1.4-1 Post-conditions

Post-condition	Use Case Scenario
For protecting patient safety, all devices and systems involved have been cleared of prior patient data, prior alarms, critical values and other related information	1

3.1.5 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary to start any scenarios, actions or events. It can be an automatic or manual process or result that in turn starts off another scenario, action or event. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

Table 3.1.5-1 Process Triggers

Process Trigger	Use Case Scenario
The Remote Monitoring Management System needs to "wake up" when it receives information from the Device Intermediary and/or according to a planned /timed event for reporting information to the clinician	1
The Case Manager reviews a monitoring session on the Remote Monitoring Management System and decides to share a remote monitoring summary document for reporting information to the patient's PHR	1
The Case Manager reviews a monitoring session on the Remote Monitoring Management System and decides to share a remote monitoring summary document for reporting information to the health information exchange	1
The patient receives on his or her PHR System a remote monitoring summary document from the Case Manager working on his or her Remote Monitoring Management System	1
The patient decides to check via his or her PHR System if a remote monitoring summary document is available from the Health Information Exchange	1
The clinician decides to check via his or her EHR System if a remote monitoring summary document is available from the Health Information Exchange	1



Process Trigger	Use Case Scenario
After his review, the clinician decides to make available to the patient on his or her PHR System a remote monitoring summary document	1
After his review, the patient decides to make available to his clinician via his or her PHR System a remote monitoring summary document	1

3.2 DETAILED DESIGN

This section provides a detailed description of the technical design, along with an analysis of the main interactions and decisions between all actors, actions and data in support of the specific requirements for each scenario of the Use Case. In addition, this section provides the data element details and an overview of the HITSP constructs used to meet the business and technical requirements for this Use Case. Any variances in the Security and Privacy implementation are also described here.

Note that with respect to Security and Privacy, local implementation policy as determined by risk assessment, including assessment of jurisdictional and regulatory requirements, will determine which assurance level of nonrepudiation of origin is needed. For instance, in document-based transmissions, a low level is offered by the basic use of HITSP/TP13 Manage Sharing of Documents construct. A medium level of assurance is offered by the use of the HITSP/TP13 construct option called “Document Integrity”. A high level of assurance is offered by the use of the HITSP/C26 Nonrepudiation of Origin construct which requires the existence of a Public Key Infrastructure (PKI) (See TN900 for a discussion on the challenges with PKI's).

The interoperability problem that this Use Case solves is the standardized method for a patient to send results (or observations) from a remote monitoring device installed in the patient's home (or somewhere other than the clinician's office), to a clinician providing care to that patient. The transfer of this data may be accomplished either directly to an individual clinician's EHR System, or via the services of a Health Information Exchange (HIE) that is established to facilitate this kind of sharing of clinical information. In addition to the data being transferred and persisted in the target clinician's EHR System, it may also be desirable for the patient to retain this remote monitoring data in their Personal Health Record (PHR) System. In all situations, however, it is expected that the data that is recorded by the remote monitoring device itself will first be sent to a Device Intermediary, and then forwarded to a Remote Monitoring Management System (RMMS) for appropriate processing prior to sending it on for access by the clinician.

Some possible implementation variants with a combination of different functions provided by various HITSP Business Actors were illustrated in the high-level Business System Interfaces diagram (Figure 2.2.4-1). Independent of how the business actors denoted in that diagram may be combined, the roles of their associated technical actors are required in order to accomplish the remote monitoring information exchange.



Besides the technical actors related to the security, privacy and infrastructure underpinnings of this information exchange, the following capabilities are necessary to accomplish the interchange:

1. Transfer data from a remote monitoring device

- a. The Device Observation Reporter (DOR) technical actor of the Device Intermediary receives data from the monitoring device itself (e.g. blood pressure cup) and maps the received data to transactions providing consistent syntax and semantics. The format of the “raw” data received from the various devices themselves is considered out-of-scope for this specification
- b. This data are then forwarded to the Remote Monitoring Management System (RMMS) where the Device Observation Consumer (DOC) technical actor is responsible for collecting and processing the device data in accordance with pre-defined protocols (e.g. aggregation of data for a defined interval, comparison to an acceptable range, etc), before it is further sent onto to the clinician. It is conceivable that there is some level of human interaction by a care coordinator using the RMMS to ready the data for the clinician's use, but this is not a mandatory step and is likely to become less and less a requirement as the RMMS systems increase in their processing functionality
- c. At this point, the data to be transferred to the clinician EHR System is intended to be in a condition that can leverage industry-standard transports deployed for other medical summary and clinical document interchange. A Personal Health Monitoring Content Document focused on the Remote Monitoring Observation data set is used that leverages the HITSP-specified technical actors of Content Source/Consumer as well as Document Source/Consumer for its transport

2. Verify patient eligibility and authorize insurance

- a. In addition to the transactions to accomplish the remote monitoring data exchange as described above, the technical design also reflects the administrative transactions between a healthcare provider and a health plan for verifying the patient's eligibility for remote monitoring services, and, if needed, to request approval from the health plan to authorize remote monitoring services, when required by the patient's health plan contract
- b. These are accomplished respectively by the Provider's Administrative and Financial System fulfilling the requirements of the following two sets of technical actors:
 - i. Eligibility Information Receiver technical actor querying the Eligibility Information Source technical actor for eligibility information
 - ii. Information Receiver for Health Plan Authorization technical actor querying the Information Source for Health Plan Authorization
- c. The administrative-focused Business Actors identified in Section 2.0 serving as the eligibility and authorization resources are the Provider's Administrative and Financial System and the Health Plan System, respectively
- d. When the provider stakeholder is a pharmacy, different HITSP constructs (i.e. HITSP/TP46 Medication Formulary and Benefits Information and HITSP/T79 Pharmacy to Health Plan Authorization Request and Response) are used for the eligibility and the health plan authorization than the ones used for other types of provider stakeholders (i.e.



HITSP/T40 Patient Health Plan Eligibility Verification and HITSP/T68 Patient Health Plan Authorization Request and Response)

3.2.1 TECHNICAL ACTOR ROLE DESCRIPTIONS

This section identifies the Technical Actors used within the Interoperability Specification. Note that a Technical Actor represents an internal software component or IT system, which supports a specific aspect of a real world business information interchange (e.g., set of message exchanges). Technical Actors implement system data exchange transactions, which support real world Business Actor information interchanges (see Section 2.2.3 for Business Actor definitions). The table below identifies the Technical Actors and provides a description of the Technical Actor roles involved in the Interoperability Specification.

Table 3.2.1-1 Technical Actor Role Descriptions

Technical Actor(s)	Actor Role	Construct
Access Control Service (ACS)	The enterprise security service that supports and implements user-side and/or service side access control capabilities. This service would be utilized by the Service User, and/or Service Provider	HITSP/TP20
Administrative Transport Client	A Provider sending a request to a health-plan has a Client role	HITSP/T85
Administrative Transport Server	A Health Plan responding to a request from a Provider has a Server role	HITSP/T85
Audit Record Repository	Provides a repository for audit events	HITSP/T15
Audit Record Source	Creates and communicates an Audit Record to the Audit Record Repository on behalf of another actor that performs an action requiring logging	HITSP/T15
Consent Directive Requestor	Accesses Consent Directives located through a Consent Registry from Consent Repositories	HITSP/TP30
Consent Originator	Captures Consent Directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry	HITSP/TP30
Consent Registry	Responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a Manage Consent Directive Metadata Request	HITSP/TP30
Consent Repository	Responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point	HITSP/TP30
Content Consumer	Responsible for viewing, import, or other processing of content created by a Content Creator Actor	HITSP/C74 HITSP/C80 HITSP/C83 HITSP/TP30
Content Creator	Responsible for the creation of content and transmission to a Content Consumer	HITSP/C74 HITSP/C80 HITSP/C83



Technical Actor(s)	Actor Role	Construct
Device Observation Consumer	The actor responsible for receiving and processing device data from the Device Observation Reporter	HITSP/T73
Device Observation Reporter	Receives device data and maps the received data to transactions providing consistent syntax and semantics	HITSP/T73
Document Consumer	Queries a Document Registry Actor for documents meeting certain criteria and retrieves selected documents from one or more Document Repository actors	HITSP/C19 HITSP/TP13
Document Recipient	Receives a set of documents sent by another actor. Typically this document set will be made available to the intended recipient who will choose to either view it or integrate it into a Health Record	HITSP/C19 HITSP/T31
Document Registry	Maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration	HITSP/C19 HITSP/TP13
Document Repository	Responsible for both the persistent storage of these documents as well as for their registration with the appropriate Document Registry. It assigns a Uniform Resource Identifier (URI) to documents for subsequent retrieval by a Document Consumer	HITSP/TP13
Document Source	Producer and publisher of documents. It is responsible for sending documents to a Document Repository Actor. It also supplies metadata to the Document Repository Actor for subsequent registration of the documents with the Document Registry Actor	HITSP/C19 HITSP/TP13 HITSP/T31
Eligibility Information Receiver	The system that initiates an inquiry to the Eligibility Information Source about an individual's insurance eligibility, coverage and benefits	HITSP/T40 HITSP/TP46
Eligibility Information Source	The system which holds and maintains the information regarding the individual's insurance eligibility, coverage and benefits, and responds to the queries initiated by the Eligibility Information Receiver	HITSP/T40 HITSP/TP46
Identity Provider	Receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider)	HITSP/C19
Information Receiver for Health Plan Authorization	The system that initiates a request to the Information Source for Health Plan Authorization about an individuals health insurance requirements to obtain an authorization approval for purposes of benefit coverage determination in order to refer a patient for healthcare services	HITSP/T68 HITSP/T79
Information Source for Health Plan Authorization	The system that initiates a request to the Information Source for Health Plan Authorization about an individuals' health insurance requirements to obtain an authorization approval for purposes of benefit coverage determination in order to refer a patient for healthcare services	HITSP/T68 HITSP/T79
Node	The originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the <i>Secure Node</i> in the IHE-ITI-TF ATNA Transaction	HITSP/T17
Patient Demographics Consumer	Queries the Patient Demographics Supplier for a list of patient demographic information, if any, and receives a list of corresponding patient demographic information from the Patient Demographics Supplier	HITSP/T23
Patient Demographics Supplier	Receives the query for a list of corresponding patient demographics from the Patient Demographics Consumer, sends a list of corresponding patient demographic information to the Patient Demographics Consumer, maintains one or more Patient Information Sources of patient demographics data	HITSP/T23



Technical Actor(s)	Actor Role	Construct
Patient Identifier Cross-Reference Consumer	Queries the Patient Identifier Cross-Reference Manager for a list of corresponding patient identifiers, if any and receives a list of corresponding patient identifiers from the Patient Identifier Cross-Reference Manager	HITSP/TP22
Patient Identifier Cross-Reference Manager	Receives the query for a list of corresponding patient identifiers from the Patient Identifier Cross-Reference Consumer. Sends a list of corresponding patient identifiers to the Patient Identifier Cross-Reference Consumer. Receives patient demographic information from the Patient Identity Source	HITSP/TP22
Patient Identity Source	Sends patient demographic information when requested, assigns a unique identifier to each instance of a patient, and maintains a collection of identity traits	HITSP/TP22
Service Provider	Represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion	HITSP/TP20
Service User	Represents any individual entity (such as a clinician or an EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transactions	HITSP/TP20
Time Client	Establishes time synchronization with one or more Time Servers using either the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) algorithms. Maintains the local computer system clock synchronization with Coordinated Universal Time (UTC) based on synchronization with the Time Servers	HITSP/T16
Time Server	Provides Network Time Protocol (NTP) time services to Time Clients. It is either directly synchronized to a Coordinated Universal Time (UTC) master clock (e.g. satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s)	HITSP/T16

3.2.2 CONSTRUCT REQUIREMENTS

This section incorporates the comprehensive business and technical requirements and a detailed specification of the transactions and information content specified to complete the information exchange actions identified in each Use Case scenario.

Table 6.4-1 (see Section 6.0) provides a mapping of the HITSP constructs that will be used in the design of the Interoperability Specification, and the data and information exchange requirements that are being satisfied by the construct. The requirements are limited to those that are deemed within scope for this Table, which are described in Section 3.1. Further details about the required technical actors, transactions, and content are also provided in the sections below.

The UML sequence diagrams used in this section incorporate the detailed data requirements for the selected standards (defined in Section 2.2.2), with the Technical Actors, and their specific and detailed Transactions and content (encapsulated in the HITSP constructs listed above). The detailed actor Transactions described in these diagrams show all common or independent technical actors, data, and the specific transactions from the HITSP constructs that are used for the Interoperability Specification.



Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1

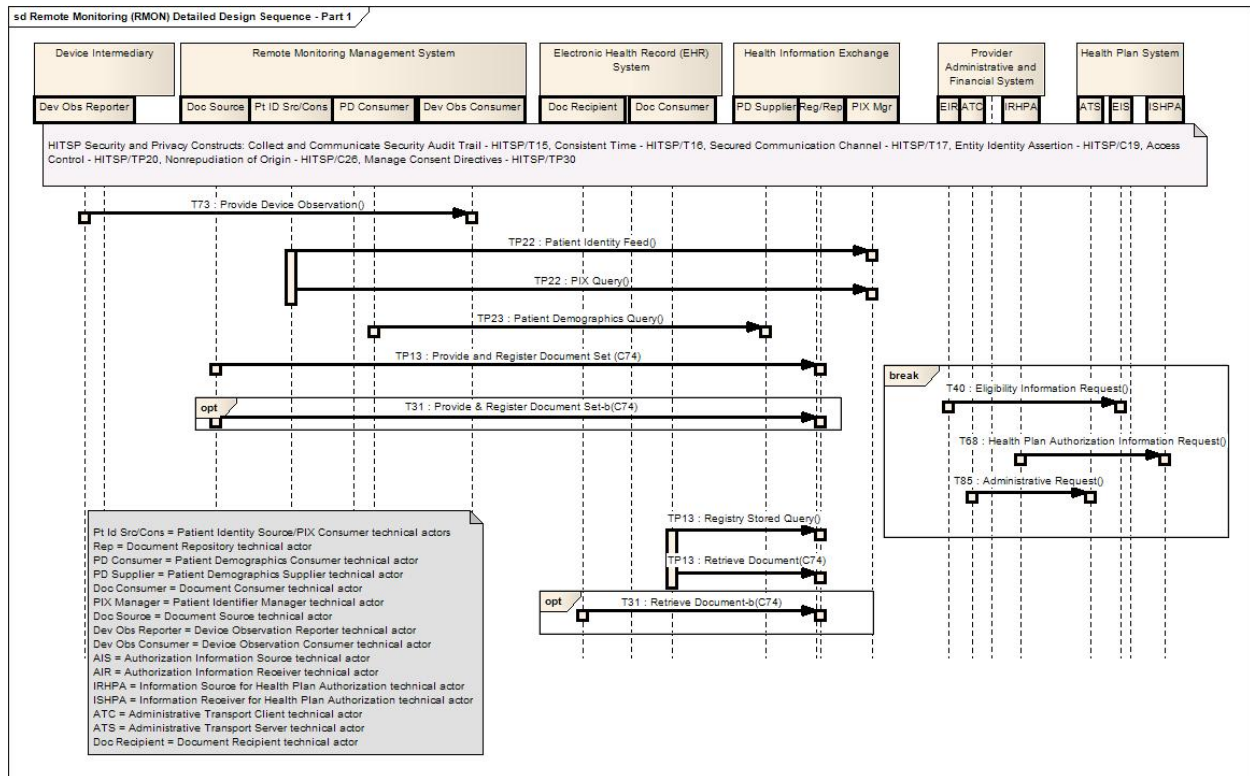
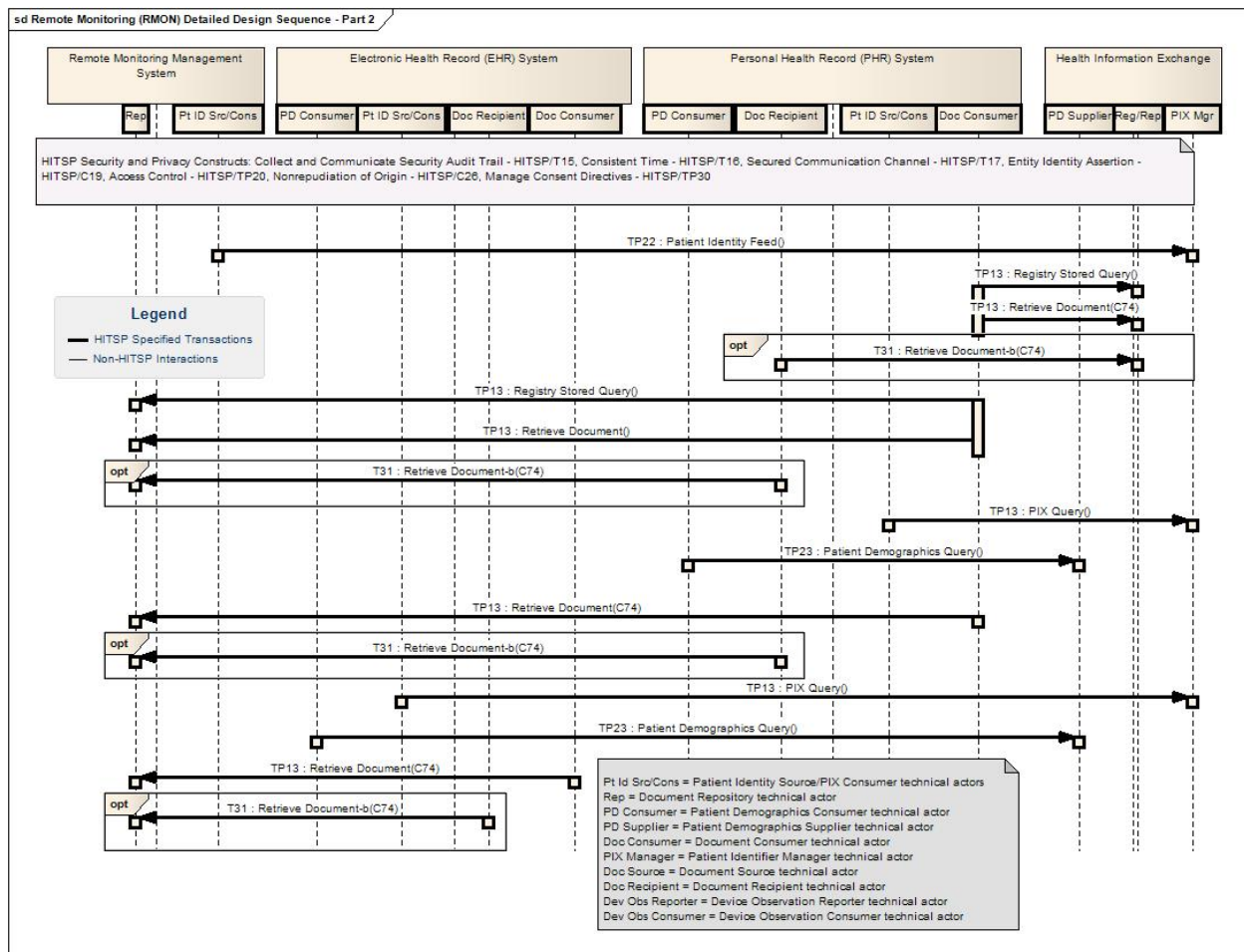


Figure 3.2.2-2 Detailed Sequence Diagram for Scenario 2



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

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

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



This table also includes the corresponding technical actors associated with the relevant Security and Privacy constructs that are used for this Interoperability Specification. Section 1.2 provides a summary description of all the referenced HITSP constructs. Note that this table only shows the business and technical actors that are implemented by the specification. Business actors that are out of scope, or gaps are not included in this section, however, they are discussed in Section 3.1 if they are out of scope or in Section 4.2 if they are found to be gaps where there are no standards.

It is not yet known how the following actors will be secured, since the associated constructs have not yet been written:

- Device Intermediary
- Provider Administrative and Financial System
- Health Plan System

In the absence of this detail, the baseline Security and Privacy constructs (per HITSP/TN900) have been applied. When the constructs and corresponding detailed design are available, the list of Security and Privacy associated technical actors and constructs will need to be revised.

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

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
Device Intermediary	Device Observation Reporter	R	HITSP/T73 [planned June 2009 as per Section 4.3.1]	Provide Device Observation	C[202]
	Audit Record Source	C[113]	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	C[114]	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	C[115]	HITSP/TP20	Access Control Request	O
	Identity Provider	C[118]	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	C[115]	HITSP/TP20	Access Control Request	R
	Service Provider	C[115]	HITSP/TP20	Access Control Request	O



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
Remote Monitoring Management System	Device Observation Consumer	R	HITSP/T73 [planned June 2009 as per Section 4.3.1]	Provide Device Observation	C[202]
	Document Source	C[111]	HITSP/TP13	Provide & Register Document Set-b (online mode)	R
			HITSP/C19	Convey Assertion	O
	Document Source	C[111]	HITSP/T31	Provide & Register Document Set-b	R
			HITSP/C19	Convey Assertion	O
	Content Creator	R	HITSP/C74	Remote Monitoring Observation Document	R
	Patient Identity Source	C[101]	HITSP/TP22	Patient Identity Feed	R
	Patient Identifier Cross Reference Consumer	C[101]	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C[101]	HITSP/T23	Patient Demographics Query	R
	Document Repository	O	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	R	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider	R	HITSP/TP20	Access Control Request	O
EHR System (Clinician)	Document Consumer	C[112]	HITSP/TP13	Registry Stored Query	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Document Recipient	C[112]	HITSP/T31	Provide & Register Document Set-b	R
			HITSP/C19	Convey Assertion	O
	Patient Identity Source	C[101]	HITSP/TP22	Patient Identity Feed	R



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Patient Identifier Cross Reference Consumer	C[101]	HITSP/TP22	PIX Query	R
	Patient Demographics Consumer	C[101]	HITSP/T23	Patient Demographics Query	R
	Document Repository	O	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Content Consumer	R	HITSP/TP30	Consent Document Component	R
			HITSP/C74	Remote Monitoring Observation Document	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	R	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider	R	HITSP/TP20	Access Control Request	O
PHR System (Patient)	Document Consumer	C[112]	HITSP/TP13	Registry Stored Query	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Document Recipient	C[112]	HITSP/T31	Provide & Register Document Set-b	R
			HITSP/C19	Convey Assertion	O
	Document Repository	O	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Patient Identity Source	C[101]	HITSP/TP22	Patient Identity Feed	R
	Patient Identifier Cross-Reference Consumer (PIX Consumer)	C[101]	HITSP/TP22	PIX Query	R
				PIX Update Notification	O



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Patient Demographics Consumer	C[101]	HITSP/T23	Patient Demographic Query	R
	Content Consumer	R	HITSP/TP30	Consent Document Component	R
		R	HITSP/C74	Remote Monitoring Observation Document	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R
	Consent Directive Requester	R	HITSP/TP30	Registry Stored Query	R
				Retrieve Document Set-b	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider	R	HITSP/TP20	Access Control Request	O
Infrastructure Services	Document Registry	C[119]	HITSP/TP13	Register Document Set-b	R
				Registry Stored Query	R
	Document Repository	R	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
			HITSP/C19	Convey Assertion	O
	Patient Identifier Cross Reference Manager (PIX Manager)	C[119]	HITSP/TP22	PIX Query	R
				Patient Identity feed	R
				PIX Update Notification	R
	Patient Demographics Supplier	C[119]	HITSP/T23	Patient Demographics Query	R
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Provide and Register Document Set	R
				Retrieve Document	R
	Consent Registry	O	HITSP/TP30	Registry Stored Query	R
				Register Document Set	R
	Consent Originator	O	HITSP/TP30	Provide and Register Document Set	R



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
Provider Administrative and Financial System	Eligibility Information Receiver	C[116]	HITSP T40	Eligibility Information Request	R
				Eligibility Information Response	R
			HITSP/TP46	Medication and Formulary Eligibility Request	R
				Medication and Formulary Eligibility Response	R
	Information Receiver for Health Plan Authorization	C[116]	HITSP/T68	Health Plan Authorization Information Request	R
				Health Plan Authorization Information Response	R
			HITSP/T79	Pharmacy to Health Plan Authorization Request	R
				Pharmacy to Health Plan Authorization Response	R
	Administrative Transport Client	R	HITSP/T85	Administrative Request	R
				Administrative Response or Error	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	R	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider	R	HITSP/TP20	Access Control Request	O
Health Plan System	Eligibility Information Source	C[117]	HITSP/T40	Eligibility Information Request	R
				Eligibility Information Response	R
		C[117]	HITSP/TP46	Medication and Formulary Eligibility Request	R
				Medication and Formulary Eligibility Response	R
	Information Source for Health Plan	C[117]	HITSP/T68	Health Plan Authorization Information Request	R



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Authorization			Health Plan Authorization Information Response	R
		C[117]	HITSP/T79	Pharmacy to Health Plan Authorization Request	R
				Pharmacy to Health Plan Authorization Response	R
	Administrative Transport Server	R	HITSP/T85	Administrative Request	R
				Administrative Response or Error	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Consent Directive Requester	R	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
	Service User	R	HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider	R	HITSP/TP20	Access Control Request	O

* **NOTE:** Optionality = “R” for Required, “R2” for Required if Known or “O” for Optional, or “C” for Conditional. If applicable, conditional footnotes are further described below.

Implementation Conditions/Constraints

The following table describes the implementation conditions or constraints placed on the technical actors, transactions, or content. The constraint codes listed below correspond to the codes placed in the Actor and Transaction/Content optionality columns in Table 3.2.3-1 above. For example, the Patient Demographics Consumer Technical Actor has an optionality code of C^{[105] [106]} which represents a conditionally required Actor with the constraint codes of 105 and 106 described in the table below.

