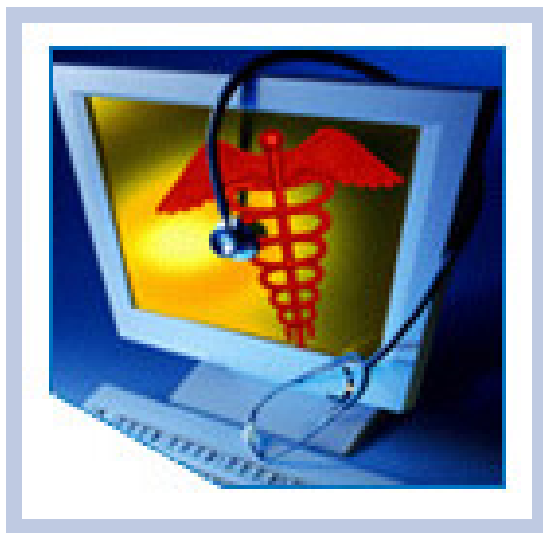


HITSP Remote Monitoring Use Case Requirements, Design and Standards Selection

HITSP/RDSS56



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

**Consumer Perspective Technical Committee
(Formerly Consumer Empowerment Technical Committee)**

With input from:

**Administrative and Financial Domain Technical Committee
Care Management and Health Records Domain Technical Committee
Security, Privacy and Infrastructure Domain Technical Committee (Formerly Security and Privacy Technical Committee)**



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Consumer Perspective Technical Committee With input from: Administrative and Financial Domain Technical Committee Care Management and Health Records Domain Technical Committee Security, Privacy and Infrastructure Domain Technical Committee (Formerly Security and Privacy Technical Committee)	June 27, 2008



TABLE OF CONTENTS

1.0	INTRODUCTION	6
1.1	Purpose	6
1.2	Audience.....	6
1.3	How to Use this Requirements, Design and Standards Selection Document.....	6
1.3.1	Conventions, Acronyms and Resources/References.....	7
1.4	Copyright Permissions.....	7
2.0	REQUIREMENTS ANALYSIS	9
2.1	Use Case Synopsis	9
2.2	Use Case Requirements	11
2.2.1	Mapping of Use Case Requirements to Interoperability Requirements	11
2.2.2	Data and information Requirements Matrix.....	23
2.2.3	Identification of Business Actors, and Scenarios	25
2.2.4	High-Level UML Business Sequence Diagram	26
3.0	DESIGN.....	34
3.1	Scope of Design	34
3.1.1	Assumptions	36
3.1.2	Constraints	36
3.1.3	Pre-conditions.....	37
3.1.4	Post-conditions	37
3.1.5	Process Triggers	38
3.2	Detailed Design	38
3.2.1	Technical Actor Role Descriptions	40
3.2.2	Sequence Diagram for Process Flow	42
3.2.3	Mapping of Business Actors to Technical Actors and Constructs with optionality	43
3.2.4	Data Detail.....	49
3.2.5	New HITSP Constructs.....	49
3.2.6	Modifications to Existing HITSP Constructs	50
3.2.7	Document Map	54
4.0	CANDIDATE STANDARDS.....	56
4.1	List of Selected and Candidate Standards	56
4.1.1	Regulatory and Guidance Standards	57
4.1.2	Selected and Candidate Standards.....	57
4.2	Gaps Where There Are No Standards	58
4.3	Standard Overlaps.....	59



5.0	NEXT STEPS	60
6.0	APPENDIX	61
6.1	Description of Standards	61
7.0	CHANGE HISTORY	63



FIGURES AND TABLES

Figure 2.2.4-1 Business System Interfaces	27
Figure 2.2.4-2 Business Sequence Diagram – 7.1.1	28
Figure 2.2.4-2 Business Sequence Diagram – 7.1.2 and 7.1.3	28
Figure 2.2.4-2 Business Sequence Diagram – 7.1.4 and 7.1.5	29
Figure 2.2.4-2 Business Sequence Diagram – 7.2.1	29
Figure 2.2.4-2 Business Sequence Diagram – 7.2.2 and 7.2.3	30
Figure 2.2.4-2 Business Sequence Diagram – 7.2.4 and 7.2.5	30
Figure 2.2.4-2 Business Sequence Diagram – 7.3.4 and 7.3.2	31
Figure 2.2.4-2 Business Sequence Diagram – 7.3.4 and 7.3.5	32
Figure 2.2.4-2 Business Sequence Diagram – 7.3.6	33
Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1	43
Figure 3.2.7-1 Requirements, Design, and Standards Selection Document Map	55
Table 1.3.1-1 Reference Documents	7
Table 2.2.1-1 Mapping of Use Case Requirements to Interoperability Requirements	12
Table 2.2.2-1 Data Element and Information Requirements	23
Table 2.2.3-1 Business Actors	25
Table 3.1-1 Scoping Clarifications	34
Table 3.1.1-1 Assumptions	36
Table 3.1.2-1 Constraints	37
Table 3.1.3-1 Pre-conditions	37
Table 3.1.4-1 Post-conditions	37
Table 3.1.5-1 Process Triggers	38
Table 3.2.1-1 Technical Actor Role Descriptions	40
Table 3.2.3-1 Business-Technical Actor Mapping to Transaction and/or Content	44
Table 3.2.4-1 Data Element Constraints	49
Table 3.2.5-1 New HITSP Constructs	49
Table 3.2.6-1 Existing HITSP Constructs	50
Table 4.1.1-1 Regulatory and Guidance Standards	57
Table 4.1.2-1 Selected and Candidate Standards Linked to Requirements	58
Table 4.2-1 Use Case Events and Associated Gaps	59
Table 4.3-1 Standard Overlaps	59
Table 6.1-1 Description of Standards	61



1.0 INTRODUCTION

As an introduction to the HITSP Remote Monitoring Use Case Requirements, Design and Standards Selection, this section describes the purpose of the document, the intended audience for the technical content of the document, and how to use this document. It acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Requirements Analysis.

1.1 PURPOSE

The Requirements, Design and Standards Selection document is used to define the requirements for the Use Case and the detailed HITSP Interoperability Specification design map of existing standards and specifications that will be used to meet the stated requirements. It is intended to describe the process by which the Use Case was analyzed, standards were selected and the design was developed.

1.2 AUDIENCE

The Requirements, Design and Standards Selection document is designed to be used by the HITSP Technical Committees or Work Groups to document their analysis and decisions, other analysts who need to understand and evaluate the requirements, design and selected standards, and by those intending to test the resulting Interoperability Specifications against the Use Case requirements. Understanding and using the relevant set of Interoperability Specifications is a key requirement for establishing interoperability compliance.

1.3 HOW TO USE THIS REQUIREMENTS, DESIGN AND STANDARDS SELECTION DOCUMENT

The Requirements, Design and Standards Selection document is divided into five main related sections. Each section provides background information for the Interoperability Specification. Section 1.0 provides a brief introduction to the document. Users of this document who are familiar with the content may choose to proceed to Section 2.0. In Section 2.0, the Requirements Analysis provides a general overview of the Use Case and the specific requirements of the Use Case including a mapping of the Use Case requirements to the extracted interoperability requirements, the data requirements of the Use Case, and an identification of the scenarios, business actors, their interactions, and data elements used in those interactions. The design for the Interoperability Specification is provided in Section 3.0. This includes the scope of the design, mapping of interoperability requirements to the specific technical requirements, actor interactions and groupings, detailed descriptions of data used by the Use Case actors, and a description of existing or new HITSP constructs that will be used by the Interoperability Specification. Section 4.0 describes the Standards Selection process, provides a table of the selected and candidate standards, a Gaps and Overlaps discussion and plan for resolution. Section 5.0 describes the next steps in the HITSP standards harmonization process and Section 6.0 provides relevant appendix material.



1.3.1 CONVENTIONS, ACRONYMS AND RESOURCES/REFERENCES

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

Table 1.3.1-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
Remote Monitoring Detailed Use Case, March 21, 2008	AHIC Use Case that is the basis of this 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 glossary of terms used in all the Security and Privacy construct documents• A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment <p>HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.</p>

1.4 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.



NOTE: HITSP will work with the appropriate standards organizations to obtain applicable copyright information for candidate standards.



2.0 REQUIREMENTS ANALYSIS

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

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

2.1 USE CASE SYNOPSIS

This section provides a synopsis of the 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, may be a key enabler for the management of chronic health problems and initial management of new conditions. Remote monitoring may 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 may benefit from the ability for the patient to gather and communicate remote monitoring information electronically from measurement devices in the 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 ADL measurements (e.g., ADL biosensors, pedometers, sleep actigraphy)



- Clinicians, care managers, and disease management programs can benefit by being able to better manage patients with 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 measurements captured by remote monitoring devices can be communicated to PHRs for access by patients or family caregivers. The remote monitoring information can also be transmitted to clinicians and care managers to assist them in monitoring and managing their patients. In order for remote monitoring data captured from a patient's device to be available within a PHR or EHR, remote monitoring information must 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. The most 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. An information exchange may provide a mechanism for clinicians and care coordinators (such as case managers, physician office support personnel, clinical call centers, etc.) to access and review remote monitoring information and determine which information should be communicated to the clinician's EHR. An information exchange 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 other information exchange capabilities or health record banks. Lastly, a remote monitoring device may connect directly to an EHR or PHR via a point-to-point device interface, although this method is less prevalent in the market today. The Remote Monitoring Use Case focuses on the need to communicate information to the EHR or PHR specifically, not 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 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.

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 requirement of this Use Case.

With appropriate safeguards for patient privacy and security, 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 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 REQUIREMENTS TO INTEROPERABILITY REQUIREMENTS

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



Key:

