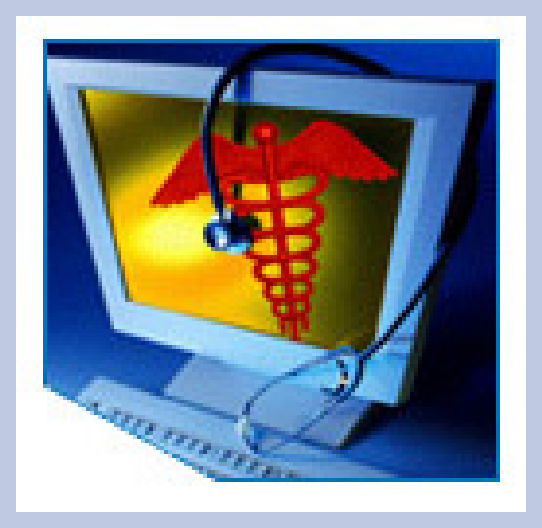
August 27, 2008
Version 1.2

HITSP Emergency Responder Electronic Health Record Interoperability Specification

HITSP/IS04



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Provider Perspective Technical Committee
(Formerly Care Delivery Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Care Delivery Technical Committee	July 20, 2007
1.0.1	Review Copy	Care Delivery Technical Committee	December 5, 2007
1.1	Released for Implementation	Care Delivery Technical Committee	December 13, 2007
1.1.1	Review Copy	Provider Perspective Technical Committee	August 20, 2008
1.2	Released for Implementation	Provider Perspective Technical Committee	August 27, 2008

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Emergency Responder Electronic Heath Record (ER-EHR) Interoperability Specification, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for the Interoperability Specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Interoperability Requirements.

1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

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

Pre-hospital care and emergency response lack interoperable information technology infrastructure and Standard Development Organizations (SDO) consensus standards. From an interoperability perspective, the American Health Information Community (AHIC) Emergency Responder Electronic Health Record (ER-HER) Use Case treats pre-hospital care similar to hospital care in spite of heterogeneous pre-hospital organizational structures and overlapping policy jurisdictions which must deal with cross-affinity domain interactions, poor communications, emerging technologies and policies. Additionally, first responders must potentially deal with unreliable communications, power and failure prone systems while working under stressful conditions with inadequate resources. HITSP was challenged by wanting to focus on interoperability, achieve closure, be pragmatic and have a futuristic perspective.

The ER-EHR Use Case focuses on the deployment of standardized, widely available and secure solutions for accessing and exchanging current and patient-specific historical health information. The historical information typically resides or is available from a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR). The current data can be generated by a variety of emergency responders. The Use Case is driven by the requirements of timely electronic access and exchange of critical health information which should support the assessment, stabilization and treatment of the victims of emergency incidents, as well as, on a treatment non-interference basis, facilitate family member reunification and expedite next-of-kin notification following such incidents. This could range from routine incidents involving individuals suffering from motor vehicle crashes or acute episodes of illness, to large groups of people suffering as the result of mass casualty incidents including natural disasters, pandemics and terrorism.

The ER-EHR Use Case covers the workflow from the time responders become aware that there is an emergency. It covers the perspective of incident commencement and situational awareness (9-1-1, Dispatch or Emergency Communications System) to on-site care providers (Emergency Medical Services (EMS), Law Enforcement, Fire) and emergency care clinicians. Emergency care clinicians involved in the care and treatment of emergency incident victims, medical examiner/fatality managers investigating