Table 3.2.3-2 Implementation Conditions/Constraints

Constraint Code	Constraint Description
101	Shall support (Patient Identity Source plus PIX Consumer) and/or Patient Demographics Consumer
111	Business actor shall support at least one of these technical actors to communicate outbound content
112	Business actor shall support at least one of these technical actors to receive or retrieve inbound content



Constraint Code	Constraint Description
113	Device intermediary shall support Audit Record Source if acting as a shared resource (more than 1 patient or more than 1 remote management system etc)
114	Consent Directive Requestor is required if Consent was not applied as a precondition for the remote monitoring session (see HITSP/T17)
115	Service User is required if Access Control was not applied as a precondition for the remote monitoring session (see HITSP/T17)
116	Business actor shall support at least one of these technical actors depending on the type of stakeholder, i.e. pharmacy vs. non-pharmacy
117	Business actor shall support at least one of these technical actors depending on the type of stakeholder, i.e. a health plan offering pharmacy benefits vs. one that only offers medical benefits
118	There must be at least one in a group of business actors
119	There can be ONLY one in a group of business actors
201	Shall support either HITSP Registration and Medication History Document Content Component or Laboratory Report Document Component, or both
202	<p>The Device Observation Reporter and the Device Observation Consumer shall support the applicable nomenclature codes from ISO/IEEE 11073-10101, the Generic Device Data - IEEE P11073-20601™ Optimized exchange protocol], as specified in one or more of the following subsets.</p> <ol style="list-style-type: none"> 1. Blood Glucose Meter - IEEE P11073-10417™ Dev specialization – Glucose meter] 2. Blood Pressure Monitor - IEEE P11073-10407™ Dev specialization – Blood pressure monitor] 3. Oxygen Saturation (Pulse Oximeter) - IEEE P11073-10404™ Dev specialization – Pulse oximeter] 4. Temperature (Thermometer) - IEEE P11073-10408™ Dev specialization – Thermometer] 5. Weight (Weighing Scale) - IEEE P11073-10415™ Dev specialization – Weighing scale]

3.2.4 CONSTRUCT DEPENDENCIES

The following table shows a list of constructs with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific construct. To support a dependent construct, a technical actor must implement all the required actions in the pre-requisite construct, or be grouped together with another construct as specified in the table below:

Table 3.2.4-1 Construct Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
HITSP/C74 - Remote Monitoring Observation Document	HITSP/C80 - Clinical Document and Message Terminology	Pre-condition	Date element terminology will be specified in C80 and used in this construct

3.2.5 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

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



Table 3.2.5-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
PHM Report document (DR30 thru DR37)	HITSP/C74 - Remote Monitoring Observation Document	For all original data, it is required that the sender include a reference to the originating personal health device	General	Ensure traceability back to the source of the data
PHM Report document (DR30 thru DR37)	HITSP/C74 - Remote Monitoring Observation Document	Senders shall communicate all attachments referenced or contained in the PHM Report document	General	Remove optionality for sending attachments
PHM Report document (DR30 thru DR37)	HITSP/C74 - Remote Monitoring Observation Document	Senders shall communicate all attachments specified in the PHM Report in the same message	General	Ensure that all attachments are sent in the same message
Device ID (DR34)	HITSP/C74 - Remote Monitoring Observation Document	For processed data, Senders should include a reference to the device that processed the data	General	Ensure that the source device is identified in the message



4.0 STANDARDS SELECTION

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

- **Evaluation:** The Technical Committee evaluates the standards using the Tier 2 Readiness Criteria
- **Selection:** Based on the Tier 2 evaluations, named standards are selected and listed in the table of selected standards below. It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts
- **Gap and Overlap Analysis and Recommendations:** The Technical Committee also identifies and analyzes gaps and overlaps within the standards industry as they relate to the specific Use Case. The Technical Committee provides a description of the gaps, including missing or incomplete standards, a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps

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

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



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

4.1 STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. In addition, adherence to the selected standards alone is not sufficient to ensure interoperability. In order to ensure interoperability for the Use Case, and to claim conformance to the specification, an implementation must satisfy all the requirements and mandatory statements listed in the HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also be constrained as specified in Table 3.1.2-1, and implement all of the required technical actors from Table 3.2.3-1, within the scope and implementation subset that is selected.

The standards used by this Interoperability Specification fall into the following categories:

- Regulatory guidance is a legal or other authoritative declaration that HITSP must abide by in standards selection (see Section 4.1.1)
- Selected standards are necessary for interoperability. These are standards that are used to meet information exchange requirements of associated constructs. For example, they are used to realize direct information exchange, to provide the transport mechanism, to specify the content, or to address security (see Section 4.1.2)
- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Interoperability Specification (see Section 4.1.3)

4.1.1 REGULATORY GUIDANCE

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



Table 4.1.1-1 Regulatory and Guidance Standards

Standard	Description
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. For more information see the Code of Federal Regulations, Title 45, Parts 160, et. Seq.
Medicare Prescription Drug Improvement and Modernization Act of 2003 (Pub.L. 108-173, 117 Stat. 2066, also called Medicare Modernization Act or MMA)	The Medicare Prescription Drug Improvement and Modernization Act of 2003 (MMA) initiated improvements in the Medicare system. The legislation provided a voluntary program for prescription drug coverage under Medicare. Additionally, the MMA allows a tax deduction to individuals for amounts contributed to health savings security accounts, provides the disposition of unused health benefits in cafeteria plans and flexible spending arrangements. For more information visit www.cms.hhs.gov .

NOTE: For Regulatory and Guidance Standards relating to the Security and Privacy of Health Information, please see HITSP/TN900 Security and Privacy Technical Note

4.1.2 SELECTED STANDARDS

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

Note that the standards selected for this Interoperability Specification are as defined in Section 4.0 above.

Table 4.1.2-1 Selected Standards Linked to HITSP Constructs

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Accredited Standards Committee (ASC) X12 270 and 271 transaction standards version 4010, using the Insurance Subcommittee (X12N) Implementation Guides Version Reference Numbers 004010X92	HITSP/T40 - Patient Generic Health Plan Eligibility Verification HITSP/TP46 - Medication Formulary and Benefits Information	
Accredited Standards Committee (ASC) X12 270 and 271 Transaction Standards Version 4010, using the Insurance Subcommittee (X12N) Addenda 004010X92A1	HITSP/T40 - Patient Generic Health Plan Eligibility Verification HITSP/TP46 - Medication Formulary and Benefits Information	
Accredited Standards Committee (ASC) X12 270 Transaction Version Standards Release 004010	HITSP/T40 - Patient Generic Health Plan Eligibility Verification HITSP/TP46 - Medication Formulary and Benefits Information	
Accredited Standards Committee (ASC) X12 271 Transaction Version Standards Release 004010	HITSP/T40 - Patient Generic Health Plan Eligibility Verification HITSP/TP46 - Medication Formulary and Benefits Information	
Accredited Standards Committee (ASC) X12 278 Transaction Version Standards Release 004010	HITSP/T68 - Patient Health Plan Authorization Request and Response	



Standard Name	HITSP Construct	Remarks/ Minor Gaps
Accredited Standards Committee (ASC) X12 278 transactions standard version 4010, using the Insurance Subcommittee (X12N) Implementation Guides Version Reference Numbers 004010X94	HITSP/T68 - Patient Health Plan Authorization Request and Response	
Accredited Standards Committee (ASC) X12 278 Transactions Standard Version 4010, using the Insurance Subcommittee (X12N) Addenda 004010X94A1	HITSP/T68 - Patient Health Plan Authorization Request and Response	
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	HITSP/C26 – Non-repudiation of Origin	
CDC Race and Ethnicity Code Sets	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Centers for Disease Control and Prevention Implementation Guide for Immunizations Data Transaction using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol. Implementation Guide Version 2.2 June 2006	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Council for Affordable Quality Health Care (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase I Operating Rules	HITSP/T40 - Patient Generic Health Plan Eligibility Verification	
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #260 Eligibility Data Content Rule v2.0.0	HITSP/T40 - Patient Generic Health Plan Eligibility Verification	
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #259 AAA Error Code Reporting Rule v2.0.0	HITSP/T40 - Patient Generic Health Plan Eligibility Verification	
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #258 Normalizing Last Name Rule v2.0.0	HITSP/T40 - Patient Generic Health Plan Eligibility Verification	
Council for Affordable Quality Healthcare (CAQH) Phase II Core #270 Connectivity Rule v2.0.0	HITSP/T85 - Administrative Transport to Health Plan	
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	HITSP/C26 – Non-repudiation of Origin	
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	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Food and Drug Administration (FDA) - Unique Ingredient Identifier (UNII)	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Food and Drug Administration (FDA) - National Drug Code (NDC)	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74



Standard Name	HITSP Construct	Remarks/ Minor Gaps
Health Level Seven (HL7) HL7 Version 3 Standard: Clinical Document Architecture (CDA), Release 2	HITSP/C83 - CDA Content Modules	
Health Level Seven (HL7) Implementation Guide for CDA Release 2.0 Personal Health Monitoring Report (PHMR) DSTU Release 1, July 2008 Ballot	HITSP/C74 - Remote Monitoring Observation	
Health Level Seven (HL7) Implementation Guide for CDA Release 2: History and Physical (H&P) Notes	HITSP/C83 - CDA Content Modules	
Health Level Seven (HL7) Implementation Guide for CDA Release 2: Consultation Note	HITSP/C83 - CDA Content Modules	
Health Level Seven (HL7) Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD), April 01, 2007	HITSP/C83 - CDA Content Modules	
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/TP20 – Access Control	Underlying standard referenced in Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0
Health Level Seven (HL7) Version 2.3.1 Chapter 2 – Control, Chapter 3 – Patient Administration	HITSP/TP22 - Patient ID Cross-Referencing	
Health Level Seven (HL7) Version 2.5, Chapter 2 – Control, Chapter 3 – Patient Administration, Chapter 5 - Query	HITSP/T23 - Patient Demographics Query HITSP/TP22 - Patient ID Cross-Referencing	
Health Level Seven (HL7) Version 2.5.1 – Vocabularies and Value Sets	HITSP/C80 - Clinical Document and Message Terminology	
Health Level Seven (HL7) Version 3.0 – Vocabularies and Value Sets	HITSP/C80 - Clinical Document and Message Terminology	
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/TP30 - Manage Consent Directives	
HUGO Gene Nomenclature Committee at the European Bioinformatics Institute - Gene Names	HITSP/C80 - Clinical Document and Message Terminology	
Extensions to the ISO/IEEE 11073-10101 — Part 10101: nomenclature, based on IEEE P11073-20601™ Optimized exchange protocol - Annex H IEEE P11073-10417™ Dev specialization – Glucose meter- Annex C IEEE P11073-10407™ Dev specialization – Blood pressure monitor - Annex C IEEE P11073-10404™ Dev specialization – Pulse oximeter - Annex C IEEE P11073-10408™ Dev specialization – Thermometer - Annex C IEEE P11073-10415™ Dev specialization – Weighing scale - Annex C	HITSP/C74 - Remote Monitoring Observation Document Component	



Standard Name	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008-2009, Cross-Community Access (XCA), Trial Implementation, October 10, 2008	HITSP/TP13 - Manage Sharing of Documents	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Patient Identifier Cross-Referencing Integration Profile (PIX)	HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication Profile (ATNA)	HITSP/T15 - Collect and Communicate Security Audit Trail	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	HITSP/T17 - Secured Communication Channel	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Consistent Time (CT) Integration Profile	HITSP/T16 - Consistent Time	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	HITSP/C19 - Entity Identity Assertion	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	HITSP/C26 - Nonrepudiation of Origin	



Standard Name	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 5.0 or later, Patient Demographics Query (PDQ) Integration Profile	HITSP/T23 - Patient Demographics Query	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008 - 2009, Pediatric Demographics, Draft for Trial Implementation (August 22, 2008)	HITSP/T23 - Patient Demographics Query HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) 2007-2008 Trial Implementation Supplement Cross-enterprise Document Reliable Interchange (XDR) Release 3	HITSP/T31 - Document Reliable Interchange	
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Revision 4.0	HITSP/C83 - CDA Content Modules	
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
International Organization for Standardization (ISO) ISO 3166-1	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	HITSP/T16 - Consistent Time	
Internet Society – Tags for Identifying Languages - 2005	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
Logical Observation Identifiers Names and Codes (LOINC®)	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
National Cancer Institute (NCI) Thesaurus	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
National Council for Prescription Drug Programs (NCPDP) Formulary and Benefits Standard Implementation Guide	HITSP/TP46 - Medication Formulary and Benefits Information	
National Council for Prescription Drug Programs (NCPDP) Telecommunication Standard Implementation Guide Version 5.1	HITSP/T79 - Pharmacy Authorization Request and Response HITSP/TP46 - Medication Formulary and Benefits Information	
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	HITSP/TP20 - Access Control	



Standard Name	HITSP Construct	Remarks/ Minor Gaps
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/TP20 - Access Control	
Unified Code for Units of Measure (UCUM)	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
United States Postal Service (USPS) – Postal Codes	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74
VHA National Drug File Reference Terminology (NDF-RT) Formulary	HITSP/C80 - Clinical Document and Message Terminology	Vocabulary enabled by HITSP/C74

4.1.3 INFORMATIVE REFERENCE STANDARDS

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

Table 4.1.3-1 Informative Reference Standards

Standard Name	Description
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 Name	Description
ASTM International Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	<p>Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management.</p> <p>The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards.</p> <p>Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org.</p>
ASTM International Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	<p>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, to the Privacy Act of 1974 (1)." For more information visit www.astm.org.</p>
Council for Affordable Quality Healthcare (CAQH) Phase I CORE #153 Connectivity Rule	Base standard for CAQH Phase II CORE #270 Connectivity Rule.
Federal Medication Terminologies	<p>A set of controlled terminologies and code sets developed and maintained as part of a collaboration between the Food and Drug Administration, National Library of Medicine, Veterans Health Administration, National Cancer Institute and Agency for Healthcare Research and Quality related to medications, including medication proprietary and nonproprietary names, clinical drug code (RxNorm); ingredient names and Unique Ingredient Identifiers (UNII); routes of administration, dosage forms, and units of presentation from the NCI Thesaurus (NCIt); and certain pharmacological drug classes from the National Drug File Reference Terminology (NDF-RT) .</p> <p>The Federal Medication Terminology leverages medication models maintained by the Food and Drug Administration (ex. UNII, NDC Codes), National Library of Medicine (RxNorm), the Veterans Health Administration (NDF-RT), and the National Cancer Institute (NCIt). For more information visit www.cancer.gov/cancertopics/terminologyresources/page4.</p>
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	<p>HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org.</p>
Health Level Seven (HL7) Version 3.0	<p>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.</p>