Considered out of scope – no interoperability requirements

Considered out of scope – as described in Section 3.1

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

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
Remote Monitoring	7.1 Clinician [With clinician as actor, assumption is that 7.1.x is covering requirements for the Remote Monitoring Management System to the EHR- interfaces #4, and #3 & #5 in Figure 2.2.4-1]	1. Communication of Remote Monitoring Information to EHR or PHR	7.1.1 Evaluate patient and order remote monitoring		The Use Case does not present a holistic set of either the categories or specific types of remote monitoring datasets that need to be addressed. Instead it represents a compliment of data sets as a list of non- exhaustive examples of remote monitoring requirements. The general categories of data identified, typical examples of remote monitoring information for that category and specific elements associated with each of these examples are included in Table 2.2.2-1	#1 – Identification/ Remote Monitoring Registration Data #2 - Physiological Measurement Data #3 - Medication Management and Administration Data #4 - Activities of Daily Living Data #5 – Device and Measurement Descriptive Data #6 – Free-text Notes #7 – Care Coordination Notes #8 – Alerts, Alarms and Notices
				7.1.1.1 Evaluate patient and order tests as appropriate	Verify patient eligibility with health plan for remote monitoring services and equipment; Identify benefits, limits, exclusion, co-pay, deductible, patient responsibility	#10 - Eligibility Query Info
				7.1.1.2 Recommend remote monitoring	Request health plan authorization for remote monitoring equipment and services	#11 - Remote Monitoring Authorization Info
				7.1.1.3 Clinician orders remote monitoring	May not be included in 2008 version of this IS	
				7.1.1.3 a Patient enrolls in remote monitoring or disease management program	Remote Monitoring Management System should use an unambiguous Patient ID. The ID should be consistent/cross-referenced with the ordering physician's EHR	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
					[Note: HITSP constructs TP22, T23 might be considered for this.] Need to better understand the enrollment process and what entity performs the remote monitoring/disease mgmt program? More than just the patient inquiry will be required. It needs to be determined exactly what construct to use to send patient enrollment information	
				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	Notification directed from the patient to the clinician is not considered to be a valid work step in the setup of remote monitoring service. A CPTC-generated public comment will be posted against this RDSS to allow for further discussion by the CPTC membership to resolve. This will be made prior to the issuance of the IS	#9 – Remote Monitoring Notification Data
			7.1.3 Receive remote monitoring summary		Use Case Figure 7-1, Flow 4	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				7.1.3.1 Remote monitoring information is communicated to the clinician's EHR	<p>INTERFACE #4 (and INTERFACE #3+#5): The data transmitted from Remote Monitoring Management System to EHR system includes:</p> <ol style="list-style-type: none"> 1) Measurements captured by devices 2) Representation of notes, summary and other kinds of narrative information that may be added by care givers or by the user themselves; added by device intermediary that represent trends of user's health 3) Representation of graphs that may be. A distinction must be made between original device data and processed summary data 4) Must be able to update a previously submitted record 5) A unique patient ID (as defined in Setup above) must be associated with the device data 6) Descriptive Device data must be included (see Data Requirements Table) 7) A global unique document ID must be included 8) UCUM must be used for units of measure <p>[Note: It is recommended that the Data Content be compliant with HL7 SDTC PHM (CCD for personal health) profiled by Continua XHR interface Interoperability Guidelines.]</p> <p>As highlighted in the high- level business diagram 2.2.4- 1, interaction between the Remote Monitoring Management System and EHR system may be:</p> <ul style="list-style-type: none"> • Point-to-point [Interface #4] • Through an HIE where other information may also be shared (e.g., 	<p>#1 – Identification/ Remote Monitoring Registration Data #2 - Physiological Measurement Data #3 - Medication Management and Administration Data #4 - Activities of Daily Living Data #5 – Device and Measurement Descriptive Data #6 –Free-text Notes #7 – Care Coordination Notes #8 – Alerts, Alarms and Notices</p>



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
					<p>registration, medication, laboratory results) [Interface #3 + #5]. This should be implemented in a form consistent with the other HITSP ISs such as IS 01, IS 03, IS 04, IS 07</p> <ul style="list-style-type: none"> No external interaction if both business actors are combined into a single real world system <p>ALL INTERFACES:</p> <ul style="list-style-type: none"> All Store/Forward data must have Universal time stamps with a resolution of at least 1 second Sufficient security, authentication, and audit logging must be used [Note: It is recommended that the Data Transport be compliant with IHE XDR.b profiled by Continua XHR interface Interoperability Guidelines (e.g., use "online mode only)] Data must only be provided to Authorized users. [Note: It is recommended that HITSP constructs C19, C26, TP20 be considered] 	
				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	<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</p>	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				received	appropriate, this would be covered in the Consultation & Transfers of Care Use Case	
				7.1.4.2 The clinician evaluates the patient	Workflow - no applicable interoperability requirements	
			7.1.5 Modify treatment plan and communicate with patient		Use Case Figure 7-1, Flow 5 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 Transfers of Care Use Case	
				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. The clinician doing an eligibility check for the services deemed appropriate is required. Notify health plan authorization of reduction/curtailment of remote monitoring services	
				7.1.5.2 The clinician communicates a change in care plan to the patient and other information recipients	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 Transfers of Care Use Case	
Remote Monitoring	7.2 Care Coordinator [With Care Coordinator as actor, assumption is that 7.2.x is covering]	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 prior to being sent to the Care Coordinator using the Remote Monitoring Mgmt System (see Data Requirements Table 2.2.2-1)	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
	requirements for the Device Intermediary to Care Coordinator- interface #2, in Figure 2.2.4-1]			7.2.1.1 Initiate remote monitoring for the patient	<p>INTERFACE #2 : The data transmitted from the Device Intermediary to the Remote Monitoring Management System requires the following:</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 sufficient data integrity (i.e., must not be altered or destroyed either by attack or accident) 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 and 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 <p>ALL INTERFACES:</p> <ul style="list-style-type: none"> • All Store/Forward data must have Universal time stamps with a resolution of at least 1 second • Sufficient security, authentication, and audit logging must be used [Note: It is recommended 	<p>#1 – Identification/ Remote Monitoring Registration Data</p> <p>#2 - Physiological Measurement Data</p> <p>#3 - Medication Management and Administration Data</p> <p>#4 - Activities of Daily Living Data</p> <p>#5 – Device and Measurement Descriptive Data</p> <p>#6 – Free-text Notes</p> <p>#7 – Care Coordination Notes</p> <p>#8 – Alerts, Alarms and Notices</p>



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
					that the Data Transport be compliant with IHE XDR.b profiled by Continua XHR interface Interoperability Guidelines (e.g., use "online mode only") <ul style="list-style-type: none">Data must only be provided to Authorized users. [Note: It is recommended that HITSP constructs C19, C26, TP20 be considered]	
				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	Data must only be provided to Authorized users	
			7.2.2 Access or receive monitoring information		Use Case Figure 7-1, Flow 3 Data values must not be altered or destroyed either by attack or accident	
				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 system internal capability. No Interoperability requirement EHR capability (As per high-level diagram for architectural variants this combines the business actors of Remote Monitoring Management System (RMMS) and EHR)	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
			7.2.3 Determine if clinician intervention is needed			
				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	Document- based Care Coordination Notes may need to be shared with ordering clinician	#7 – Care Coordination Notes
			7.2.5 Communicate monitoring information		Use Case Figure 7-1, Flow 4	
				7.2.5.1 Care coordinator documents summary of clinician and/or patient interaction	Document-based Care Coordination Notes may need to be shared with ordering clinician	#7 – Care Coordination Notes
				7.2.5.2 Care coordinator communicates remote monitoring information and assessment information to the clinician	INTERFACE #4 (and INTERFACE #3+#5): The data transmitted from Remote Monitoring Management System to EHR system includes: 1) Measurements captured by devices 2) Representation of notes, summary and other kinds of narrative information that may be added by care givers or by	#1 – Identification/ Remote Monitoring Registration Data #2 - Physiological Measurement Data #3 - Medication Management and Administration Data #4 - Activities of



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
					<p>the user themselves; added by device intermediary that represent trends of user's health</p> <p>3) Representation of graphs that may be a distinction, must be made between original device data and processed summary data</p> <p>4) Must be able to update a previously submitted record</p> <p>5) A unique patient ID (as defined in Setup above) must associated with the device data</p> <p>6) Descriptive device data must be included (see Data Requirements Table)</p> <p>7) A global unique document ID must be included</p> <p>8) UCUM must be used for units of measure</p> <p>[Note: It is recommended that the Data Content be compliant with HL7 SDTC PHM (CCD for personal healthcare) profiled by Continua XHR interface Interoperability Guidelines]</p> <p>A Free Text Notes section must also be available in addition to device data and formal clinical documents</p>	<p>Daily Living Data</p> <p>#5 – Device and Measurement Descriptive Data</p> <p>#6 – Free-text Notes</p> <p>#7 – Care Coordination Notes</p> <p>#8 – Alerts, Alarms and Notices</p>
				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 [With patient as actor, assumption is that 7.3.x is covering requirements for the Device	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 This "Personal Area Network" device interface is out of scope of the Use Case and needs to be covered elsewhere (i.e., Continua Guidelines) and will not be explicitly called. [It is	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
	to the Device Intermediary- interface #1]				recommended that HITSP point to these to ensure industry alignment]	
				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. 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 and is out of scope of this RDSS	
			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	
			7.3.3 Transmit monitoring data from device		Use Case Figure 7-1, Flow 2	
				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, Flow 3	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				7.3.4.1 Remote monitoring information is communicated to the patient's PHR	INTERFACES #6 and INTERFACES [#3 + #7] 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	
				7.3.4.2 Patient reviews remote monitoring information within the PHR	PHR system internal capability. No Interoperability requirement	
			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		Use Case Figure 7-1, Flow 5 Workflow- no applicable interoperability requirements. Actions regarding treatment plan decisions are specifically described in the Consultation and Transfers of Care Use Case	
				7.3.6.1 Patient discusses treatment or management with their clinician	Workflow - no applicable interoperability requirements	



Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s) (includes security requirements)	Data Requirement Number
				7.3.6.2 Patient accesses modified treatment plan information provided by a personal clinician	The communication of structured treatment plans in a standardized format requires further standards development. The requirements in this regard are expected to be included in the Consultation and Transfers of Care Use Case As a result, this requirement is considered out-of-scope for the Remote Monitoring Use Case	
				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	

2.2.2 DATA AND INFORMATION REQUIREMENTS MATRIX

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

Table 2.2.2-1 Data Element and Information Requirements

Requirement Number	Description	
Data Requirement #1	Identification/Remote Monitoring Registration Data	Patient ID, Provider ID, Device ID (Device Type, Brand, Serial Number), Other Identifying Information – Case Manager, Other Identifying Information – Device Manufacturer or Intermediary, Data Recipient(s) ID
Data Requirement #2	Physiological Measurement Data	
	2.1 Blood Glucose Meter [see IEEE P11073-10417™ Dev specialization – Glucose meter or similar]	Glucose Level, Blood Glucose Level, Glucose Control Measurement, Interstitial Fluid Glucose Level, Sample Location, Measurement Condition, Tester, Meter event
	2.2 Blood Pressure Monitor [see IEEE P11073-10407™ Dev specialization – Blood pressure monitor or similar]	Systolic Pressure, Diastolic Pressure, Mean Aerial Pressure, Pulse
	2.3 Brain Activity	Ambulatory EEG
	2.4 Cholesterol	



Requirement Number	Description	
	2.5 Esophageal pH	
	2.6 Heart Rate	
	2.7 Heart Rhythm	AECG, Holter Monitor, Cardiac Implants
	2.8 Implantable Cardioverter Defibrillator (ICD) Monitoring	Inter cardiac Pressure, Intrathoracic Fluid, EGM Waveforms
	2.9 Lung Function	FEV1, FVC, PEV
	2.10 Oxygen Saturation (Pulse Oximeter) [see IEEE P11073-10404™ Dev specialization – Pulse oximeter]	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
	2.11 Respiration Rhythm	
	2.12 Temperature (Thermometer) [see IEEE P11073-10408™ Dev specialization – Thermometer]	Temperature
	2.13 Weight (Weighing Scale) [see IEEE P11073-10415™ Dev specialization – Weighing scale]	Body Weight, Body Height, Body Mass Index
Data Requirement #3	Medication Management and Administration Data	
	3.1 Electronic Pillbox	Patient Alerts and Medication Administration Tracking
	3.2 Medication Pumps	Medication Administration
	3.3 Medication Infusion Devices	Medication Administration
Data Requirement #4	Activities of Daily Living (ADL) Data	ADL Biosensors and Detection Devices, Emergency Alerting [with Global Positioning System (GPS)], Fall Detection, Pedometer (Steps Moved), Sleep Actigraphy
Data Requirement #5	Device and Measurement Descriptive Data	
	5.1 Generic Device Data [See IEEE P11073-20601™ Optimized exchange protocol]	Manufacturer, Device ID, Serial #, Type, Model #, FW Version #, HW Version #, Time Accuracy, Measurement Accuracy, Regulatory Info, Etc.
	5.2 Measurement Descriptive Data	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
	5.3 Measurement Error Data	Device Malfunction, User Error During Measurement, Measurement Cancelled by Patient (Stopped measurement process or marked measurement as invalid)
Data Requirement #6	Free Text Notes (e.g., Patient-entered Measurement Instance Specific Details)	Free text, Language, Max length (are there constraints that need to be considered with different message specs, e.g. CDA)
Data Requirement #7	Care Coordination Notes	Clinical Document (e.g., Care Coordinator Reason for Referral/Summary, Care Management Program Notification, Care Manager to Clinician Summary)