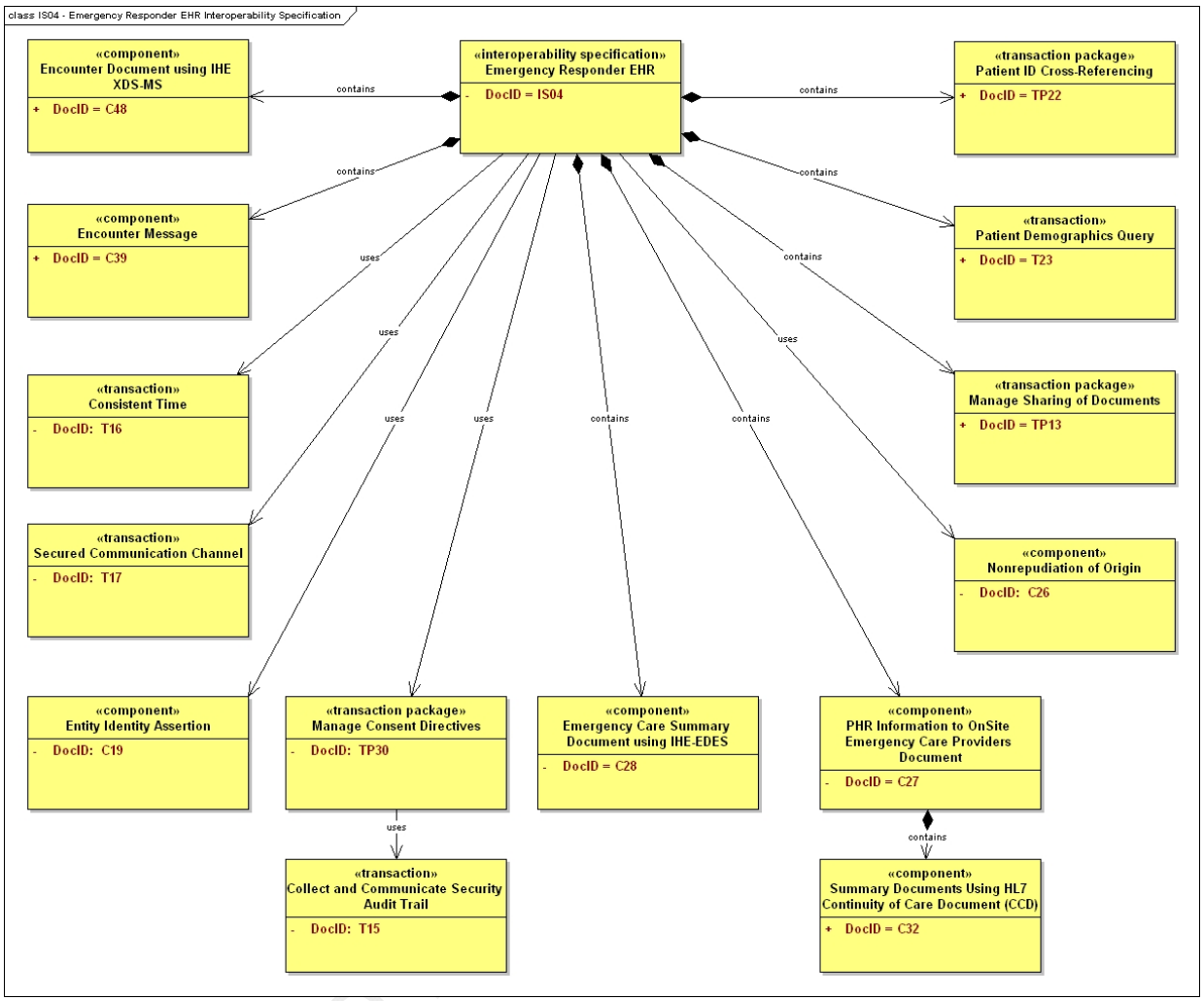
cause of death, emergency managers, and public health practitioners also use information generated/collected by various responders. This Use Case focuses on interoperability requirements and does not attempt to include all of their functions and interactions.