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



Standard Name	Description
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, and staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org .
International Organization for Standardization (ISO) Health Informatics -- Functional and Structural Roles (ISO SF Roles), Technical Specification #21298, Draft May, 2007	<p>This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed.</p> <p>Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare actors.</p> <p>Directory services: structural roles are usefully recorded within directories of healthcare providers (see for example, ISO TS 21091 Health Informatics -- Directory services for security, communications, and identification of professionals and patients).</p> <p>Audit trails: functional roles are usefully recorded within audit trails for health information applications.</p> <p>Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics -- Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary.</p> <p>For more information visit www.iso.org.</p>
National Cancer Institute (NCI) Thesaurus: Route of Administration	<p>Route of Administration is the path by which a particular drug product is introduced on or into the body. The medication terminology is maintained by the NCI Thesaurus, a reference terminology and biomedical ontology used in a growing number of NCI and other systems. It covers vocabulary for clinical care, translational and basic research, and public information and administrative activities. The NCI Thesaurus provides definitions, synonyms, and other information on nearly 10,000 cancers and related diseases, 8,000 single agents and combination therapies, and a wide range of other topics related to cancer and biomedical research. It is part of the Federal Medication Terminologies. For more information visit www.cancer.gov.</p>
Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security SOAP Message Security Version 1.0	Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e. support multiple security token formats. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message. For more information visit www.oasis-open.org .
Organization for the Advancement of Structured Information Standards (OASIS) Simple Object Access Protocol (SOAP) Version 1.1	SOAP is a protocol specification for invoking methods on servers, services, components and objects. SOAP codifies the existing practice of using XML and HTTP as a method invocation mechanism. The SOAP specification mandates a small number of HTTP headers that facilitate firewall/proxy filtering plus an XML vocabulary that is used for representing method parameters, return values, and exceptions." {DevelopMentor} SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. For more information visit www.oasis-open.org .



Standard Name	Description
Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity	This classification provides a minimum standard for maintaining, collecting, and presenting data on race and ethnicity for all Federal-reporting purposes. The categories in this classification are social-political constructs and should not be interpreted as being scientific or anthropological in nature. The standards have been developed to provide a common language for uniformity and comparability in the collection and use of data on race and ethnicity by Federal agencies. For more information visit www.census.gov .

4.2 GAPS WHERE THERE ARE NO STANDARDS

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

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

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

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

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Summary Description	Identified Gaps	Recommended Resolution
7.1.3 Receive remote monitoring summary	<p>Action 7.1.3.1 Clinician receives remote monitoring summary from the remote monitoring mgmt system or HIE.</p> <p>The information exchange requirements for this event are reflected in:</p> <p>IER18 Send/receive clinical document</p> <p>IER61 Provide and Register Document Set and/or</p> <p>IER38 Query/Retrieve Document Set</p>	<p>The following data requirements do not have standards available to have their related information be captured and reported to the clinician in accordance with the System Data Exchange Figure 2.2.4-1:</p> <p>DR37</p> <p>DR82 through DR88</p> <p>DR90</p> <p>DR93 through DR96</p> <p>DR98 and DR99</p>	<p>Based on the ongoing standards development work underway in the industry in regards to the Remote Monitoring, the projected set of devices and their related measurements/information to be addressed by the HITSP TC is depicted the Roadmap Matrix shown in Table 4.2-2. Data and device requirements included in this Use Case which are addressed in 2009 will remain on the HITSP TC roadmap for attention in subsequent years</p>



Event Code	Summary Description	Identified Gaps	Recommended Resolution
7.2.2 Access or receive monitoring information	<p>Action 7.2.2.1 The care coordinator reviews a patient's remote monitoring information via information intermediary.</p> <p>The information exchange requirements for this event is reflected in:</p> <p>IER39 Send/receive device observation data</p>	<p>The following data requirements do not have standards available to have their related information be captured and reported to the clinician in accordance with the System Data Exchange Figure 2.2.4-1:</p> <p>DR37 DR82 through DR88 DR90 DR93 through DR96 DR98 and DR99</p>	<p>Based on the ongoing standards development work underway in the industry in regards to the Remote Monitoring, the projected set of devices and their related measurements/information to be addressed by the HITSP TC is depicted the Roadmap Matrix shown in Table 4.2-2. Data and device requirements included in this Use Case which are addressed in 2009 will remain on the HITSP TC roadmap for attention in subsequent years</p>
7.2.5 Communicate monitoring information	<p>Action 7.2.5.2 Care coordinator communicates remote monitoring information and assessment information to the clinician</p> <p>The information exchange requirements for this event are reflected in:</p> <p>IER18 Send/receive clinical document IER61 Provide and Register Document Set and/or IER38 Query/Retrieve Document Set</p>	<p>The following data requirements do not have standards available to have their related information be captured and reported to the clinician in accordance with the System Data Exchange Figure 2.2.4-1:</p> <p>DR37 DR82 through DR88 DR90 DR93 through DR96 DR98, and DR99</p>	<p>Based on the ongoing standards development work underway in the industry in regards to the Remote Monitoring, the projected set of devices and their related measurements/information to be addressed by the HITSP TC is depicted the Roadmap Matrix shown in Table 4.2-2. Data and device requirements included in this Use Case which are addressed in 2009 will remain on the HITSP TC roadmap for attention in subsequent years</p>
7.3.4 Receive remote monitoring data	<p>Action 7.3.4.1 Patient receives remote monitoring summary from the remote monitoring mgmt system or HIE.</p> <p>The information exchange requirements for this event are reflected in:</p> <p>IER18 Send/receive clinical document IER61 Provide and Register Document Set and/or IER38 Query/Retrieve Document Set</p>	<p>The following data requirements do not have standards available to have their related information be captured and reported to the clinician in accordance with the System Data Exchange Figure 2.2.4-1:</p> <p>DR37 DR82 through DR88 DR90 DR93 through DR96 DR98, and DR99</p>	<p>Based on the ongoing standards development work underway in the industry in regards to the Remote Monitoring, the projected set of devices and their related measurements/information to be addressed by the HITSP TC is depicted the Roadmap Matrix shown in Table 4.2-2. Data and device requirements included in this Use Case which are addressed in 2009 will remain on the HITSP TC roadmap for attention in subsequent years</p>
7.1.1 Evaluate patient and order remote monitoring	<p>Action 7.1.1.3 Clinician orders remote monitoring. The information exchange requirements for this event are reflected in:</p> <p>IER18 Send/receive clinical document IER61 Provide and Register Document Set and/or IER38 Query/Retrieve Document Set</p>	<p>The communication of remote monitoring services orders in a standardized format (i.e. DR39) requires further standards development</p>	<p>January 2009; Review the planned AHIC Use Cases for Order Administration and reach out to the appropriate SDO or standards development groups regarding activities for this interface requirement and add this to the HITSP TC roadmap accordingly</p>



Event Code	Summary Description	Identified Gaps	Recommended Resolution
7.1.5 Modify treatment plan and communicate with patient 7.3.6 Patient discusses treatment plan with clinician	For Actions: 7.1.5.2 The clinician communicates a change in care plan to the patient and other information recipients 7.3.6.2 Patient accesses modified treatment plan information provided by a personal clinician The information exchange requirements for this event are reflected in IER24 Communication of a Structured Treatment Plan and Revisions Thereof.	The communication of structured treatment plans in a standardized format (i.e. DR40) requires further standards development. The requirements in this regard are expected to be included in the Consultation and Transfer of Care Use Case As a result, this requirement is considered out-of-scope for the Remote Monitoring Use Case	January 2009; Review the requirements related to Treatment Plans and their administration in the Consultation and Transfer of Care Use Case with the Provider PTC. Ensure the Remote Monitoring activity is appropriately reflected in the options of treatment plan oversight and data collection
7.1.3 Receive remote monitoring summary 7.2.5 Communicate monitoring information 7.3.4 Receive remote monitoring data	For Actions: 7.1.3.1 Remote monitoring information is communicated to the clinician's EHR 7.2.5.2 Care coordinator communicates remote monitoring information and assessment information to the clinician. 7.3.4.1 Remote monitoring information is communicated to the patient's PHR The information exchange requirements for this event are reflected in: IER18 Send/receive clinical document IER61 Provide and Register Document Set and/or IER38 Query/Retrieve Document Set	General rules regarding specific terminology choices for the remote monitoring summary document (C74 Remote Monitoring Observation Document) such as, LOINC, SNOMED-CT, ISO/IEEE 11073 MDC, UCUM units of measure, etc	2009: HITSP will be working with Continua and IHE to harmonize a set of terminology rules

Table 4.2-2 Remote Monitoring Roadmap

AHIC March 2008 Remote Monitoring Use Case	IS77-Dec 2008	IS77- Dec 2009
Physiological Measurement Data Types and Devices (Examples provided below are not comprehensive)		
• Blood Glucose [DR80]	Included	2008
• Blood Pressure [DR81]	Included	2008
• Brain Activity (e.g., Ambulatory EEG) [DR82]		No
• Cholesterol [DR83]		Yes



AHIC March 2008 Remote Monitoring Use Case	IS77-Dec 2008	IS77- Dec 2009
• Esophageal pH [DR84]		No
• Heart Rate [DR85]	Included	2008
• Heart Rhythm (e.g., AECG, Holter Monitor, Cardiac Implants) [DR86]		Yes (1-3 Channel ECG and rhythm) No (Cardiac Implants, Holter Monitor)
• Implantable Cardioverter Defibrillator (ICD) Monitoring (e.g., Inter cardiac Pressure, Intrathoracic Fluid, EGM Waveforms) [DR87]		No
• Lung Function [e.g., FEV1 (forced expiratory in 1 sec), FVC (forced vital capacity), PEV(peak expiratory volume), PEFR (peak expiratory flow rate)], i.e. Spirometry measures [DR88]		Yes
• Oxygen Saturation [DR89]	Included	2008
• Respiration Rhythm [DR90]		Yes (Respiration rate through ECG)
• Temperature [DR91]	Included	2008
• Weight [DR92]	Included	2008
Medication Management and Administration Data and Device Types:		
• Electronic Pillbox – Patient Alerts and Medication Administration Tracking [DR93]		Yes
• Medication Pumps – Medication Administration [DR94]		Yes (Reporting Pump activity) No (Pump Programming)
• Medication Infusion Devices – Medication Administration [DR95]		Yes (Reporting Infusion Pump activity) No (Infusion Pump Programming)
Activities of Daily Living Data and Device Types: [DR96]		
• ADL Biosensors and Detection Devices		Yes
• Emergency Alerting, Global Positioning System (GPS)		Yes (Emergency alerting)
• Fall Detection		Yes (Simple fall)
• Pedometer (Steps Moved)		Yes
• Sleep Actigraphy		Yes (Simple)
Measurement Metadata – Device/Device Intermediary-Generated: [DR97]		
• Device Identification Information	Yes	2008
• Patient Identification Data	Yes	2008
• Device Type	Yes	2008
• Device Setting Information		Yes
• Date/Time of Measurement	Yes	2008
• Data Source (Device-generated vs. Patient-entered)		Yes
• Measurement Characteristics (Raw vs. Summary Data)		Yes
• Measurement Scale/Units	Yes	2008



AHIC March 2008 Remote Monitoring Use Case	IS77-Dec 2008	IS77- Dec 2009
<ul style="list-style-type: none"> Device Calibration/Programming Data 	Yes	2008
Error Details: [DR98]		
<ul style="list-style-type: none"> Device Malfunction 	Yes	2008
<ul style="list-style-type: none"> User Error During Measurement 		Yes
<ul style="list-style-type: none"> Measurement Cancelled by Patient (Stopped measurement process or marked measurement as invalid) 	Yes	2008
Patient-Entered Measurement Descriptive data: [DR99]		
<ul style="list-style-type: none"> Measurement-Instance Specific Details (e.g., patient-entered accompanying the measurement such as stress level, position) 		Yes
<ul style="list-style-type: none"> Measurement Error Details 		Yes
Alerts and Notices [DR37]		
<ul style="list-style-type: none"> Normal Range 		Yes
<ul style="list-style-type: none"> Normal Range for Patient 		Yes (potential for remote patient-specific setting of normal ranges)
<ul style="list-style-type: none"> Alert (Low Value, High Value, Change in Trend) 		Yes

4.3 STANDARD OVERLAPS

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

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

Table 4.3-1 Use Case Requirements and Associated Standards Overlaps

Requirement Number	Summary Description	Standard Overlap	Recommended Resolution
IER39	For Action 7.2.2.1, The care coordinator reviews a patient's remote monitoring information via information intermediary	The following data requirements have overlapping standards available to have their related information be captured and reported to the clinician in accordance with the System Data Exchange Figure 2.2.4-1. DR30, DR35, DR36, DR80, DR81, DR89, DR91, DR92, and DR97	June 2009: See Section 4.3.1 Strategy for HITSP/IS77 and Completing IER39 (HITSP/T73)

4.3.1 STRATEGY FOR HITSP/IS77 AND COMPLETING IER39 (HITSP/T73)

1. HITSP/IS77 Remote Monitoring Interoperability Specification



IHE, Continua, and HITSP TCs have achieved consensus on the system data exchanges 1, 3, 4, 5, 6, 7 depicted in Figure 2.2.4-1. On System Data Exchange #2, Device Intermediary to the Remote Monitoring System, there is additional work to be done. The results of this work will be documented in the planned HITSP construct entitled T73 – Aggregate Device Information Communication.