Requirement Number	Description	
Data Requirement #8	Alerts, Alarms and Notices	Normal Range, Normal Range for Patient, Alert (Low Value, High Value, Change in Trend); including evidentiary numeric, waveform and annotation data to validate alarm
Data Requirement #9	Remote Monitoring Notification Data (see Note in Table 2.2.1-1, Action 7.1.2.1a)	Patient ID, other elements TBD
Data Requirement #10	Eligibility Query Information Note: Potential for leveraging HITSP/T40 for this purpose	Identify benefits, limits, exclusion, co-pay, deductible, patient responsibility and other elements TBD
Data Requirement #11	Remote Monitoring Authorization Information	TBD

2.2.3 IDENTIFICATION OF BUSINESS ACTORS, AND SCENARIOS

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

Table 2.2.3-1 Business Actors

Business Actor	Description	Use Case Scenario
Device Intermediary	A system that supports one or more devices that provide measurements from a patient under remote monitoring and feeds this captured measurements to a care management system	Communication of Remote Monitoring Information to EHR or PHR
EHR System	The Electronic Health Record (EHR) System is a secure, real-time, point-of-care, patient-centric information resource for clinicians	Communication of Remote Monitoring Information to EHR or PHR
PHR System	The system that supplies the Personal Health Record (PHR), a secure, real-time, point-of-care, person-centric information resource, for consumers (including health record banks)	Communication of Remote Monitoring Information to EHR or PHR
Health Information Exchange	A Health Information Exchange (HIE) 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	Communication of Remote Monitoring Information to EHR or PHR



Business Actor	Description	Use Case Scenario
Health Plan Payment Authorization System	The system which holds and maintains the information regarding the individual's insurance requirements related to an authorization for benefit coverage determination and reimbursement purposes when a patient is referred for care or services, and responds to the query initiated by the Authorization Information Receiver	
Healthcare Services Eligibility System	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	
Provider Administrative and Financial System	Systems used by healthcare providers 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	
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	

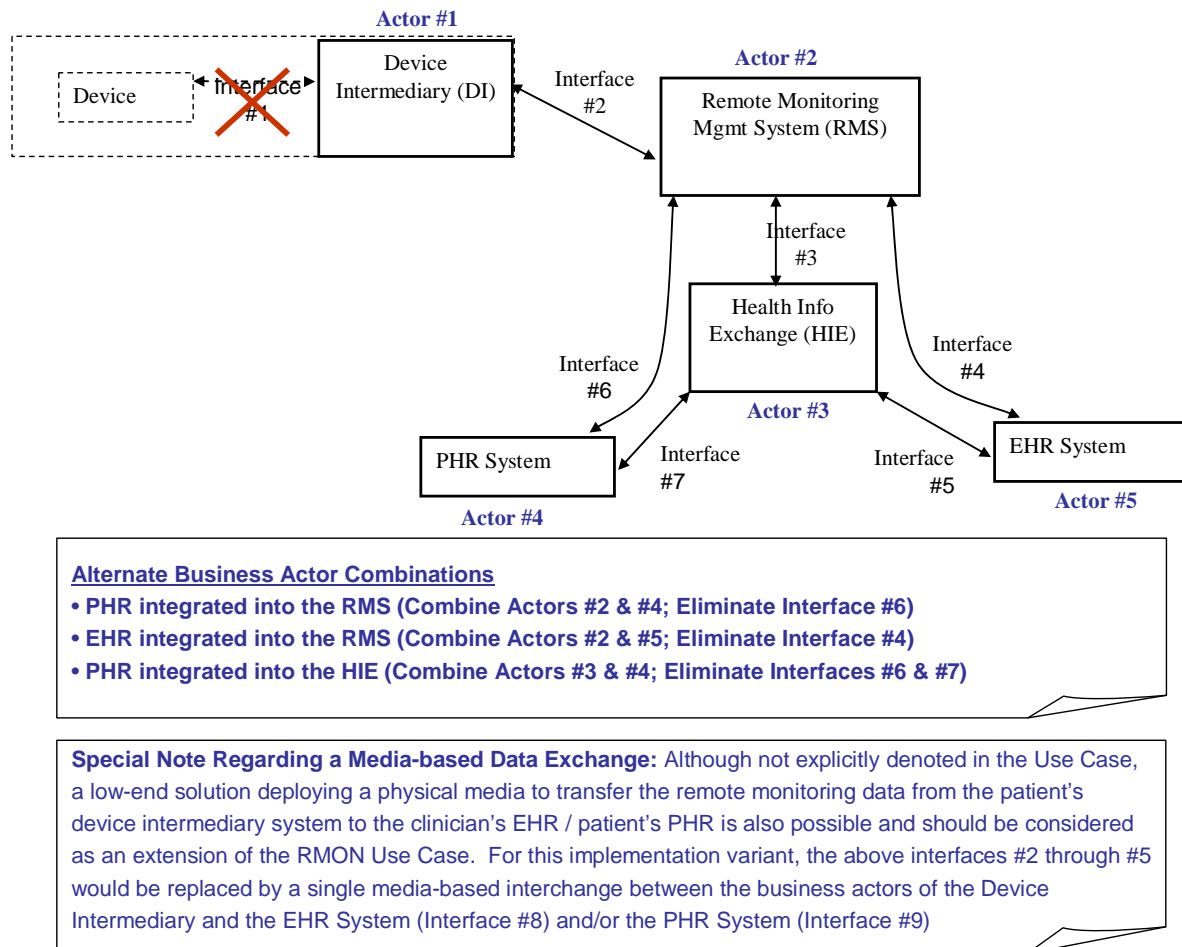
2.2.4 HIGH-LEVEL UML BUSINESS SEQUENCE DIAGRAM

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 UML diagrams that follow 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 identifies 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



Legend:

- Interface #1 is proposed to be placed out of scope on the basis of the remote monitoring requirements of the Use Case
- Interfaces #3 thru #7 are expected to be identical in terms of content
- Interfaces #3, #4, and #6 are expected to be identical. Interfaces #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; however the maturity of the standards may not permit addressing them in 2008