The Emergency Responder EHR envisioned by this Use Case is an amalgam of current emergency incident and patient-specific historical health information collected over time from a number of sources. Patient-specific historical health information includes Emergency Contact Registry (ECON) data, Personal Health Record (PHR) data and Electronic Health Record (EHR) data. Current emergency incident information includes all information from the first notification to an Emergency Responder through the completion of the last encounter. This is defined as an Episode of Care. These data are collected from the beginning of the incident, from a number of systems and are assembled into a growing ER-EHR that is used by the actors within the Use Case as the incident proceeds through the scenarios. We have referred to these data throughout the Interoperability Specification as the Episode of Care Record, which is ultimately loaded into the ER-EHR repository. The reader should recognize that Episode/of/Care data includes the pre-hospital Patient Care Report and patient-specific historical data from the Personal Health Record (PHR), Emergency Contact Registry (ECON) and /or Electronic Health Record (EHR). Moreover, the Episode of Care Record is comprised of a number of Encounter Records, including the ED and Definitive Care. The HL7 Continuity of Care (CCD) Clinical Summary is used to provide initial clinical information to the emergency responders and is used at each hand off of care to provide clinical information to the Emergency Care Department, Definitive Care, transfer or final disposition of the Episode of Care.

1.2 INTEROPERABILITY SPECIFICATION DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant context(s) for the use of HITSP constructs that further identify and constrain standards where necessary. In addition to ISs, there are three other types of HITSP constructs called Transaction Packages (TP), Transactions (T), and Components (C). The roadmap depicted in Figure 1.2-1 identifies the HITSP constructs used to meet the IS requirements. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses. The following diagram is limited to existing HITSP constructs. It includes neither candidate standards we recommend, nor gaps for standards that we identify.

Figure 1.2-1 Interoperability Specification Document Map



1.2.1 LIST OF CONSTRUCTS

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

Table 1.2.1-1 List of Constructs

Construct	Description
HITSP/T15	Collect and Communicate Security Audit Trail
HITSP/T16	Consistent Time
HITSP/T17	Secured Communication Channel
HITSP/C19	Entity Identity Assertion
HITSP/T23	Patient Demographics Query
HITSP/TP13	Manage Sharing of Documents
HITSP/TP20	Access Control
HITSP/TP22	Patient ID Cross Referencing
HITSP/TP30	Manage Consent Directives
HITSP/C28	Emergency Care Summary Document Using IHE Emergency Department Encounter Summary (EDES)
HITSP/C32	Summary Documents Using HL7 Continuity of Care Document (CCD)
HITSP/C39	Encounter Message
HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS)

1.3 COPYRIGHT PERMISSIONS

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

1.4 REFERENCE DOCUMENTS

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

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

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
Emergency Responder Electronic Health Record (ER-EHR) Detailed Use Case, December 20, 2006	AHIC Use Case that is the basis of this Interoperability Specification.

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

2.0 INTEROPERABILITY REQUIREMENTS

This section provides a high level description of the Emergency Responder EHR 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 ER-EHR Use Case, including applicable scenarios that are part of the Use Case. This ER-EHR Use Case scenario covers the use of an ER-EHR from the perspective of those responders that first learn about an event (9-1-1), and dispatch care (Dispatch) (hereafter referred to as “Emergency Communications Systems or Systems”), then on-site emergency care providers (EMS, Law Enforcement, Fire etc.) and emergency care clinicians. It includes those involved in the care and treatment of emergency incident victims, medical examiner/fatality managers investigating the cause of death, emergency managers, and public health practitioners using information contained in the ER-EHR.

The Use Case begins with the notification (Awareness) of the incident and collection of information about the victim and incident. This is followed by dispatch of on-site care providers to the scene of an emergency incident, including providing them with this information. It follows the patient through initial treatment, the evacuation process to emergency medical treatment facilities, transfer from facility to facility, and ends when the incident and care is completed and final patient disposition updates are added to the EHR/PHR.