For Consumer Grade and Clinical Grade applications, the IEEE 11073 PHD nomenclature provides semantic interoperability and has been concluded as the resolution of the data requirements for the devices being addressed in this release of the IS77 document.

For devices beyond those specified in Section 3.1 and future extended clinical-grade devices, nomenclature should be drawn from the following:

- ISO/IEEE 11073-10101:2004(E) – Health Informatics Point-of-care medical device communication Part 10101: Nomenclature, First Edition
- IHE Patient Care Device Technical Framework Supplement 2008-2009 – Rosetta Terminology Mapping (RTM) – Defines observation identifiers and co-constraints such as units-of-measure, enumerations, external measurement site identifiers and instrumentation hierarchy which also defines IEEE 11073 to UCUM Units-Of-Measure Mapping

Ultimately all new terms used in this version of IS77 (defined in IEEE P11073-104XX) will be merged into ISO/IEEE 11073-10101 base nomenclature standards.

Table 4.3-2 Selected Nomenclature Standards for HITSP/T73

Standard Name
Extensions to the ISO/IEEE 11073-10101 — Part 10101: nomenclature, based on IEEE P11073-20601™ Optimized exchange protocol - Annex H IEEE P11073-10417™ Dev specialization – Glucose meter- Annex C IEEE P11073-10407™ Dev specialization – Blood pressure monitor - Annex C IEEE P11073-10404™ Dev specialization – Pulse oximeter - Annex C IEEE P11073-10408™ Dev specialization – Thermometer - Annex C IEEE P11073-10415™ Dev specialization – Weighing scale - Annex C
Health Level Seven (HL7) Version 2.5 Ch7 Observation Reporting
IEEE P11073-20601 Health informatics – Personal health device communication – Part 20601: Application profile – Optimized exchange protocol
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework Year 1: 2006-2007 Volume 1 – Integration Profiles Volume 2 – Transactions
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework Supplement 2008-2009 – Rosetta Terminology Mapping (RTM)
ISO/IEC and ITU-T standard X.680: Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation
ISO/IEC and ITU-T standard X.693 – Information Technology – ASN.1 Encoding Rules: XML Encoding Rules (XER)
ISO/IEEE 11073-10101:2004(E) Health informatics — Point-of-care medical device communication — Part 10101: Nomenclature, First Edition.



2. HITSP 2009 Work for Completion of HITSP/T73 Construct for IER39/System Data Exchange #2
IHE, Continua and HITSP TCs are highly motivated to work together. IHE and Continua have already signed an MOU. To converge on a single solution for System Data Exchange #2, additional work will be needed to achieve consensus. IHE, Continua and HITSP will make their best effort to complete this work by June 2009. In the event that this does not happen, it is recommended that HITSP convene an interim cross-organizational team of HITSP TC members to review the progress, collect information (e.g., industry survey of manufacturers/consumers of RMON Device Intermediary), and provide a recommendation to the HITSP Board. We used a similar approach to achieve consensus with CCD. None of us want an interim approach, so this statement is just to motivate us all to achieve consensus.



5.0 TECHNICAL IMPLEMENTATION

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

5.1 CONFORMANCE CRITERIA

In order to claim conformance to the specification, an implementation must satisfy all the requirements and mandatory statements listed in the HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must be constrained as specified in Table 3.1.2-1, and implement all of the required actors from Table 3.2.3-1, within the scope, subset or implementation option that is selected from Section 5.2 below.

Claims of conformance to this specification must be made using the following language:

This product conforms to the HITSP/IS77 Remote Monitoring Interoperability Specification, available at www.hitsp.org.

5.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

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

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

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

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



5.3 TEST METHODS

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

A Health Information Technology (HIT) Implementation Testing website has been developed in collaboration with Healthcare Information Technology Standards Panel (HITSP), the National Institute of Standards and Technology (NIST), the Certification Commission for Healthcare Information Technology (CCHIT), and the Office of the National Coordinator (ONC) to advance conformance and interoperability testing capabilities. This website provides HIT implementers with the necessary resources to support and test their implementation of standards-based health systems. For more information, visit NIST at www.nist.gov.



6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF STANDARDS

The following table contains descriptions of the selected standards from Section 4.1.2 above:

Table 6.2-1 Description of Standards

Standard Name	Description
Accredited Standards Committee (ASC) X12 270 and 271 Transaction Standards Version 4010, using the Insurance Subcommittee (X12N) Addenda 004010X92A1	Many of the version X12N 004010 Implementation Guides, including all of those adopted under HIPAA, have Addenda that contain updates -- only -- to the original Implementation Guides. These Addenda are identified as version 004010A1. Implementation Guide 004010X092A1 describes transactions for Health Care Eligibility Benefit Inquiry and Response. Implementation Guides are published by Washington Publishing Company. For more information visit www.wpc-edl.com .
Accredited Standards Committee (ASC) X12 270 and 271 transaction standards version 4010, using the Insurance Subcommittee (X12N) Implementation Guides Version Reference Numbers 004010X92	Detailed Implementation Guides based on release 004010 of the X12 standards. These Implementation Guides provide details on the use of X12 standards to accomplish specific transaction functions. Some of the version 004010 Implementation Guides, but not all, have been adopted as Implementation Specifications under HIPAA. Implementation Guides are published by Washington Publishing Company. For more information visit www.wpc-edl.com .
Accredited Standards Committee (ASC) X12 270 Transaction Version Standards Release 004010	The objective of the Health Care Eligibility/Benefit Inquiry (270) is to provide for the exchange of eligibility inquiry to individuals within a health plan. This transaction can be used by healthcare providers to request coverage and payment information on the member/insured in a batch environment where real time processing is not required. This transaction is also used to provide additional patient eligibility information to support administrative reimbursement for healthcare products and services. This standard is required by HIPAA.
Accredited Standards Committee (ASC) X12 271 Transaction Version Standards Release 004010	The objective of the Health Care Eligibility, Coverage, or Benefit Information (271) is to provide for the response to eligibility inquiries about individuals within a health plan. This transaction can be used to receive coverage and payment information on a member/insured in a batch environment where real time processing is not required. This transaction is also used to provide additional patient eligibility information to support administrative reimbursement for healthcare products and services. This standard is required by HIPAA.
Accredited Standards Committee (ASC) X12 278 Transaction Version Standards Release 004010	The objective of the Health Care Service Review – Request for Review and Response (278) is to provide for the exchange of service review requests from a healthcare provider to a health plan, and a corresponding response from the health plan to that healthcare provider. This transaction can be used by healthcare providers to request approval and coverage information on the patient for a particular service type or service. This standard is required by HIPAA. This standard is required by regulatory guidance.
Accredited Standards Committee (ASC) X12 278 Transactions Standard Version 4010, using the Insurance Subcommittee (X12N) Addenda 004010X94A1	Many of the version X12N 004010 Implementation Guides, including all of those adopted under HIPAA, have Addenda that contain updates -- only -- to the original Implementation Guides. These Addenda are identified as version 004010A1. Implementation Guide 004010X094A1 describes transactions for Health Care Service Review – Request for Review and Response. Implementation Guides are published by Washington Publishing Company. For more information visit www.wpc-edl.com . This standard is required by regulatory guidance.



Standard Name	Description
Accredited Standards Committee (ASC) X12 278 transactions standard version 4010, using the Insurance Subcommittee (X12N) Implementation Guides Version Reference Numbers 004010X94	Detailed Implementations Guide based on release 004010 of the X12 standards. These Implementation Guides provide details on the use of X12 standards to accomplish specific transaction functions. Some of the version 004010 Implementation Guides, but not all, have been adopted as Implementation Specifications under HIPAA. This standard is required by regulatory guidance. Implementation Guides are published by Washington Publishing Company. For more information visit www.wpc-edi.com .
Accredited Standards Committee (ASC) X12 Standards Release 004010	Release (version) 004010 of the Accredited Standards Committee (ASC) X12 standards including the X12.5 Interchange Control, X12.6 Application Control Structure, 270 Eligibility, Coverage or Benefit Inquiry, 271 Eligibility, Coverage or Benefit Information and other control standards for the uniform electronic interchange of business transactions. Published by the Data Interchange Standards Association (DISA). For more information visit www.x12.org .
American Medical Association (AMA) Current Procedural Terminology (CPT®) Fourth Edition (CPT-4); CPT Evaluation and Management Codes	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 .
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Defines a document structure for use by electronic signature mechanisms, describes the characteristics of an electronic signature process. Defines minimum requirements for different electronic signature mechanisms, defines signature attributes for use with electronic signature mechanisms, describes acceptable electronic signature mechanisms and technologies, defines minimum requirements for user identification, access control, and other security requirements for electronic signatures, and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism. For more information visit www.astm.org .
CDC Race and Ethnicity Code Sets	The U.S. Centers for Disease Control and Prevention (CDC) has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards. For more information visit www.cdc.gov .
Centers for Disease Control and Prevention Implementation Guide for Immunizations Data Transaction using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol. Implementation Guide Version 2.2 June 2006	This Guide is intended for use by immunization registries that want to participate in a strictly-defined record exchange agreement that limits the amount of optionality normally expected when using the HL7 standard. The Guide describes the most frequently used segments in their entirety, while giving a minimum description of segments containing only a few useful fields for registries. The Guide fully describes the fields within the segments used frequently by immunization registries, while the others are omitted in this document. With this limited scope, this <i>Guide</i> can in no way serve as a substitute for a thorough study of the entire set of HL7 specifications for electronic data interchange in healthcare environments. For more information visit www.cdc.gov/vaccines/programs/iis/stds/downloads/hl7guide.pdf .
Council for Affordable Quality Health Care (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase I Operating Rules	Provide agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.caqh.org .
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #258 Normalizing Last Name Rule v2.0.0	Provides agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.caqh.org .



Standard Name	Description
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #259 AAA Error Code Reporting Rule v2.0.0	Provides agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.cagh.org .
Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase II #260 Eligibility Data Content Rule v2.0.0	Provides agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.cagh.org .
Council for Affordable Quality Healthcare (CAQH) Phase II Core #270 Connectivity Rule v2.0.0	<p>The CORE #270 Connectivity Rule v2.00 developed by CAQH/CORE Connectivity Subgroup. It includes the following:</p> <ul style="list-style-type: none"> • Scope definition, rationale and policy guidelines • Message envelope and submitter authentication standards (payload agnostic) • Basic conformance requirements for stakeholders in terms of the chosen standards • Message envelope metadata names, syntax and semantics • Message envelope schemas and examples of use • Error handling • Glossary of terms <p>For further information visit www.cagh.org.</p>
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	Extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European Directive. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with this document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. For more information visit www.etsi.org .
<p>Extensions to the ISO/IEEE 11073-10101 — Part 10101: nomenclature, based on</p> <p>IEEE P11073-20601™ Optimized exchange protocol - Annex H</p> <p>IEEE P11073-10417™ Dev specialization – Glucose meter- Annex C</p> <p>IEEE P11073-10407™ Dev specialization – Blood pressure monitor - Annex C</p> <p>IEEE P11073-10404™ Dev specialization – Pulse oximeter - Annex C</p> <p>IEEE P11073-10408™ Dev specialization – Thermometer - Annex C</p> <p>IEEE P11073-10415™ Dev specialization – Weighing scale - Annex C</p>	These are extensions to the ISO/IEEE 11073-10101 'base' nomenclature, based on the X73 Personal Health Device base standard and specializations. Ultimately all new terms originally defined in IEEE P11073-104XX will be merged into ISO/IEEE 11073-10101. For more information visit www.iso.org



Standard Name	Description
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.
Federal Medication Terminologies	A set of controlled terminologies and code sets developed and maintained as part of a collaboration between the Food and Drug Administration, National Library of Medicine, Veterans Health Administration, National Cancer Institute and Agency for Healthcare Research and Quality related to medications, including medication proprietary and nonproprietary names, clinical drug code (RxNorm); ingredient names and Unique Ingredient Identifiers (UNII); routes of administration, dosage forms, and units of presentation from the NCI Thesaurus (NCIt); and certain pharmacological drug classes from the National Drug File Reference Terminology (NDF-RT) . The Federal Medication Terminology leverages medication models maintained by the Food and Drug Administration (ex. UNII, NDC Codes), National Library of Medicine (RxNorm), the Veterans Health Administration (NDF-RT), and the National Cancer Institute (NCIt). For more information visit www.cancer.gov/cancertopics/terminologyresources/page4 .
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 for CDA Release 2.0 Personal Health Monitoring Report (PHMR) DSTU Release 1, July 2008 Ballot	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: History and Physical (H&P) Notes	The HL7 Implementation Guide for CDA Release 2: History and Physical (H&P) Notes defines additional constraints on the CDA Header and Body used in a History and Physical document in the U.S. realm, and provides examples of conforming fragments in the body of the document and an example of a conforming XML instance.
Health Level Seven (HL7) Implementation Guide for CDA Release 2: Consultation Note.	The HL7 Implementation Guide for CDA Release 2: Consultation Note defines additional constraints on the CDA Header and Body used in a Consultation document in the U.S. realm, and provides examples of conforming fragments in the body of the document and an example of a conforming XML instance.