Figure 2.2.4-2 Business Sequence Diagram – 7.1.1

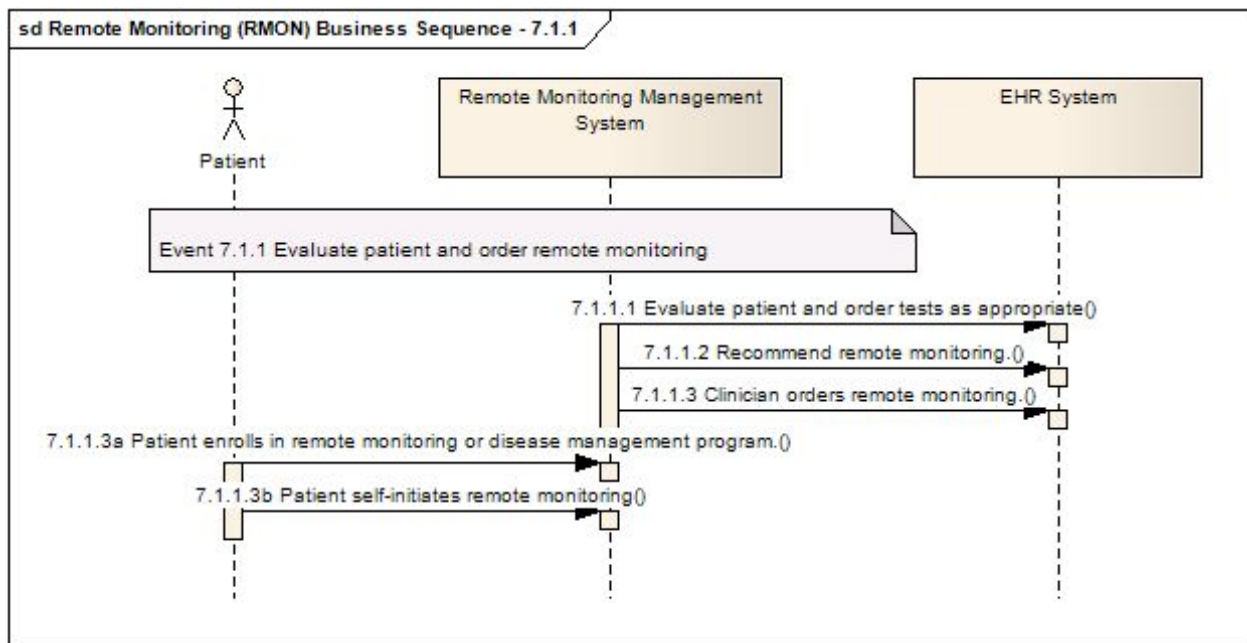


Figure 2.2.4-2 Business Sequence Diagram – 7.1.2 and 7.1.3

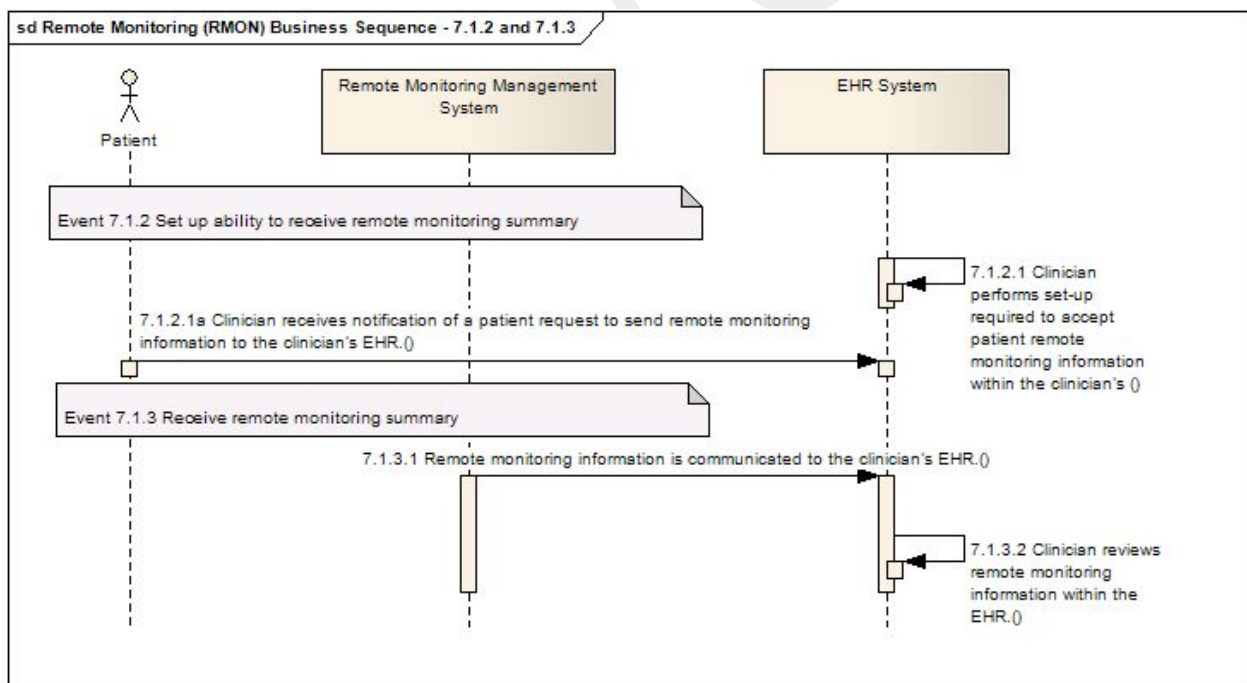


Figure 2.2.4-2 Business Sequence Diagram – 7.1.4 and 7.1.5

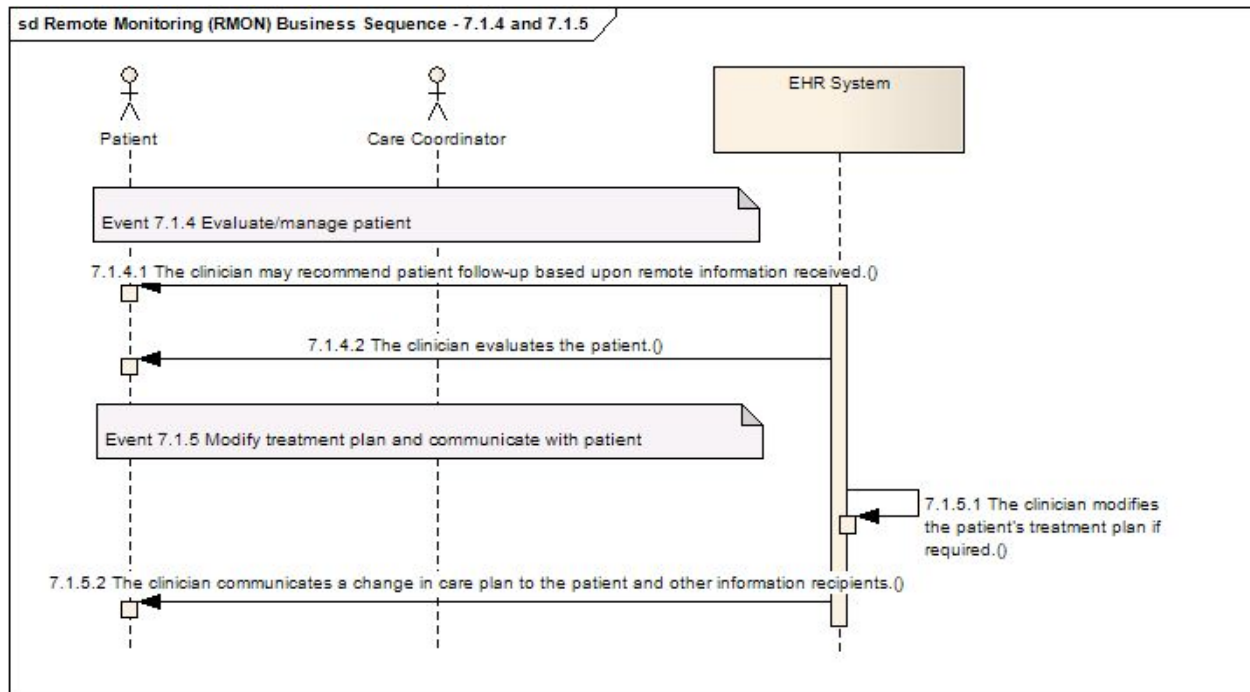


Figure 2.2.4-2 Business Sequence Diagram – 7.2.1

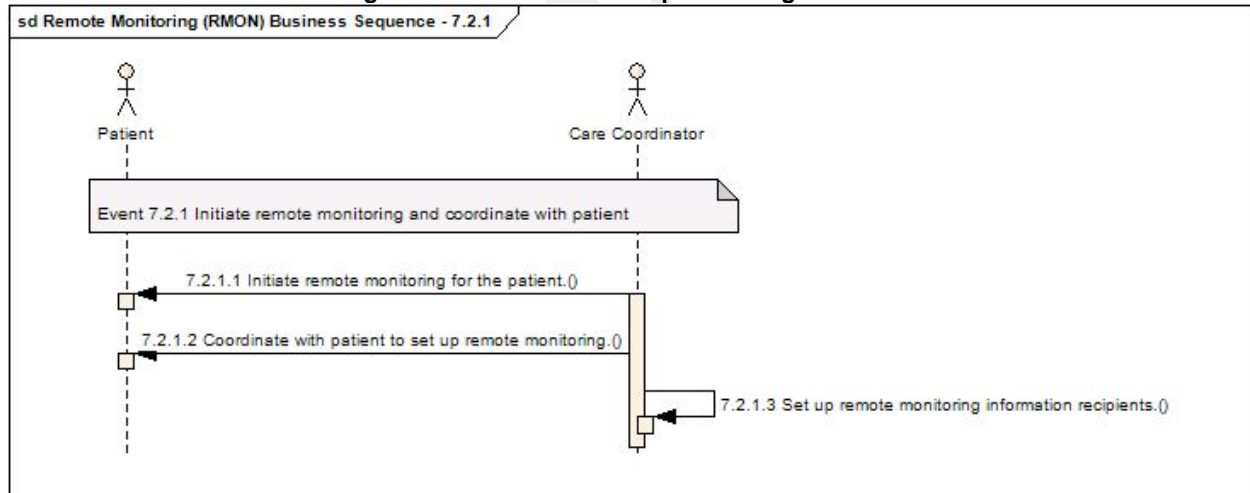


Figure 2.2.4-2 Business Sequence Diagram – 7.2.2 and 7.2.3

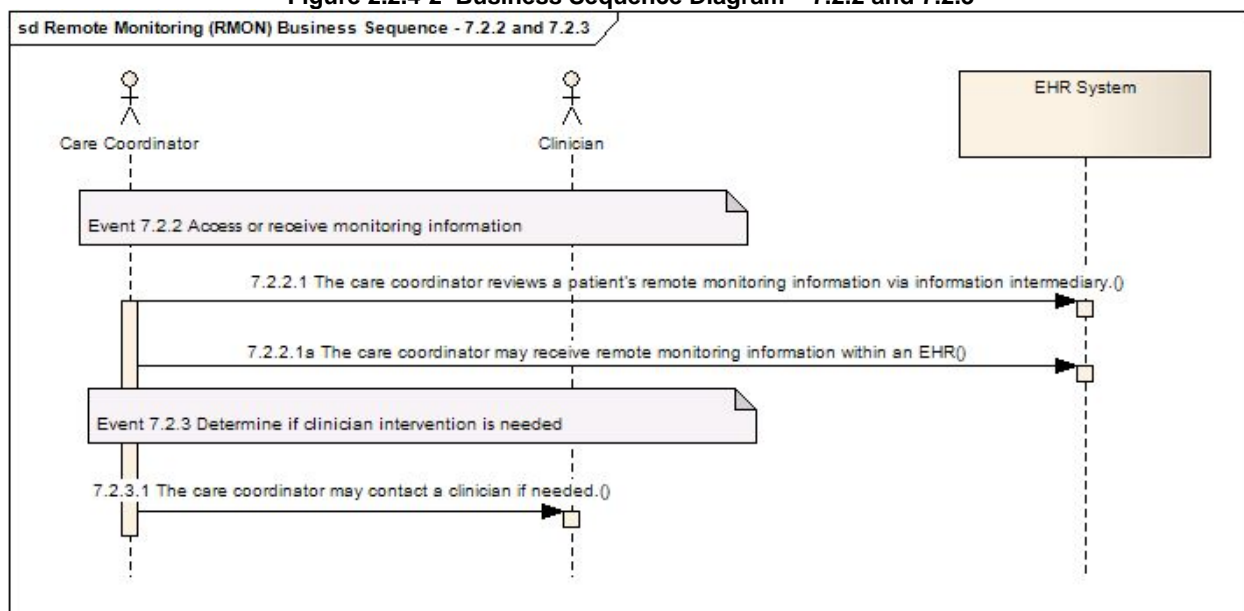


Figure 2.2.4-2 Business Sequence Diagram – 7.2.4 and 7.2.5

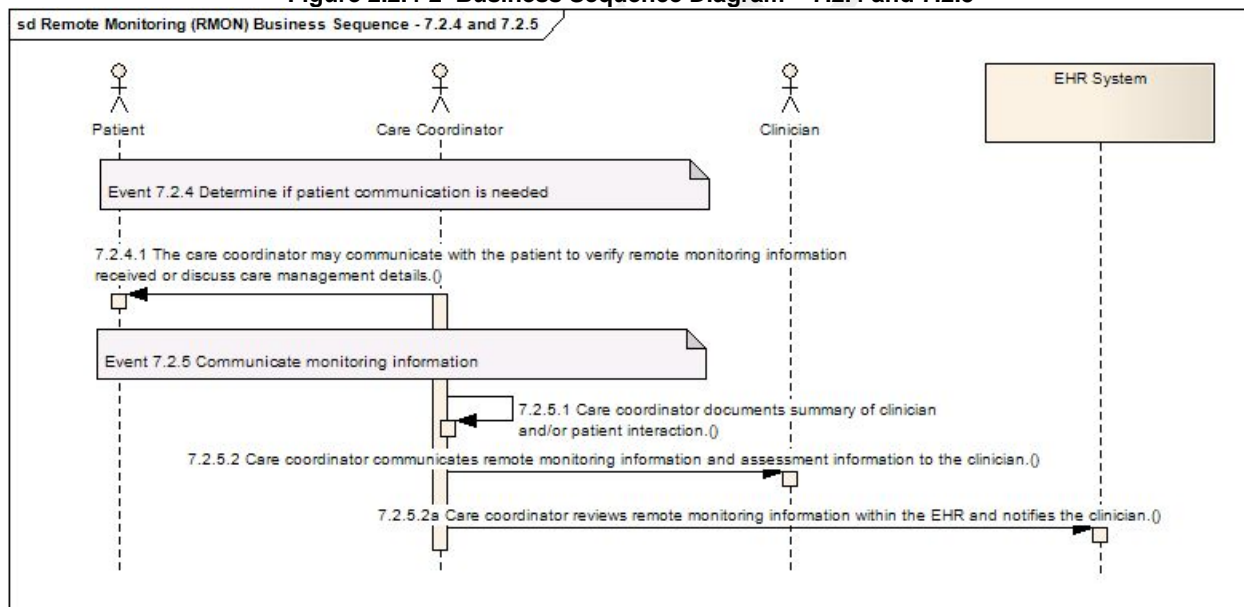


Figure 2.2.4-2 Business Sequence Diagram – 7.3.4 and 7.3.2

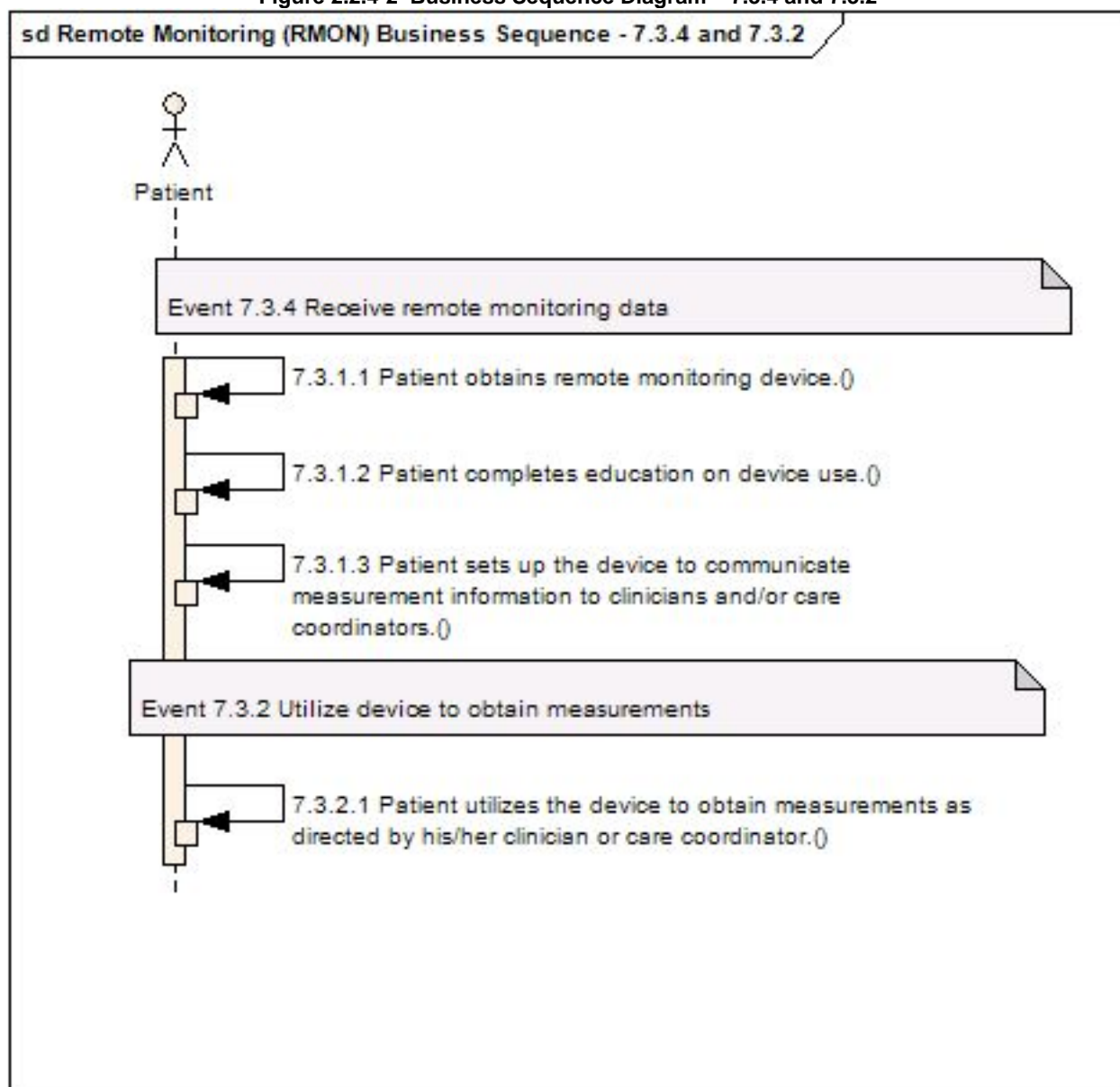


Figure 2.2.4-2 Business Sequence Diagram – 7.3.4 and 7.3.5

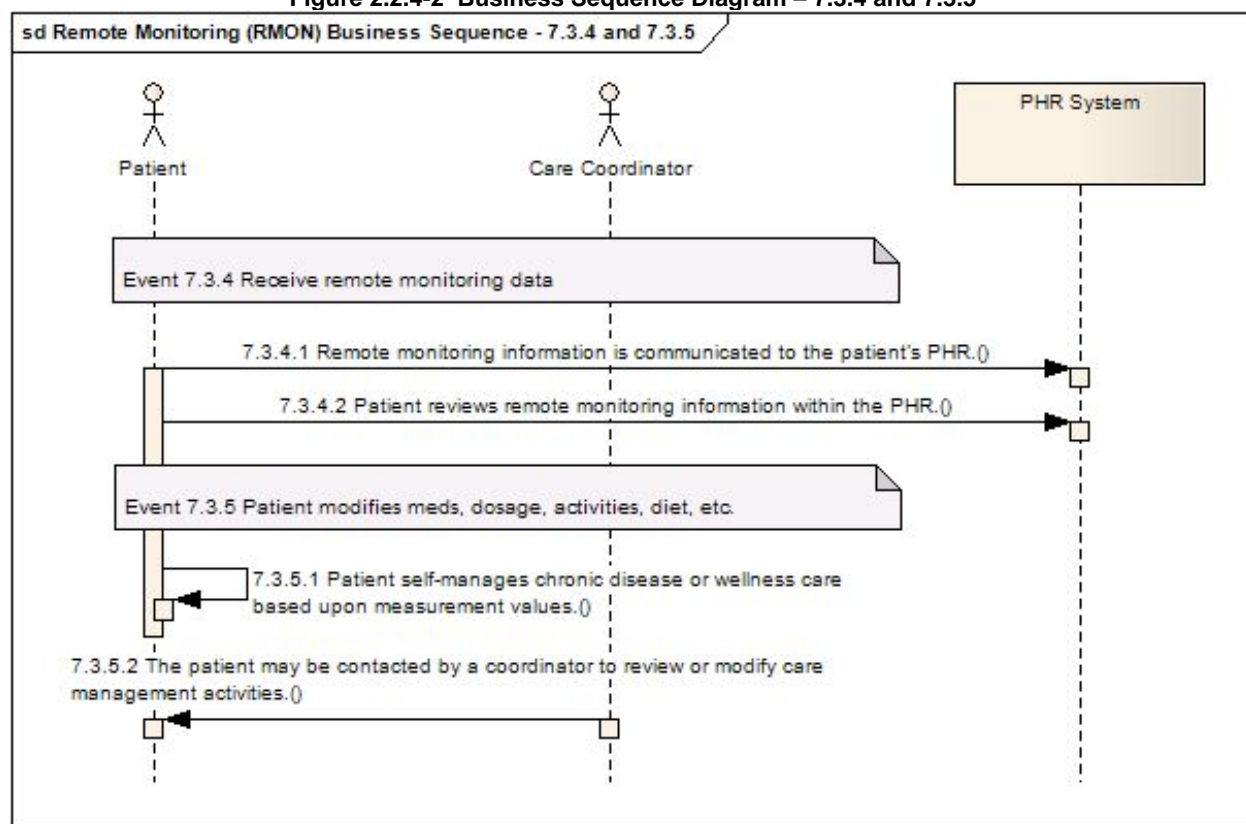
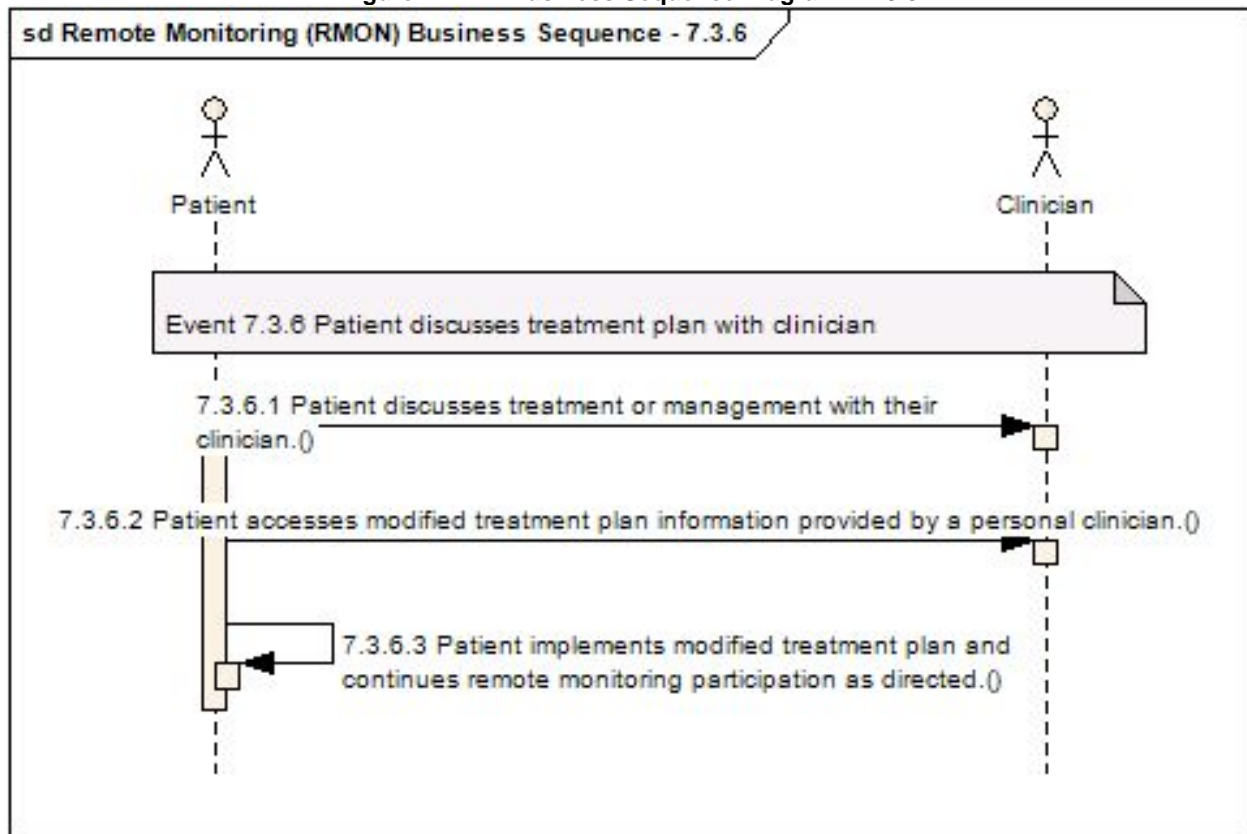


Figure 2.2.4-2 Business Sequence Diagram – 7.3.6



3.0 DESIGN

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

3.1 SCOPE OF DESIGN

This section describes the scope of the design as it relates to the requirements for 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 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• Weighting 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>#1 Identification/Remote Monitoring Registration Data</p> <p>#2.1 Blood Glucose Meter [see IEEE P11073-10417™ Dev specialization – Glucose meter]</p> <p>#2.2 Blood Pressure Monitor [see IEEE P11073-10407™ Dev specialization – Blood pressure monitor]</p> <p>#2.10 Oxygen Saturation (Pulse Oximeter) [see IEEE P11073-10404™ Dev specialization – Pulse oximeter]</p>	Include the Remote Monitoring measurements for the devices indicated in the 2008 IS development cycle.