Several years ago the National Association of State EMS Officials (NASEMSO) in conjunction with its federal partners at the National Highway Traffic Safety Administration (NHTSA) and the Trauma/EMS Systems program of the Health Resources and Services Administration's (HRSA) Maternal Child Health Bureau worked to develop a national EMS database—known as NEMSIS. In addition, the NEMSIS Technical Center was created and is managed by the University of Utah School of Medicine. Along with the development of the national system, the NEMSIS program, in collaboration with EMS Stakeholders, developed a national set of data standards, standard data definitions and XML Schema Definitions for exchanging EMS data (or pre-hospital data) among EMS services, local and state governments and the national NEMSIS program. Today, during or after the completion of an emergency run by EMS Services

(Ambulance) the EMS Service completes a report called “the Patient Care Report (PCR)” also called an Ambulance “Run Report.” These reports are based upon the NEMSIS data standards.

Health surveillance and situational information is periodically sent to public health systems to support biosurveillance programs. Similarly, situation and appropriate patient information is sent to other stakeholders, including emergency managers. Hospitals or other appropriate care facilities continually update their resource availability. Emergency Operations Centers (EOC) and public health systems may be local, regional, state or federal.

Information useful to any form of emergency medical response may reside in multiple locations, and may be contributed by public and private parties which traditionally have not been part of emergency medical response or care. These can range from public health agencies managing Points of Dispensing (PODs) or a vaccine inventory, to a personal physician, to commercial providers of Personal Health Records (PHR), Emergency Contact Registries (ECON), and/or Electronic Health Records (EHR), to automaker Telematics Service Providers (TSP) such as General Motors’ OnStar and Mercedes-Benz TeleAid with vehicle crash data (e.g., key crash metrics, air bag deployment, multiple impacts, rollover, etc.).

Two major concepts are described: Small scale incidents and large scale incidents. A small scale incident is one in which a moderate number of individuals are injured/ ill (require medical attention or treatment), and where the medical resources of an individual city, county or metropolitan area are sufficient to provide medical response and treatment for the casualties. The ability to provide routine care is not compromised. The timescale for response is normally expected to be less than twenty-four hours. Examples may include routine incidents such as motor vehicle crashes, and less common events such as chemical spills or the collapse of an office building.

A large scale or mass casualty incident is one in which the number of casualties/patients is such that the local resources must be augmented by external resources (regional, state and/or federal). The incident may occur across several geographic areas or it may be nationwide in scope. The ability to provide routine care will potentially be curtailed. External command and control is required to best match casualty needs to capabilities. The timescale for on-site response is typically greater than twenty-four hours and may extend to days, weeks or months. In a mass casualty incident, such as a pandemic flu, response and/or care may need to be provided on a virtual/remote basis. Communication networks may be partially or completely unavailable. It is likely that medical treatment facilities will be unable to process incoming patients as rapidly as is required, and triage decisions become critical. Examples may include the crash of a large airliner, a bridge collapse, school bus accident, a large scale terrorist attack, a major military combat operation, a large scale terrorist attack, a major military combat operation, a large natural or man-made disaster such as Hurricane Katrina or an occurrence of pandemic disease.

Additional perspectives address “Provider Authentication and Authorization Information Flows,” which defines requirements and provides commentary on:

1. Medical licensing and certification entities which communicate provider-specific licensing and credential information to the Health Information Service Provider
2. DOD, PHS, Federal Emergency Management, and other appropriate entities who confirm the licensing and credential information of their medical and related providers
3. DOD, PHS and Federal Emergency Management entities who provide additional information about the medical privileges of the clinical care provider based on the role the provider fulfills within their entity
4. Health Information Service Provider who maps the licensing and certification information
5. Incident control personnel who request confirmation of the medical credentials of a clinical care provider
6. Incident control personnel who request confirmation of the public safety credentials of an on-site law enforcement care provider
7. Emergency Communications System (ECS), on-site, ED or other emergency care provider who requests access to emergency information
8. ECS, on-site, ED, or other emergency care provider who seeks to send emergency information

2.1.1 THE EMERGENCY COMMUNICATIONS SYSTEM ACTOR AND FUNCTIONS

In the past, emergency medical response has generally been viewed as a voice call to 9-1-1 followed by the dispatch of an EMT or other first responder who provides stabilizing on-site care to a patient and transports them to a hospital for treatment. That responder typically had very limited information about the patient or hospital resource availability. This ER-EHR Use Case conceives of a much broader and richer information environment in which both medical and non-medical actors play critical roles, contributing, sharing and using information to create more informed and efficient emergency medical response.