Standard Name	Description
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 Ch7 Observation Reporting	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, and timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. For more information visit www.hl7.org .
Health Level Seven (HL7) Version 2.5, 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 .
Health Level Seven (HL7) Version 2.5.1 – Vocabularies and Value Sets	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 – Vocabularies and Value Sets	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



Standard Name	Description
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 .
HUGO Gene Nomenclature Committee at the European Bioinformatics Institute - Gene Names	For each known human gene, HUGO approves a gene name and symbol (short-form abbreviation). All approved symbols are stored in the HGNC database. Each symbol is unique and HUGO ensures that each gene is only given one approved gene symbol. In preference each symbol maintains parallel construction in different members of a gene family and can also be used in other species, especially the mouse. For more information visit www.genenames.org .
Human Genome Variation Society (HGVS) - Description of Sequence Variants – February, 20, 2008	Discussions regarding the uniform and unequivocal description of sequence variants in DNA and protein sequences (mutations, polymorphisms) were initiated by two papers published in 1993; Beaudet AL & Tsui LC and Beutler E. Current rules (den Dunnen, JT and Antonarakis, SE [2000]) however do not extensively cover all types of variants and the more complex changes. These pages list, based on the last publication, the existing nomenclature recommendations as well as the most recent suggestions. The article den Dunnen JT and Antonarakis SE (2000). Hum.Mutat. 15:7-12 provide more detail explanation. For more information visit www.hgvs.org/mutnomen/recs.html#intro .
IEEE P11073-20601 Health informatics – Personal health device communication – Part 20601: Application profile – Optimized exchange protocol	Establishes a normative definition of communication between personal telehealth thermometer devices and compute engines (e.g. cell phones, personal computers, personal health appliances, set top boxes) in a manner that enables plug-and-play interoperability. It specifies the use of specific term codes, formats, and behaviors in telehealth environments restricting optionality in base frameworks in favor of interoperability. Annex C contains the required nomenclature. For more information visit standards.ieee.org/ .
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. 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 actor specific requirements. 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 .



Standard Name	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 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) 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) 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.
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. For more information visit www.ihe.net .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. For more information visit www.ihe.net .



Standard Name	Description
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) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 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 actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise. For more information visit www.ihe.net .
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. 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) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	The Basic Patient Privacy Consents (BPPC) profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Actors can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. For more information visit www.ihe.net .
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 .



Standard Name	Description
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework Supplement 2008-2009 – Rosetta Terminology Mapping (RTM)	The Rosetta Terminology Mapping (RTM) profile is to harmonize the use of existing ISO/IEEE 11073-10101 nomenclature terms by systems compliant with IHE PCD profiles. The profile also specifies the correct units-of-measure and enumerated values permitted for each numeric parameter to facilitate safe and interoperable communication between devices and systems. The Rosetta Table also is designed to serve as a temporary repository that can be used to define new nomenclature terms that are currently not present in the ISO/IEEE 11073-10101 nomenclature. For more information visit www.ihe.net/Technical_Framework/index.cfm .
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework Year 1: 2006-2007 Volume 1 – Integration Profiles Volume 2 – Transactions	Defines and constrains HL7 V2.5 messaging for medical device data using the ISO/IEEE 11073-10101 Nomenclature standard and device data model based on ISO/IEEE 11073-10201 Domain Information Model. This profile is capable of representing data from simple devices (e.g. thermometers) to complex devices using in acute care settings (e.g. ventilators, infusion pumps) that could also be used in step-down and home care settings. For more information visit www.ihe.net/Technical_Framework/index.cfm .
International Classification of Functioning, Disability and Health (ICF)	The International Classification of Functioning, Disability and Health, known more commonly as ICF, is a classification of health and health-related domains. These domains are classified from body, individual and societal perspectives by means of two lists: a list of body functions and structure, and a list of domains of activity and participation. Since an individual's functioning and disability occurs in a context, the ICF also includes a list of environmental factors. See www.who.int/classifications/icf/en/ .
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) ISO 3166-1	The International Standard for country codes. The purpose of ISO 3166 is to establish codes for the representation of names of countries, territories or areas of geographical interest, and their subdivisions.
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) #1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. For more information visit www.ietf.org .
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) #2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit www.ietf.org .
Internet Society – Tags for Identifying Languages - 2005	This document describes the structure, content, construction, and semantics of language tags for use in cases where it is desirable to indicate the language used in an information object. It also describes how to register values for use in language tags and the creation of user-defined extensions for private interchange. This document, in combination with RFC 4647, replaces RFC 3066, which replaced RFC 1766. For more information visit www.ietf.org/rfc/rfc4646.txt .
ISO/IEC and ITU-T standard X.680: Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation	Standard notation for the representation of data types and values that does not constrain the way the information is transmitted.



Standard Name	Description
ISO/IEC and ITU-T standard X.693 – Information Technology – ASN.1 Encoding Rules: XML Encoding Rules (XER)	Specifies XML Encoding Rules (XER) as a set of ASN.1 encoding rules for producing an XML -based verbose textual transfer syntax for data structures described in ASN.1. For more information visit en.wikipedia.org/wiki/ASN.1 and en.wikipedia.org/wiki/XML_Encoding_Rules
ISO/IEC and ITU-T standard X.693 – Information Technology – ASN.1 Encoding Rules: XML Encoding Rules (XER)	Encoding rules which generate an XML document compliant with W3C XML 1.0.
ISO/IEEE 11073-10101:2004(E) Health informatics — Point-of-care medical device communication — Part 10101: Nomenclature, First Edition.	Covers nomenclature architecture for point-of-care (POC) medical device communication (MDC). It defines the overall architecture of the organization and relationships among nomenclature components and provides specifications of semantics and syntaxes. It is intended for use within the context of IEEE Std 1073,1 which sets out the relationship between this and other documents in the POC MDC series. For more information visit www.iso.org/iso/home.htm .
ISO/IEEE 11073-10201:2004(E) Health informatics — Point-of-care medical device communication — Domain information model	Within the context of the ISO/IEEE 11073 family of standards, this standard addresses the definition and structuring of information that is communicated or referred to in communication between application entities. This standard provides a common representation of all application entities present in the application processes within the various devices independent of the syntax. The definition of association control and lower layer communication is outside the scope of this standard. For more information visit www.iso.org/iso/home.htm .
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 Cancer Institute (NCI) Thesaurus: Route of Administration	Route of Administration is the path by which a particular drug product is introduced on or into the body. The medication terminology is maintained by the NCI Thesaurus, a reference terminology and biomedical ontology used in a growing number of NCI and other systems. It covers vocabulary for clinical care, translational and basic research, and public information and administrative activities. The NCI Thesaurus provides definitions, synonyms, and other information on nearly 10,000 cancers and related diseases, 8,000 single agents and combination therapies, and a wide range of other topics related to cancer and biomedical research. It is part of the Federal Medication Terminologies. For more information visit www.cancer.gov .
National Center for Biotechnology Information (NCBI) - Genetic Reference Sequences	Established in 1988 as a national resource for molecular biology information, NCBI creates public databases, conducts research in computational biology, develops software tools for analyzing genome data, and disseminates biomedical information - all for the better understanding of molecular processes affecting human health and disease. The Entrez Nucleotide database is a collection of sequences from several sources, including GenBank, RefSeq, and PDB. The number of bases in these databases continues to grow at an exponential rate. For more information visit www.ncbi.nlm.nih.gov .
National Center for Biotechnology Information (NCBI) - Single Nucleotide Polymorphisms	Established in 1988 as a national resource for molecular biology information, NCBI creates public databases, conducts research in computational biology, develops software tools for analyzing genome data, and disseminates biomedical information - all for the better understanding of molecular processes affecting human health and disease. A key aspect of research in genetics is associating sequence variations with heritable phenotypes. The most common variations are single nucleotide polymorphisms (SNPs), which occur approximately once every 100 to 300 bases. For more information visit www.ncbi.nlm.nih.gov .



Standard Name	Description
National Council for Prescription Drug Programs (NCPDP) Formulary and Benefits Standard Implementation Guide	Provides a standard means for pharmacy benefit payers (including health plans and Pharmacy Benefit Managers) to communicate formulary and benefit information to prescribers via technology vendor systems. The service enables technology vendors to receive a range of formulary and benefit information through the service: formulary status, preferred alternatives, benefit coverage and copay information. For more information visit www.ncdp.org .
National Council for Prescription Drug Programs (NCPDP) Telecommunication Standard Implementation Guide Version 5.1	Provides prescription claim transactions between Providers and Adjudicators, and between Adjudicators (aka Payer-to-Payer). The Telecommunication Standard Implementation Guide supports the following processes: <ol style="list-style-type: none"> 1. Eligibility Verification 2. Claim 3. Service 4. Information Reporting 5. Prior Authorization 6. Predetermination of Benefits For more information visit www.ncdp.org . Version 5.1 of this document was named in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. It should be noted that the industry has requested Version D.0 for use in the next round of HIPAA
National Uniform Billing Committee (NUBC) Uniform Bill Version 2007 (UB-04) 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) 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 .
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 .
U.S. National Uniform Claims Committee Health Care Provider Taxonomy Code Set	The Health Care Provider Taxonomy code set is a collection of unique alphanumeric codes, ten characters in length. The Health Care Provider Taxonomy code set includes specialty categories for individuals, groups of individuals, and non-individuals. The National Uniform Claims Committee maintains this code set. The complete code set is available from the Washington Publishing Company at www.wpc-edi.com .
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 .



Standard Name	Description
United States Postal Service (USPS) – Postal Codes	List of United States postal codes (known in various countries as a post code, postcode, or ZIP code) appended to a postal address for the purpose of sorting mail. For more information visit www.usps.com .

6.2 USE CASE TO INFORMATION EXCHANGE AND DATA REQUIREMENTS

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

Key:

Considered out of scope – no interoperability requirements

Considered out of scope – as described in Section 3.1

Table 6.2-1 Mapping of Use Case Actions to Information Exchange Requirements

Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
Remote Monitoring: 7.1 Clinician – 1.Communication of Remote Monitoring Information to EHR or PHR			
7.1.1 Evaluate patient and order remote monitoring			
	7.1.1.1 Evaluate patient and order tests as appropriate	IER14 Send/receive health plan eligibility	DR06 Health Plan Eligibility Information
	7.1.1.2 Recommend remote monitoring	IER15 Send/receive health plan authorization	DR38 Health plan authorization
	7.1.1.3 Clinician orders remote monitoring	IER36 Send/receive remote monitoring service order	DR39 Remote Monitoring Services Order
	7.1.1.3 a Patient enrolls in remote monitoring or disease management program	Workflow: no applicable interoperability requirements.	



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.1.1.3b Patient self-initiates remote monitoring	Workflow: no applicable interoperability requirements	
7.1.2 Set up ability to receive remote monitoring summary			
	7.1.2.1 Clinician performs set-up required to accept patient remote monitoring information within the clinician's EHR	EHR system internal capability. No Interoperability requirement	
	7.1.2.1a Clinician receives notification of a patient request to send remote monitoring information to the clinician's EHR.	Workflow- no applicable interoperability requirements. Notification directed from the patient to the clinician is not considered to be a valid work step in the setup of remote monitoring service	
7.1.3 Receive remote monitoring summary		See Figure 7-1, System Data Exchange #4 or #3 and #5	



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.1.3.1 Remote monitoring information is communicated to the clinician's EHR	<p>As highlighted in the High-Level Business Diagram 2.2.4-1, system data exchanges between the Remote Monitoring Management System and EHR system may be Point-to-point:</p> <p>IER10 Identify patient</p> <p>IER2 Send data over secured communication channel</p> <p>IER3 Create audit log entry</p> <p>IER4 Synchronize system time</p> <p>IER5 Consent Mgt and Access Control</p> <p>IER18 Send/receive clinical document</p> <ul style="list-style-type: none"> Through an HIE where other information may also be shared (e.g., registration, medication, laboratory results) <p>IER61: Provide and Register Document Set</p> <p>IER10: Identify patient</p> <p>IER2: Send data over secured communication channel</p> <p>IER3: Create audit log entry</p> <p>IER4: Synchronize system time</p> <p>IER5: Consent Mgt and Access Control</p> <p>IER38: Query/Retrieve Document Set</p> <ul style="list-style-type: none"> No external interaction if both business actors are combined into a single real world system 	<p>DR30 Identification/ Remote Monitoring Registration Data</p> <p>DR80 thru DR92 - Physiological Measurement Data</p> <p>DR93 thru DR95 - Medication Management and Administration Data</p> <p>DR96 - Patient Sensor Monitoring Data</p> <p>DR97 thru DR99 - Device and Measurement Descriptive Data</p> <p>DR35 Free text Notes</p> <p>DR36 Care Coordination Notes</p> <p>DR37 Alerts, Alarms and Notices</p>
	7.1.3.2 Clinician reviews remote monitoring information within the EHR	EHR system internal capability. No Interoperability requirement	
7.1.4 Evaluate/manage patient			
	7.1.4.1 The clinician may recommend patient follow-up based upon remote information received	<p>EHR functionality - no applicable interoperability requirements.</p> <p>Note: If a change to the care management plan or a transfer of care is deemed appropriate, this would be covered in the Consultation & Transfer of Care Use Case</p>	
	7.1.4.2 The clinician evaluates the patient	Workflow - no applicable interoperability requirements	
7.1.5 Modify treatment plan and communicate			