Scope Item	Event	Scoping Action	Recommended Resolution
		<p>#2.12 Temperature (Thermometer) [see IEEE P11073-10408™ Dev specialization – Thermometer]</p> <p>#2.13 Weight (Weighing Scale) [see IEEE P11073-10415™ Dev specialization – Weighing Scale]</p> <p>#5.1 Generic Device Data [See IEEE P11073-20601™ Optimized exchange protocol]</p> <p># 6 Free Text Notes (e.g., Patient-entered Measurement Instance Specific Details)</p> <p>#7 Care Coordination Notes</p> <p>#9 Remote Monitoring Notification Data</p> <p>In addition, it is considered that there are two distinct levels of data interchange in terms 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 & forward data exchange level are addressed</p> <p>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 which can be comprised of the following data types:</p> <ul style="list-style-type: none"> • Episodic data • Document batch data • Control/status data 	
#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>#.2.3 through #2.9, #2.11, #3, #4, #5.2, #5.3, and #8</p> <p>At this point, it is recommended that for this cycle, real-time streaming data exchange is not included but will be retained as part of the requirements in future cycles</p>	Reflect these devices and measurements listed in the Data Requirements Table 2.2.2-1 on the roadmap for CPTC work in future cycles
#3	7.1.1.3a Alternate Action: Patient enrolls in remote monitoring or disease management	Patient enrollment is unclear; need to better understand the enrollment process and entity is used for the remote monitoring/disease mgmt program? More than just the patient inquiry will be needed; it needs to be determined exactly what construct to use in order to send patient enrollment information?	Reach out to the appropriate SDO or standards development groups regarding activities for this interface requirement and add this to the CPTC roadmap accordingly



Scope Item	Event	Scoping Action	Recommended Resolution
#4	7.1.1 Evaluate patient and order remote monitoring	The process for electronic ordering of remote monitoring may require standards and procedure designations that are not currently available and are therefore recommended not be included in 2008 version of the IS	Reach out to the appropriate SDO or standards development groups regarding activities for this interface requirement and add this to the CPTC roadmap accordingly
#5	7.1.5 Modify treatment plan and communicate with patient	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 Transfers of Care Use Case	Review the requirements related to treatment plans and their administration in the Consultation and Transfers 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 (Interfaces #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

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 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.	Remote Monitoring

3.1.2 CONSTRAINTS

This section describes the constraints that limit the use of the Requirements and Design, or to which the design must conform in order to be used within the described context. 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 scenario. 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 Use Case scenario.



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 preconditions 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 preconditions 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	All
Authentication service to authenticate requestors and/or data submissions from various locations	All
Security and Privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient Security and Privacy	All
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	All
Support the following HITSP Security and Privacy constructs: HITSP/C19 Entity Identity Assertion – Provide assertion HITSP/T16 Consistent Time – Maintain time HITSP/T17 Secured Communication Channel – Authenticate node HITSP/T15 Collect and Communicate Security Audit Trail – Record audit event in repository HITSP/TP30 Manage Consent Directive – Capture/Request consent directive HITSP/TP20 Access Control – Access control request	All
All pre-conditions from the lower level constructs are incorporated	All
When needed, the patient is uniquely registered with the Patient Identity Cross-Referencing service	All
Patient Identities (name, demographics etc.) are known and are consistent with policies	All

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
No applicable post-conditions	



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. Communication of Remote Monitoring Information to EHR or PHR
The CPTC will finalize what triggers are necessary in support of the 7 bi-directional interfaces shown in Table 2.2.4-1	All

3.2 DETAILED DESIGN

This section will provide 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 planned constructs used to meet the business and technical requirements for this Use Case. Opportunities for reuse of existing HITSP constructs are outlined, along with a description of any necessary updates to existing constructs. Any variances in the Security and Privacy implementation are also described here.

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 of assurance is offered by the basic use of HITSP/TP13 - Manage Sharing of Documents construct. A medium level of assurance is offered by 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 PKIs).

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 physician's office), to a clinician providing care to that patient. The transfer of this data may be accomplished either directly to an EHR System, or via the services of a Health Information Exchange (HIE) that is established to facilitate this kind of sharing of medical information. In addition to the data being transferred and persisted in the target EHR System, it may also be desirable for the patient to retain this remote monitoring data in their 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 (Fig 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 RDSS.
- b. This data is then forwarded to the 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 physician. 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 physician 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 new document content focused on the Remote Monitoring Observation data set will need to be defined but this is expected to leverage the HITSP-specified technical actors of Content Source/Consumer, Document Source/Consumer, for its format and transport to the clinician.

2. Ensure patient eligibility and authorize insurance reimbursement

- a. In addition to the transactions to accomplish the remote monitoring data exchange as described above, the technical design also reflects the administrative transactions for ensuring that the patient is eligible for remote monitoring services, and that an insurance reimbursement is authorized.
- b. These are accomplished respectively by the EHR 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. Payment Authorization Information Receiver querying the Payment Authorization Information Source to obtain payment authorization.
- c. The administrative-focused Business Actors identified in Section 2 serving as the eligibility and payment authorization resources are the Healthcare Services Eligibility System and the Health Plan Payment Authorization System respectively. Similarly to the clinical business actors, the administrative business actors may also be combined as an implementation variant.

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 implement real world business actor information interchanges (see Section 2.2.3). The table below identifies the technical actors and gives 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
Access Control Service (ACS)	This is the enterprise security service that supports and implements user-side access control capabilities. This is an initiator actor.
Audit Record Repository	Provides a repository for audit events.
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.
Consent Directive Requestor	The Consent Directive Requestor accesses Consent Directives located through a Consent Registry from Consent Repositories.
Consent Originator	Captures Consent Directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry.
Consent Registry	Responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a Manage Consent Directive Metadata Request.
Consent Repository	Responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns a Uniform Resource Identifier (URI) and Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point.
Content Creator	The Content Creator Actor is responsible for the creation of content and transmission to a Content Consumer.
Content Consumer	A Content Consumer Actor is responsible for viewing, import, or other processing of content created by a Content Creator Actor.
Device Observation Reporter	The Device Observation Reporter (DOR) actor receives device data and maps the received data to transactions providing consistent syntax and semantics.



Technical Actor(s)	Actor Role
Device Observation Consumer	The actor responsible for receiving and processing device data from the Device Observation Reporter.
Document Source	The Document Source is the producer and publisher of documents and information. It is responsible for sending documents to a Document Repository and a Document Recipient. It also supplies metadata to the Document Repository for subsequent registration of the documents with the Document Registry.
Document Recipient	The Document Recipient accepts sets of documents sent by a Document Source actor.
Document Consumer	The Document Consumer queries a Document Registry for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors.
Document Registry	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.
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.
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).
Node	Receives notifications of availability for documents in an XDS registry, and may optionally send acknowledgments of them.
Notification Receiver	Sends notifications of availability for documents in an XDS registry, and receives acknowledgements of these notifications.
Notification Sender	Queries the Patient Demographics Supplier to obtain patient demographic data. It may receive matches for one or more patients that enable the selection of the desired patient.
Patient Demographics Consumer	Receives patient registration and update messages from other systems in the enterprise (e.g., ADT Patient Registration systems), which may or may not represent different Patient ID Domains. It responds to queries for information.
Patient Demographics Supplier	Queries a Patient Identifier Cross Reference Manager for a set of identifiers for a patient.
Patient Identifier Cross-Reference Consumer	Responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains.
Patient Identifier Cross-Reference Manager	Provider of unique identifiers for each patient.
Patient Identity Source	Represents the system providing a protected resource and relies on the provided security service.
Service Provider (SP)	Represents the system providing a protected resource and relies on the provided security service.



Technical Actor(s)	Actor Role
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 transaction. Any Service User may also be a Service Provider.
Time Client	Establishes time synchronization with one or more Time Servers using the NTP protocol and either the NTP or SNTP algorithms. Maintains the local computer system clock synchronization with UTC based on synchronization with the Time Servers.
Time Server	Provides NTP time services to Time Clients. It is either directly synchronized to a UTC master clock (e.g., satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s).
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.
Eligibility Information Receiver	The system that initiates an inquiry to the Eligibility Information Source about an individual's insurance eligibility, coverage and benefits.
Payment Authorization Information Source	The system which holds and maintains the information regarding the individual's insurance requirements related to an authorization for benefit coverage determination and reimbursement purposes when a patient is referred for care or services, and responds to the query initiated by the Authorization Information Receiver.
Payment Authorization Information Receiver	The system that initiates a request to the Authorization Information Source about an individual's insurance requirements to obtain an authorization approval for purposes of benefit coverage determination and reimbursement in order to refer a patient for care or services to another clinician or providers of care.

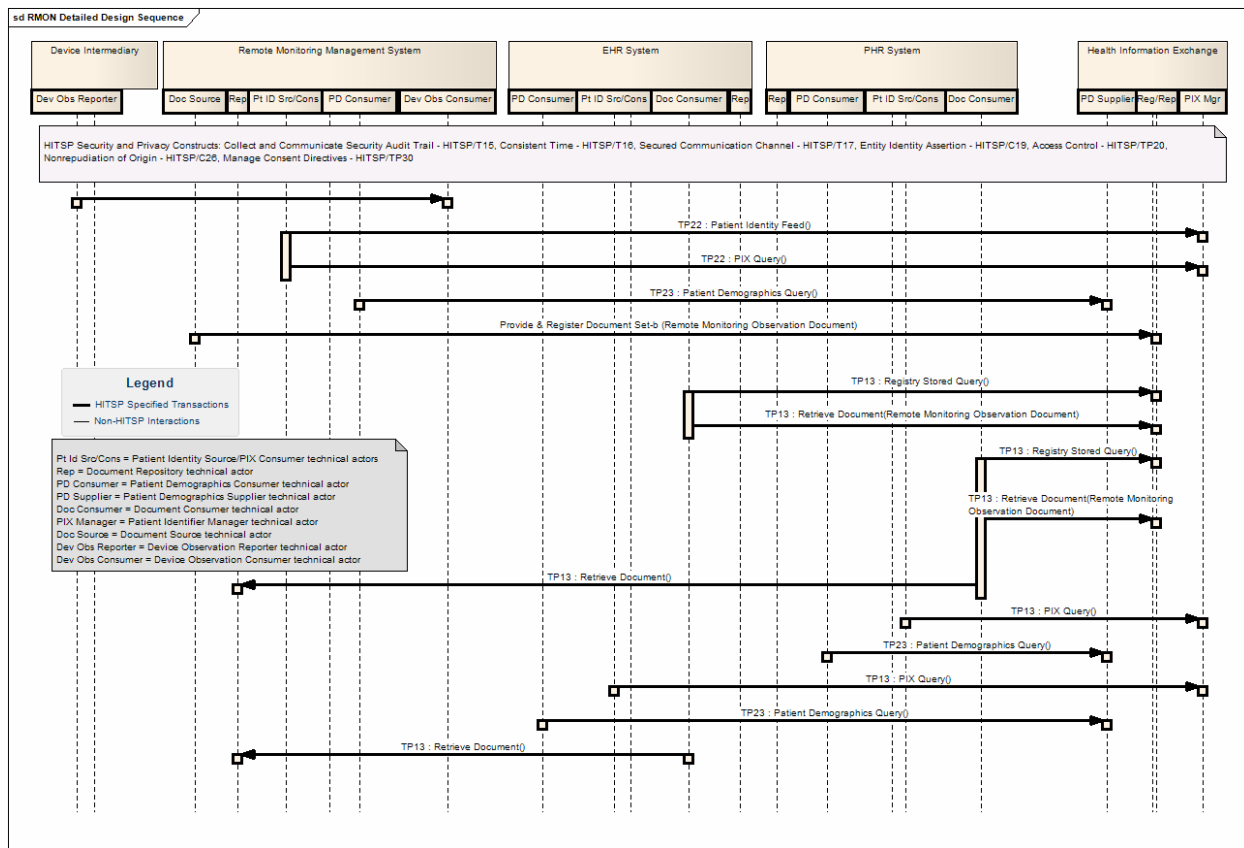
3.2.2 SEQUENCE DIAGRAM FOR PROCESS FLOW

This section incorporates the comprehensive business and technical requirements and a detailed analysis of the interactions and decisions undertaken for the primary actions in each Use Case scenario. The UML sequence diagrams used in this section incorporates 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 HITSP constructs). The detailed actor Transactions described in these diagrams show all common or independent actors, data, and the actual transactions from the HITSP constructs that are used for the Interoperability Specification.