9-1-1 call centers, Dispatch, and Emergency Management are important actors in the provision of emergency medical care and response to an incident. Each actor represents distinct functions. Often these are done in entirely separate locations by separate departments of local and state government (or companies under contract to them). Furthermore, involvement of these actors may vary depending on the location or nature of the incident. The advent of modern information technology (e.g., network-centric architectures) is expanding the traditional functions of these three actors/functions, adding capabilities and extending their role in emergency response from one time events (e.g., take a call, dispatch an ambulance), to on-going support of an incident and making the information available to all directly or indirectly involved. Network-centric architecture is favored because it allows these functions to be performed in different places, by different parties within the continuum of care.

The ER-EHR Use Case includes these actors in the initiation of the encounter record and subsequent sharing and use of the expanding amount of data about victims and incidents. Because these actors can play very different roles in different areas and different incidents, as a technical and architectural convenience within the ER-EHR Interoperability Specification, we use the encompassing terms “Emergency Communications System (ECS)” to represent the future functions of 9-1-1/Public Safety

Answering Points (PSAPs) (and the information sources and parties, public and private, that connect to it), Dispatch (including EMD), Emergency Communications Systems, and Emergency Management/Emergency Operations Centers (EOCs), whether they are provided in one or more locations, and whether or not they are provided virtually.

We note that they, like all participants in the ER-EHR Use Case, are "architecturally equal", i.e. they must all be equally interoperable. Their rights to send and receive data vary based on policy decisions, not architecture or technology use. The ECS Actor logically includes the following, either as physical entities or functions:

- 9-1-1 (also referred to as Public Safety Answering Points or PSAPs) is the public's point of contact with the emergency medical response system. This includes both individual 9-1-1 callers, and public and private data sources initiating a response request (e.g., police communicating the need for emergency medical response and the identity of the victim; telematics automatic crash notification; heart monitor alarm; hazmat truck crash indication), or providing information about the request. This function includes gathering as much relevant data on the victim and the incident as quickly as possible from additional sources, including accessing Personal Health Records (PHR), Emergency Contact Registries (ECON) and/or Electronic Health Records (EHR). It is important to note, however, that on-site care providers (like any other authorized party) may access and exchange patient-specific historical health information (i.e., PHR, ECON, EHR) independent of the ECS. In events such as a pandemic flu where the traditional paradigm of rushing victims to hospitals for care may be reversed, the 9-1-1 center may become the access to a form of Virtual Consult, and many of the functions described in the Use Case and herein as being done by EMS or emergency rooms may be handled virtually through 9-1-1 or related emergency communications capabilities. The creation of an incident encounter record begins at this point. The information technologies of choice within 9-1-1 centers are a computer-aided dispatch system and a records management system. Interoperability needs to be achieved between these systems. These may then need to interoperate with heterogeneous systems among mobile EMS (or other public safety) units
- Dispatch is when an ambulance, fire truck, helicopter and/or other resources are sent to the scene. Often voice calls and small amounts of associated data are transferred from PSAPs to separate Emergency Medical Services (EMS), fire and/or police dispatch. There are increasingly sophisticated protocols with associated decision support tools, which are generically called Emergency Medical Dispatch (EMD). EMD systems today include functions that are traditionally thought of as EMS. For example, most include the option of "pre-arrival instructions" (e.g., how to help a citizen birth a child). These will become even more sophisticated with the new data being discussed herein. The information technologies of choice are a computer aided dispatch system with EMD response protocols and a records management system. Interoperability needs to be achieved between these heterogeneous systems
- Emergency management is wholly different. It is not concerned with individual events or individual patients, but instead with large-scale disasters, aggregates of patients (e.g., 40 burn patients, 10 dead, and 23 with serious head injuries) and the resources needed to treat them (from skilled people, to staffed hospital beds, to supplies). Traditionally, an Emergency Operations Center (EOC) might