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
with patient			
	7.1.5.1 The clinician modifies the patient's treatment plan if required	If an additional device or an extension of the remote monitoring period is deemed necessary, request health plan authorization for change in/augmentation of patient care plan for remote monitoring services: IER14 Send/receive health plan eligibility IER15 Send/receive health plan authorization	
	7.1.5.2 The clinician communicates a change in care plan to the patient and other information recipients	IER24 Communication of a Structured Treatment Plan and Revisions Thereof	DR40 Structured Treatment Plan
Remote Monitoring: 7.2 Care Coordinator – 1. Communication of Remote Monitoring Information to EHR or PHR			
7.2.1 Initiate remote monitoring and coordinate with patient		Device Data necessary for the EHR is typically aggregated/summarized prior to being sent to EHR/PHR by the Care Coordinator using the Remote Monitoring Mgmt System (see Data Requirements Table 2.2.2-1)	
	7.2.1.1 Initiate remote monitoring for the patient	IER14 Send/receive health plan eligibility IER15 Send/receive health plan authorization	DR06: Health Plan Eligibility Information DR38: Health Plan Authorization
	7.2.1.2 Coordinate with patient to set up remote monitoring.	Workflow: no applicable interoperability requirements	
	7.2.1.3 Set up remote monitoring information recipients	System Intermediary Set-up: Data must only be provided to Authorized users (use of an authenticated and secured channel-see IER2)	
7.2.2 Access or receive monitoring information		IER39 Send/receive device observation data IER2 Send data over secured communication channel IER3 Create audit log entry IER4 Synchronize system time IER5 (in some configurations) Consent Mgt and Access Control	DR30 Identification/ Remote Monitoring Registration Data DR80 thru DR92 Physiological Measurement Data DR93 thru DR95 Medication Management and Administration Data DR96 Patient Sensor Monitoring Data DR97 thru DR99 Device and



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
		<p>See Figure 7-1, System Data Exchange #2</p> <p>Note that this System Data Exchange has been specified to meet the following requirements:</p> <ol style="list-style-type: none"> 1) Shall support conventional networks (e.g., POTS, Cable, DSL, GPRS, CDMA) 2) Must support "always on" (e.g., Internet) and "intermittent" connections (e.g., POTS) 3) Shall support conventional Device Intermediaries (e.g., Cell Phone, PC, Set Top Boxes, PDA) 4) Device data values shall not be modified. There needs to be a sufficient data integrity (i.e., must not be altered or destroyed either by attack or accident while in transmission) 5) A tamper-resistant audit log file should record security-relevant actions 6) A mechanism must be provided to synchronize clocks with the Remote Monitoring Mgmt System 7) Sufficient Security/Privacy based on a reasonable level of risk 8) Transport sessions must be initiated from within the home or from the patient-side device 9) Message size should be reasonable (but not minimized more than less compression) due to bandwidth limitation and/or transmission cost 	<p>Measurement Descriptive Data</p> <p>DR35 Free text Notes</p> <p>DR36 Care Coordination Notes</p> <p>DR37 Alerts, Alarms and Notices</p>
	7.2.2.1 The care coordinator reviews a patient's remote monitoring information via information intermediary	EHR system internal capability. No Interoperability requirement	
	7.2.2.1a The care coordinator may receive remote monitoring information within an EHR	EHR capability (see High-Level Diagram for architectural variants combining business actors)	
7.2.3 Determine if clinician intervention is needed			



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.2.3.1 The care coordinator may contact a clinician if needed	Workflow: no applicable interoperability requirements	
7.2.4 Determine if patient communication is needed			
	7.2.4.1 The care coordinator may communicate with the patient to verify remote monitoring information received or discuss care management details	Workflow: no applicable interoperability requirements for this Use Case (Communication with patient may be performed through direct conversations or by use of the patient Provider Secure Messaging HITSP Interoperability Specification)	
7.2.5 Communicate monitoring information		Use Case Figure 7-1, System Data Exchange #4 or #3 and #5	
	7.2.5.1 Care coordinator documents summary of clinician and/or patient interaction	IER10 Identify patient IER2 Send data over secured communication channel IER3 Create audit log entry IER4 Synchronize system time IER5 Consent Mgt and Access Control IER61 Provide and Register Document Set IER38 Query/Retrieve Document Set IER18 Send/receive clinical document	DR36 Care Coordination Notes
	7.2.5.2 Care coordinator communicates remote monitoring information and assessment information to the clinician	IER10 Identify patient IER2 Send data over secured communication channel IER3 Create audit log entry IER4 Synchronize system time IER5 Consent Mgt and Access Control IER61 Provide and Register Document Set IER38 Query/Retrieve Document Set IER18 Send/receive clinical document	DR30 Identification/ Remote Monitoring Registration Data DR80 thru DR92 Physiological Measurement Data DR93 thru DR95 Medication Management and Administration Data DR96 Patient Sensor Monitoring Data DR97 thru DR99 Device and Measurement Descriptive Data DR35 Free text Notes DR36 Care Coordination Notes DR37 Alerts, Alarms and Notices



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
	7.2.5.2a Care coordinator reviews remote monitoring information within the EHR and notifies the clinician	EHR capability (See High-Level Diagram for architectural variants combining business actors)	
Remote Monitoring: 7.3 Patient – 1. Communication of Remote Monitoring Information to EHR or PHR			
7.3.1 Obtain and set up device for remote monitoring		Use Case Figure 7-1, Flow 1 In the case of home devices, such a “Personal Area Network” device interface is out of scope of the Use Case and is expected to be covered in a later extension to this Interoperability Specifications (it is likely to be compatible with the Continua Health Alliance Implementation Guidelines and other specifications for clinical devices)	
	7.3.1.1 Patient obtains remote monitoring device	Workflow: no applicable interoperability requirements	
	7.3.1.2 Patient completes education on device use	Workflow: no applicable interoperability requirements	
	7.3.1.3 Patient sets up the device to communicate measurement information to clinicians and/or care coordinators	INTERFACE #1 Devices shall be either pre-paired or discoverable. In this IS, the device is considered to be integral part of the Device Intermediary. The pairing with the Device Intermediary is per the directions in the Use Case out of scope of this IS. It is may be addressed as an extension in a later version	
7.3.2 Utilize device to obtain measurements			
	7.3.2.1 Patient utilizes the device to obtain measurements as directed by his/her clinician or care coordinator	Internal operation of the device/device intermediary	



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
7.3.3 Transmit monitoring data from device		Use Case Figure 7-1, System Data Exchange 1	
	7.3.3.1 Patient measurements are communicated to the information intermediary.	INTERFACE #1 Internal operation of the device intermediary. In the context of the Use Case, it is out of scope	
7.3.4 Receive remote monitoring data		Use Case Figure 7-1, System Data Exchange 6 or 3 and 7.	
	7.3.4.1 Remote monitoring information is communicated to the patient's PHR	<p>As highlighted in the high-level business diagram 2.2.4-1, system data exchanges between the Remote Monitoring Management System and PHR system may be Point-to-Point:</p> <p>IER10 Identify patient IER2 Send data over secured communication channel IER3 Create audit log entry IER4 Synchronize system time IER5 Consent Mgt and Access Control IER18 Send/receive clinical document</p> <ul style="list-style-type: none"> Through an HIE where other information may also be shared (e.g., registration, medication, laboratory results): <p>IER61 Provide and Register Document Set IER10 Identify patient IER2 Send data over secured communication channel IER3 Create audit log entry IER4 Synchronize system time IER5:Consent Mgt and Access Control IER38 Query/Retrieve Document Set</p> <ul style="list-style-type: none"> No external interaction if both business actors are combined into a single real world system <p>The Remote Monitoring Management System to PHR interactions may require standards that are not currently available and may not be included in 2008 version of this IS</p>	<p>DR30 Identification/ Remote Monitoring Registration Data DR80 thru DR92 Physiological Measurement Data DR93 thru DR95 Medication Management and Administration Data DR96 Patient Sensor Monitoring Data DR97 thru DR99 Device and Measurement Descriptive Data DR35 Free text Notes DR36 Care Coordination Notes DR37 Alerts, Alarms and Notices</p>
	7.3.4.2 Patient reviews remote monitoring information within the PHR	PHR system internal capability. No Interoperability requirement	



Event	Action	Information Exchange Requirement(s) (includes security requirements)	Data Requirements
7.3.5 Patient modifies meds, dosage, activities, diet, etc.			
	7.3.5.1 Patient self-manages chronic disease or wellness care based upon measurement values	Self-Coordination: no applicable interoperability requirements	
	7.3.5.2 The patient may be contacted by a coordinator to review or modify care management activities	Person-to-person out of band communication: no applicable interoperability requirements	
7.3.6 Patient discusses treatment plan with clinician			
	7.3.6.1 Patient discusses treatment or management with their clinician	Workflow: no applicable interoperability requirements	
	7.3.6.2 Patient accesses modified treatment plan information provided by a personal clinician	IER24 Communication of a Structured Treatment Plan and Revisions Thereof	DR40 Structured Treatment Plan
	7.3.6.3 Patient implements modified treatment plan and continues remote monitoring participation as directed	Device/Device Intermediary internal functionality: no applicable interoperability requirements	



6.3 USE CASE SEQUENCE DIAGRAMS

The high level sequence diagrams illustrate each Use Case scenario with a representation of a normal sequence of exchange between the primary actors. The event codes from the Use Case are annotated on the diagrams to show how the interactions relate to the Use Case. The interactions are supported by the various constructs which will be introduced in Section 3.0 of this Interoperability Specification.

Figure 6.3-1 Evaluate Patient and Order Remote Monitoring

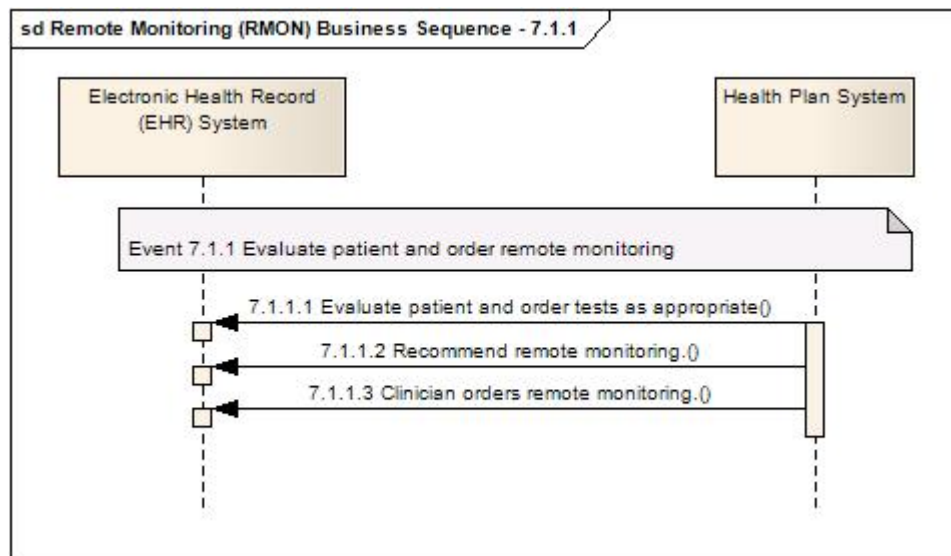


Figure 6.3-2 Setup and Receive Remote Monitoring Summary

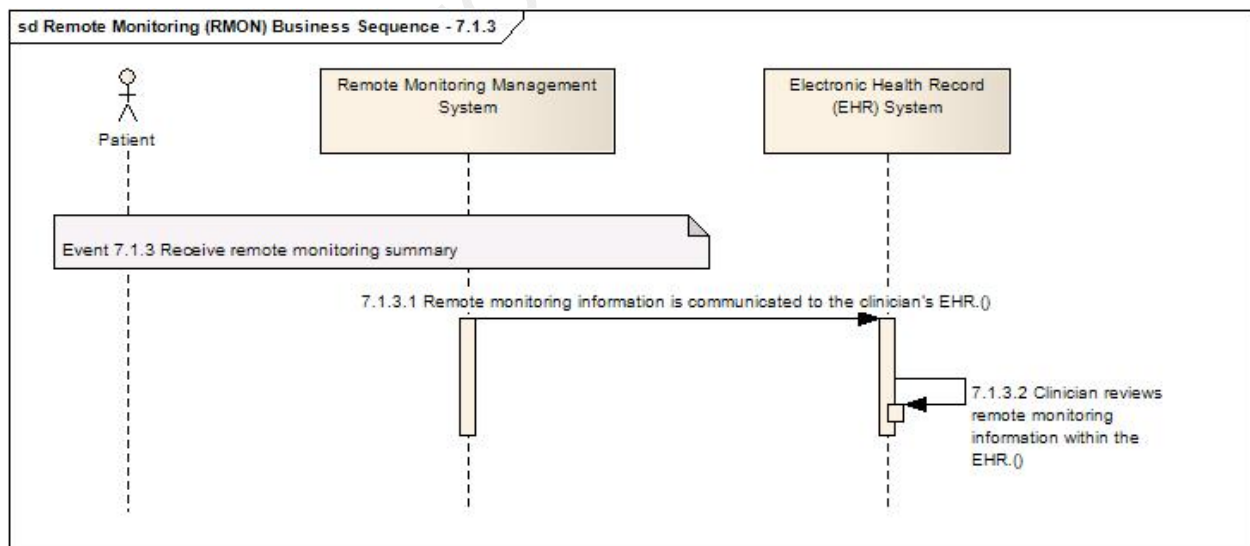


Figure 6.3-3 Evaluate/Manage Patient, and Modify Treatment Plan & Communicate with Patient