Transactions that make use of existing HITSP constructs are shown explicitly, indicating opportunities for reuse.



Figure 3.2.2-1 Detailed Sequence Diagram for Scenario 1



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

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

- The Required or Conditionally Required technical actors that shall be supported as specified in the associated construct
- The Optional technical actors that may be supported as specified in the associated construct
- All Required or Conditionally Required transactions and content subsets for each implemented technical actor assigned to the business actor that shall be supported as specified in the associated construct
- The Optional transactions and content subsets for each implemented technical actor assigned to the business actor that 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.



For the actors of:

- Health Plan Payment Authorization System
- Provider Administrative and Financial System
- Healthcare Services Eligibility System
- Device Intermediary

It is not yet known how these actors will be secured, since the associated constructs have not yet been written. In the absence of this detail, the baseline Security and Privacy constructs (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	Optionality*
Device Intermediary	Device Observation Reporter	R	HITSP/T73	Provide Device Observation	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/C19	Convey Assertion	R
				Provide Assertion	O
			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 (SP)	R	HITSP/TP20	Access Control Request	O
Remote Monitoring Management System	Device Observation Consumer	R	HITSP/T73	Provide Device Observation	R
	Document Source	C[111]	HITSP/TP13	Provide & Register Document Set-b	R
	Document Source	C[111]	HITSP/T31	Provide & Register Document Set-b	R
	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



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	Optionality*
				Register Document Set-b	R
				Retrieve Document Set	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/C19	Convey Assertion	R
				Provide Assertion	O
			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 (SP)	R	HITSP/TP20	Access Control Request	O
EHR System (Clinician)	Document Consumer	C[112]	HITSP/TP13	Registry Stored Query	R
				Retrieve Document Set	R
	Document Recipient	C[112]	HITSP/T31	Provide & Register Document Set-b	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
	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



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	Optionality*
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
			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 (SP)	R	HITSP/TP20	Access Control Request	O
PHR System (Patient)	Document Consumer	C[112]	HITSP/TP13	Registry Stored Query	R
				Retrieve Document Set	R
	Document Recipient	C[112]	HITSP/T31	Provide & Register Document Set-b	R
	Document Repository	O	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
	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
	Patient Demographics Consumer	C[101]	HITSP/T23	Patient Demographics 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/C19	Convey Assertion	R
				Provide Assertion	O
			HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	Optionality*
	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
Locator Service (HIE)	Document Registry	R	HITSP/TP13	Register Document Set-b	R
				Registry Stored Query	R
Repository (HIE)	Document Repository	R	HITSP/TP13	Provide & Register Document Set-b	R
				Register Document Set-b	R
				Retrieve Document Set	R
Patient Identifier Service (HIE)	Patient Identifier Cross Reference Manager (PIX Manager)	R	HITSP/TP22	PIX Query	R
				Patient Identity Feed	R
				PIX Update Notification	R
	Patient Demographics Supplier	R	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
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
Provider Administrative and Financial System	Eligibility Information Receiver	R	HITSP/T40	Patient Generic Health Plan Eligibility Verification	R
	Payment Authorization Information Receiver	R	HITSP/T68	Authorization Request for Health Care Services	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/C19	Convey Assertion	R
				Provide Assertion	O
			HITSP/TP20	Access Control Request	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O



Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	Optionality*
Healthcare Services Eligibility System	Access Control Service	R	HITSP/TP20	Access Control Request	O
	Service Provider (SP)	R	HITSP/TP20	Access Control Request	O
	Eligibility Information Source	R	HITSP/T40	Patient Generic Health Plan Eligibility Verification	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/C19	Convey Assertion	R
				Provide Assertion	O
			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 (SP)	R	HITSP/TP20	Access Control Request	O
Health Plan Payment Authorization System	Payment Authorization Information Source	R	HITSP/T68	Authorization Response for Health Care Services	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/C19	Convey Assertion	R
				Provide Assertion	O
			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 (SP)	R	HITSP/TP20	Access Control Request	O



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

Actor Optionality Conditions

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

C[111] - Business actor shall support at least one of these technical actors to communicate outbound content

C[112] - Business actor shall support at least one of these technical actors to receive or retrieve inbound content

Transaction/Content (T/C) Optionality Conditions

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

3.2.4 DATA DETAIL

This section details the data elements and related Transactions that were extracted from the selected standards and describes any corresponding HITSP imposed constraints (e.g., required or optional).

Table 3.2.4-1 Data Element Constraints

Data Element	Transaction	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
TBD				

3.2.5 NEW HITSP CONSTRUCTS

This section describes the new HITSP constructs (including Interoperability Specifications, Transaction Packages, Transactions and Components) that are expected to be used for the Use Case. A current list of all existing HITSP constructs that are being used can be found in Section 3.2.6.

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

Table 3.2.5-1 New HITSP Constructs

New Construct	Construct Description	Common Actors	Interoperability or Data Requirement
HITSP/C74 - Remote Monitoring Observation Document	Describes the content of a Remote Monitoring session including one or more observations to be transferred to an EHR System or an HIE Repository.	Content Creator Content Consumer	7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1



New Construct	Construct Description	Common Actors	Interoperability or Data Requirement
HITSP/T68 - Health Plan Authorization/Referral Request and Response	System Inquiries to the Eligibility Information Source and Receiver about an individual's insurance eligibility, coverage and benefits. System Inquiries to the Authorization Information Source and Receiver about an individual's insurance requirements to obtain an authorization approval for purposes of benefit coverage determination and reimbursement in order to refer a patient for care or services to another clinician or providers of care.	Eligibility Information Receiver Eligibility Information Source Payer Authorization Information Receiver Payer Authorization Information Source	7.1.1.2
HITSP/T73 - Device Intermediary to Remote Monitoring Management System Communication	Transfer device observations from a Device Intermediary to a Remote Monitoring Management System. Describes both the content and the transport for completing the transfer. At this time, a single transaction entitled « Provide Device Observation » is envisioned.	Device Observation Reporter Device Observation Consumer	7.2.1.1

3.2.6 MODIFICATIONS TO EXISTING HITSP CONSTRUCTS

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

Table 3.2.6-1 Existing HITSP Constructs

HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
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.	Time Server Time Client	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.1.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No



HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
HITSP/TP17 - Secured Communication Channel	The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of Transactions, and the mutual trust between communicating parties. It supports both application and machine credentials, and user machines (user nodes).	Node	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.1.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
HITSP/TP20 - Access Control	The Access Control Transaction Package provides the mechanism to administer security authorizations which control the enforcement of security policies including: role-based access control; entity based access control; context based access control; and the execution of consent directives. In an emergency, this construct supports the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents.	Access Control Service Service Provider Service User	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.1.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
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.	Consent Originator Consent Repository Consent Registry Consent Directive Requestor	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No



HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
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.	Audit Record Source Audit Record Repository	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.1.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
HITSP/TP22 - Patient ID Cross-Referencing	This specification includes by reference the transactions and components that comprise the Patient ID Cross-Referencing Transaction Package. The two transactions within this package are: * The IHE Patient ID Cross-Referencing (PIX) transaction * The IHE Patient Identity Feed transaction	Patient Identifier Cross-Reference Consumer Patient Identifier Cross-Reference Manager Patient Identity Source	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
HITSP/T23 - Patient Demographics Query	This PDQ Transaction is intended to provide a 'list patients and their demographics' query / 'patient(s) and their demographics identified' response message pair (QBP*Q22, RSP*K22) for use wherever such needs exist. This Transaction document extracts the Health Level Seven (HL7) version 2.5 Query and Response data mapping. The underlying basis for this extraction can be found in the Integrating the Healthcare Enterprise IT Infrastructure Technical Framework, Volume 2 (ITI TF-2), Revision 3.0: "Patient Demographics Query."	Patient Demographics Consumer Patient Demographics Supplier	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No



HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
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.	Service User Identity Provider Service Provider	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.1.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
HITSP/TP13- Manage Sharing of Documents	This 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.	Document Source Document Consumer	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No
HITSP/T31 - Document Reliable Interchange	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 to support a healthcare delivery organization or clinician who may need to communicate a clinical document to a recipient through direct communication.	Document Source Document Recipient	7.1.1.1, 7.1.1.2, 7.1.3.1, 7.2.4.1, 7.2.5.1, 7.2.5.2, 7.3.4.1	No



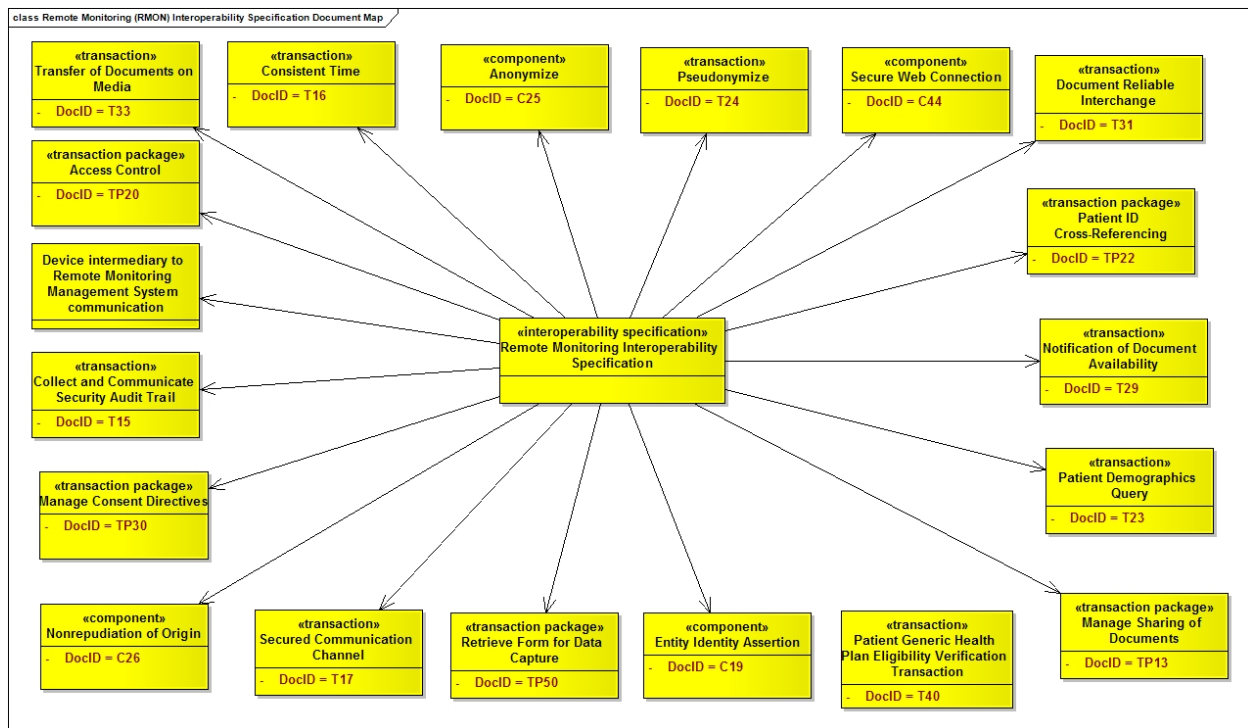
HITSP Construct	Construct Description	Technical Actors	Interoperability or Data Requirement Number	Modification Required
HITSP/T40 - Patient Generic Health Plan Eligibility Verification	This Transaction is intended to provide the status of a health plan covering the individual, along with details regarding 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, professional physician office visit, pharmacy and vision services that are included in the patient's generic health plan benefit.	Eligibility Information Receiver Eligibility Information Source	7.1.1.1	

3.2.7 DOCUMENT MAP

The document map summarizes the suite of constructs that are in the detailed map to existing standards and specifications used to satisfy the requirements imposed by the Remote Monitoring Use Case. The most effective way to see the construct breakdown is to begin with the document indicated at the top of the diagram.