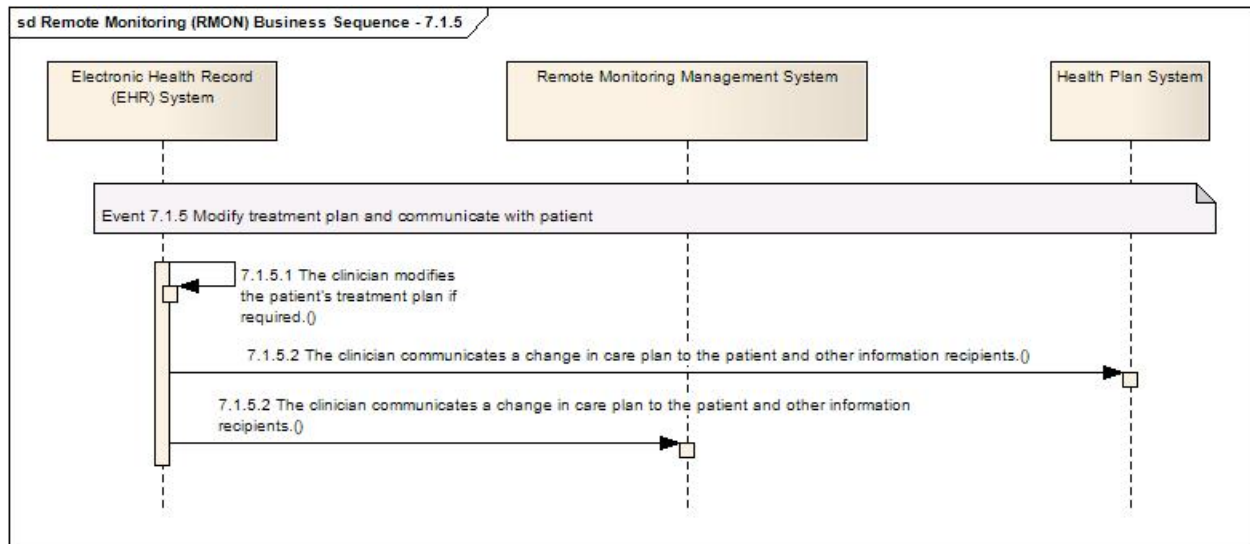


Figure 6.3-4 Initiate Remote Monitoring and Coordinate with Patient

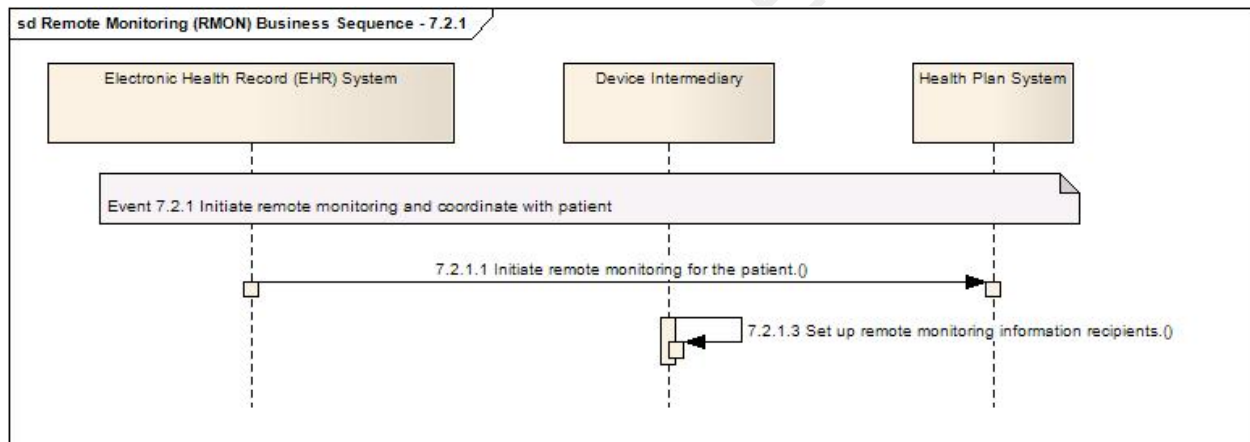


Figure 6.3-5 Receive Remote Monitoring Data, and Utilize Device to Obtain Measurements

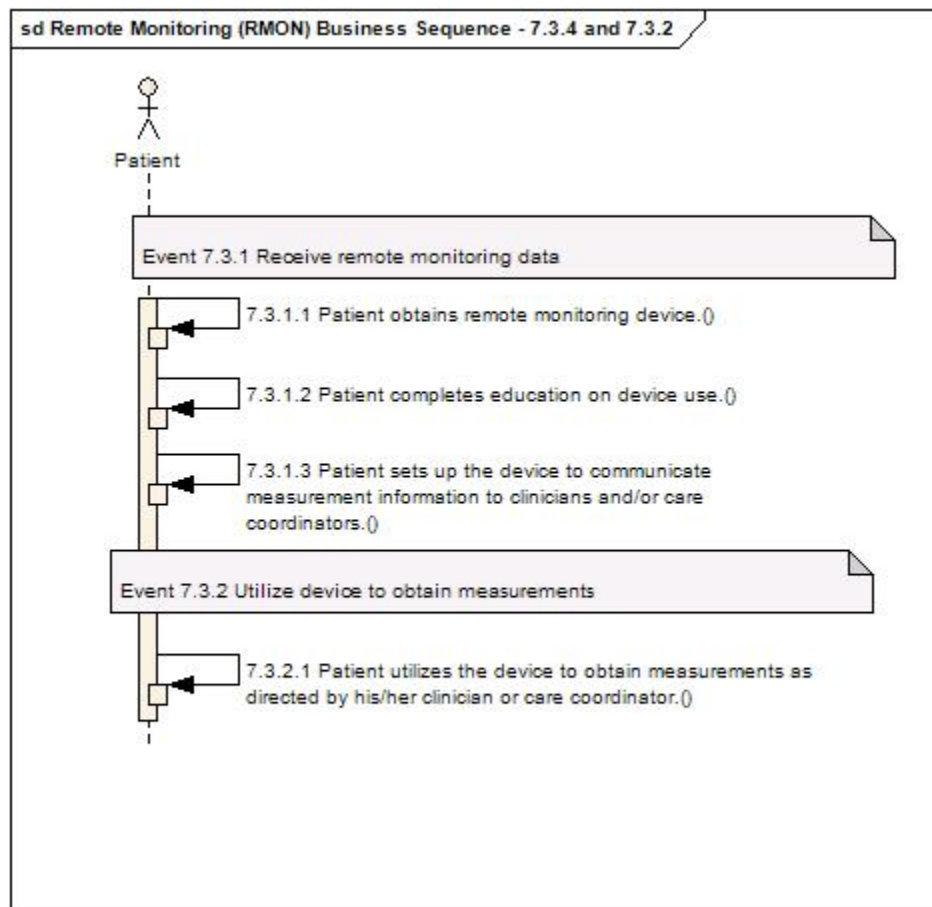
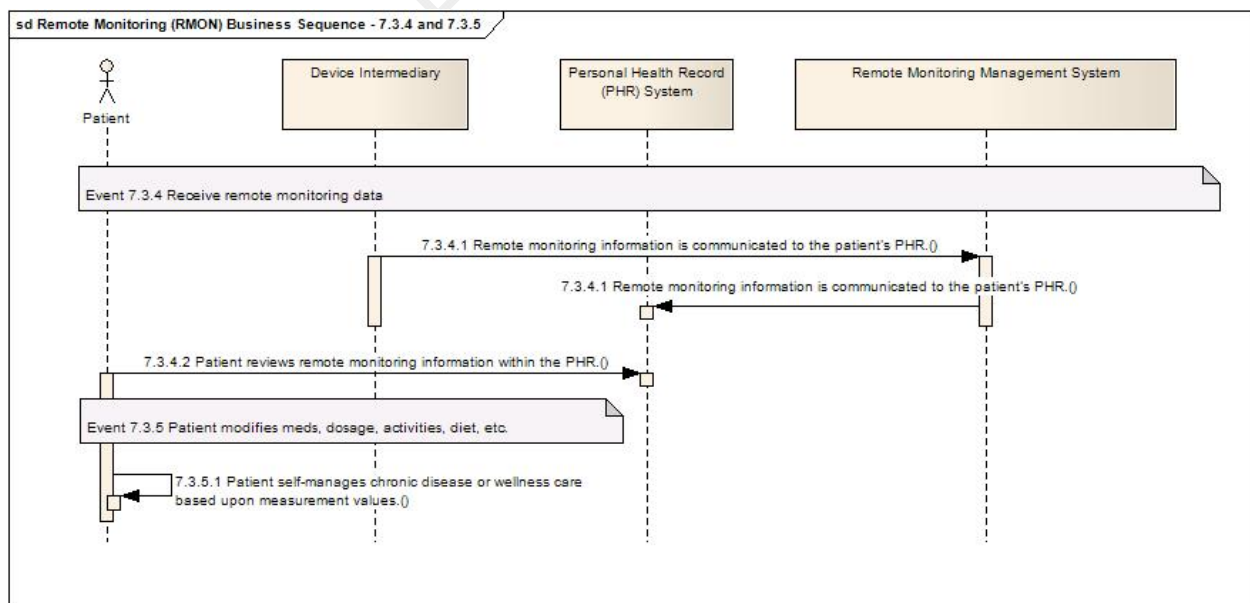


Figure 6.3-6 Receive Remote Monitoring Data, and Patient Modifies Meds, Dosage, Activities, Diet, etc.



=



6.4 MAPPING OF CONSTRUCTS TO INFORMATION EXCHANGE AND DATA REQUIREMENTS

Table 6.4-1 below provides a mapping of the HITSP constructs that will be used in the design of the Interoperability Specification, and the data and information exchange requirements that are being satisfied by the construct. These requirements are limited to those that are deemed within scope for this Table, which are described in Section 3.1.

Table 6.4-1 Mapping of Requirements to HITSP Constructs

Construct Name	Information Exchange Requirement Number (IER#)	Data Requirement Number (DR#)
HITSP/TP13- Manage Sharing of Documents	IER61, IER38	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36
HITSP/T15 - Collect and Communicate Security Audit Trail	IER03	
HITSP/T16 - Consistent Time	IER04	
HITSP/T17 - Secured Communication Channel	IER02	
HITSP/C19 - Entity Identity Assertion	IER01, IER05	
HITSP/TP20 - Access Control	IER01, IER05	DR74
HITSP/TP22 - Patient ID Cross-Referencing	IER10	
HITSP/T23 - Patient Demographics Query	IER10	
HITSP/TP30 - Manage Consent Directives	IER01, IER05	
HITSP/T31 - Document Reliable Interchange	IER61	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36,
HITSP/T40 - Patient Generic Health Plan Eligibility Verification	IER14	DR38
HITSP/TP46 - Medication Formulary and Benefits Information	IER14, IER15	DR06, DR38
HITSP/TP68 - Patient Health Plan Authorization Request and Response	IER15	DR38
HITSP/T73 - Aggregate Device Information Communication	IER39 (The nomenclatures for the DR requirements noted to the right have been concluded. See the note at the conclusion of this table for the agreed upon strategy to complete the solution for IER39)	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36
HITSP/C74 - Remote Monitoring Observation Document	IER61	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36
HITSP/T79 - Pharmacy to Health Plan Authorization Request and Response Transaction	IER15	DR38
HITSP/C80 - Clinical Document and Message Terminology	IER61	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36
HITSP/C83 - CDA Content Modules	IER61	DR30, DR80, DR81, DR89, DR91, DR92, DR97, DR35, DR36



Construct Name	Information Exchange Requirement Number (IER#)	Data Requirement Number (DR#)
HITSP/T85 - Administrative Transport to Health Plan	IER14,IER15	DR06, DR38

RELEASED FOR IMPLEMENTATION



7.0 CHANGE HISTORY

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

7.1 DECEMBER 10, 2008

The changes in this construct address the following comments received during the Public Comment and Inspection Testing period (September 29 – October 24, 2008).

4447, 5122, 5123, 5124, 5126, 5129, 5133, 5135, 5138, 5139, 5141, 5193, 5194, 5195, 5196, 5312, 5315, 5399, 5448, 5525, 5526, 5527, 5528, 5704, 5705, 5706, 5707, 5708, 5709, 5710, 5711, 5717, 5810, 5811, 5812, 5813, 5814, 5815, 5307, 5309, 5450, 5484

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

Minor editorial changes were made to this document.

7.2 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