Figure 3.2.7-1 Requirements, Design, and Standards Selection Document Map



4.0 CANDIDATE STANDARDS

This section presents the candidate standards that may support the major Use Case events described in the requirements analysis. During Interoperability Specification development, standards selection will be based on the following process:

- **Evaluation:** The Technical Committee evaluates the standards using the Tier 2 Readiness Criteria. Standards considered for use may include provisional or to be named standards
- **Selection:** Based on the Tier 2 evaluations, named standards are selected and listed in Table 4.1.2-1. 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. During the actual construction of Interoperability Specifications, the Technical Committee may need to refine this listing based on detailed analysis
- **Gap and Overlap Analysis and Recommendations:** The Technical Committee also identifies, and analyzes gaps and overlaps within the standards industry as they related to the specific Use Case. The TC will provide a description of the gaps, including missing or incomplete standards, provide a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps

Thus the following section lists a summary of the standards that will be further refined during the Interoperability Specification development phase.

4.1 LIST OF SELECTED AND CANDIDATE STANDARDS

This section presents the selected, and candidate standards that may support the Use Case events described in the requirements analysis. As used by HITSP, the term “standard” refers, but is not limited to Specifications, Implementation Guides, Code Sets, Terminologies, and Integration Profiles. A standard should be produced through a well-defined approach that supports a business process and

1. has been agreed upon by a group of experts
2. has been publicly vetted
3. provides rules, guidelines, or characteristics
4. helps to ensure that materials, products, processes, and services are fit for their intended purpose
5. is available in an accessible format
6. is subject to an ongoing review and revision process

Candidate standards are then evaluated using the HITSP Tier 2 Readiness Criteria. Final selection does not occur until the Interoperability Specifications are completed. Thus there may be additions or deletions to this list.

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



- Regulatory and guidance standards are legal or other authoritative declarations that HITSP must abide by. These may also be guidelines and recommendations that HITSP has adopted to aid in the selection of standards (see Section 4.1.1)
- Selected candidate standards are those candidate standards that are selected within the context of the specific Use Case requirements, and are evaluated for inclusion as part of the Interoperability Specification (see Section 4.1.2)

4.1.1 REGULATORY AND GUIDANCE STANDARDS

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 the Interoperability Specification.

Table 4.1.1-1 Regulatory and Guidance Standards

Standard	Description
For Regulatory and Guidance Standards relating to the Security and Privacy of Health Information, please see HITSP/TN900 Security and Privacy Technical Note	The HITSP/TN900 document is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs. It also includes a set of overarching principles and concepts, derived from an analysis of major federal and common state laws and regulations.

4.1.2 SELECTED AND CANDIDATE STANDARDS

The section provides a mapping of candidate standards that may be required to implement the requirements of the Interoperability Specification to the Use Case action codes which are supported.

Section 3.2 provides a description and listing of the new and existing constructs that are used by this Requirements, Design, and Standards Selection specification. Section 3.2.6 describes existing constructs that are expected to be used in this specification without changes (reused), or modified to include additional requirements (repurposed). Selected standards that are used by existing constructs are provided in the published construct specifications available from www.hitsp.org, and are not duplicated in this document. The following table only lists candidate standards that may be selected to meet use case requirements for new or repurposed constructs used in this specification. A detailed description of each standard is also provided in the appendix.



Table 4.1.2-1 Selected and Candidate Standards Linked to Requirements

SDO and Standard Name	Event/Action Code	Category (Construct)	Remarks/ Minor Gaps
International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers (IEEE) Health informatics -- Point-of-care medical device communication -- Part 20101: Application profiles -- Base standard, Technical Specification # ISO/IEEE 11073-20101:2004 NOTE: This standard forms the core of the personal health device data to be converted using ASN.1 XER (XML encoding rules).	7.2.1.1	HITSP/T73	This standard selection is to be deployed in the new construct HITSP/T73 - Device Intermediary to Remote Monitoring Management System Communication to satisfy Interface #2. CPTC and CMHR DTC membership will review these two standards as part of the Tier 2 due diligence process and will resolve this overlap prior to issuance of the IS document.. More information regarding the ASN1 XER may be found at http://www.itu.int/ITU-T/studygroups/com17/languages/X.693-0112.pdf .
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework 2006-2007, Revision 1.1, Device Enterprise Communication (DEC) Integration Profile	7.2.1.1	HITSP/T73	With the second option, we would expect to exchange this over web services, but as noted, there is presently no WSDL defined to do this.
Health Level Seven (HL7) Implementation Guide for PHM Report Release 1.0 Levels 1,2, and 3, Personal Health Monitoring Report (PHMR), International Realm, Based on HL7 CDA Release 2.0 (Draft Standard for Trial Use)	7.2.1.1	HITSP/C74	
Accredited Standards Committee (ASC) X12N 278 - Health Care Services Review - Request for Review and Response, Version 4010, May 2000, and Addenda to Health Care Services Review - Request for Review and Response, Version 4010, October 2002	7.1.1.2	HITSP/T68	

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 endorsement 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 Remote Monitoring Use Case event. Recommended resolutions were developed through a series of steps including the committee's initial recommendations, cross team validation of the gap, provisional recommendations and peer review by the team.



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

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Event Description	Identified Gaps	Recommended Resolution
7.1.3.1	Remote monitoring information is communicated to the clinician's EHR.	HITSP/C74 - Remote Monitoring Observation Document	There is an implementation guide in development by HL7 Structured Documents called Patient Home Monitoring (PHM). It is due for a first ballot in September 2008. It meets the Use Case requirement, but may not be approved in time for completing this Interoperability Specification by December 2008. If it fails first ballot, it is recommended to delay the IS completion, as there is no other alternative. Progress will be assessed based on the RDSS responses.
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.		
7.2.1.1	Initiate remote monitoring for the patient.	Depending on the standard selected to implement Interface #2, there may be additional SDO work necessary to satisfy all of the stipulated RMON requirements.	This should be re-assessed once the standards are selected. Potential resolutions could include: 1) accept a phased approach whereby the initial requirements are relaxed or 2) accelerate the necessary SDO work and realize interface #2 in 2009

4.3 STANDARD OVERLAPS

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

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

Table 4.3-1 Standard Overlaps

Event Code	Event Description	Standard Overlap	Recommended Resolution
No applicable overlaps			



5.0 NEXT STEPS

The first step in the HITSP harmonization process is requirements analysis and design. Upon completion of the Requirements, Design and Standards Selection for the Remote Monitoring Use Case, the following steps will occur:

- This document will be submitted to the HITSP Panel and interested Public for comment
- After the comment period, the Technical Committee or Work Group will disposition the comments, maintaining a written log of all dispositions assigned to the TC/WG
- Persuasive comments will be used to inform the construction of the Interoperability Specification (IS)
- Non-persuasive comments or comments that are not applicable to the construction of the IS will be deferred with reason/explanation (e.g., need additional information or further analysis during construction)
- In parallel to the steps described above, the Technical Committee/Work Group will begin the construction of the Interoperability Specifications



6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF STANDARDS

The following table contains descriptions of the standards that are referenced by this Requirements, Design, and Standards Selection Specification:

Table 6.1-1 Description of Standards

Standard Name	Description
Accredited Standards Committee (ASC) X12N 278 - Health Care Services Review - Request for Review and Response, Version 4010, May 2000, and Addenda to Health Care Services Review - Request for Review and Response, Version 4010, October 2002	<p>This is the HIPAA standard for referral and authorization, as referenced in §162.1302 of the Regulation. This HIPAA transaction provides standardized data requirements and content for the exchange of information between providers and review entities. This transaction allows for the following business events and processes:</p> <ul style="list-style-type: none">admission certification review request and associated responsereferral review request and associated responsehealth care services certification review request and associated responseextend certification review request and associated responseunsolicited notifications inquiries and responses. <p>The HIPAA standard X12 278 is to be used when health care services reviews and requests and responses for review are made. For more information, visit www.x12.org.</p>
Health Level Seven (HL7) Implementation Guide for PHM Report Release 1.0 Levels 1, 2, and 3, Personal Health Monitoring Report (PHMR), International Realm, Based on HL7 CDA Release 2.0 (Draft Standard for Trial Use)	<p>The purpose of this document is to describe constraints on the CDA Header and Body elements for Personal Health Monitoring Report documents.</p> <p>The Personal Health Monitoring Report is document that carries personal health monitoring data. The data transmitted from Sender is either in the form of a summary or in the form of raw data. The summarization may be a result of analysis by authentic disease management service provider. The data has multiple characteristics including:</p> <ul style="list-style-type: none">• Representation of measurements captured by devices• Representation of notes, summary and other kinds of narrative information that may be added by care givers or by the user themselves• Representation of graphs that may be added by intermediary devices that represent trends of user's health <p>In order to accommodate the wide variety of data characteristics, HL7 Clinical Document Architecture (CDA) based format is chosen. The guidelines will specify constraints on the CDA in accordance with requirements set forward by the xHR interface. These constraints will be hence forth called Personal Healthcare Monitoring (PHM) Report. For more information, visit www.hl7.org.</p>
Integrating the Healthcare Enterprise (IHE) Patient Care Device Technical Framework 2006-2007, Revision 1.1, Device Enterprise Communication (DEC) Integration Profile	<p>The Device Enterprise Communication (DEC) profile addresses the need for consistent communication of PCD data to the enterprise. Enterprise recipients of PCD data include, but are not limited to, Clinical Decision Support applications, Clinical Data Repositories (CDRs), Electronic Medical Record applications (EMRs), and Electronic Health Records (EHRs).</p> <p>The current profile does not address issues of privacy, security, and confidentiality associated with cross-enterprise communication of PCD data. For year 1 the assumption is made that the DEC profile is implemented in a single enterprise on a secure network. These aspects are on the IHE PCD roadmap for subsequent years. For more information, visit www.ihe.net</p>



Standard Name	Description
<p>International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers (IEEE) Health informatics -- Point-of-care medical device communication -- Part 20101: Application profiles -- Base standard, Technical Specification # ISO/IEEE 11073-20101:2004</p> <p>NOTE: This standard forms the core of the personal health device data to be converted using ASN.1 XER (XML encoding rules).</p>	<p>Provides the upper layer [i.e., ISO's open systems interconnection (OSI) application, presentation layer, and session layer] services and protocols for information exchange under the ISO/IEEE 11073 standards for medical device communications (MDC).</p> <p>It is the base standard of the ISO/IEEE 11073-20000 medical device application profiles (MDAP), as harmonized through the Committee for European Normalization (CEN) and ISO.</p> <p>For more information, visit www.iso.org.</p>



7.0 CHANGE HISTORY

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

No changes at this time. This is the first published version.