typically be a large conference room with representatives from each function sitting in front of a computer and telephone. Now the information technology of choice is a Consequence Incident Management System (CIMS) application that can be accessed from anywhere. It should be interoperable with the operating IT systems of other emergency agencies so it can be fed data. Unlike 9-1-1 and EMS, emergency management has an existing, near real time state and national reporting structure

- Emergency Communications System. The best practice view of the future is a network-centric state or regional system where different participants have rules-based access to information, software applications, and decision support applications, when and where they need those, rather than in defined physical locations. In such a system each function may have its own software application (e.g., CAD, CIMS), but these are interoperable with each other. EOCs and ECSs may be physical or virtual entities, but they will provide on-going information technology and communications support to all the responders to an incident – whatever its type or size. This includes supporting the functions discussed above of 9-1-1, Dispatch, and Emergency Management, and also EMS, law enforcement, hospitals, National Guard, transportation, and others

Functional roles and the information they need will differ. But from an information technology architecture standpoint these actors' interoperability requirements are the same. They are nodes on the emergency medical response network. Indeed, in this respect, they are exactly the same as every other function: EMS, air transport, hospitals, urgent care, public health and law enforcement. They need to be able to send (contribute) and receive standardized data, using standardized messaging protocols.

2.2 USE CASE REQUIREMENTS

This section describes the Use Case requirements and outlines all the given scenarios at a high level. The Use Case is driven by the requirements of emergency responders for timely electronic access and exchange of:

- Patient-specific historical health information (such as a Personal Health Record (PHR)), relating to the assessment, stabilization and treatment of the victims of emergency incidents
- Incident information
- Information (on a treatment non-interference basis) to facilitate family member reunification and expedite notification of next-of-kin following such incidents

Incidents can range from individuals suffering from routine events such as motor vehicle crashes or acute episodes of illness, to large groups of people suffering as the result of mass casualty incidents including natural disasters and terrorism (e.g., small and large scale incidents as further described above).

The Use Case describes the role of an Emergency Responder Electronic Health Record (ER-EHR) comprising at a minimum: emergency contact information, demographics, medication, special needs (ventilators-wheelchair etc…), allergy and problem list information that can be used to support emergency healthcare activities. Additionally, the Use Case describes the interactions with PHRs/ECONs/EHRs, both using and updating them. It also describes the shared data needs to meet the differing requirements of

the emergency responders. There cannot be a “minimum data set” because different actors have different information needs, and those information needs will vary by incident type.

Three perspectives are defined; ECS and on-site care, emergency care and definitive care. Each of these perspectives may provide actual and/or virtual care. In addition, for the sake of simplicity, we use description of Emergency Communications System (ECS) (described in Section 2 below) to include a variety of persons, places and functions, including the functions of 9-1-1, dispatch, emergency management, and on-going communication/IT support to emergency response and care.

In this Use Case, ECS staff receives reports of an incident and gathers information on the event and the victims from public and private sources, such as a Personal Health Record (PHR), Emergency Contact Registry (ECON), and/or Electronic Health Record (EHR) provider. They make initial dispatch decisions, search or query for the patient’s PHR/ECON/EHR, start an episode of care record and share information with the on-site care providers as they proceed towards the incident. Trained emergency dispatch staff, may also provide standardized pre-arrival instructions. It is important to note, however, that any emergency care provider may access and exchange patient-specific historical health information, (i.e., PHR, ECON, EHR) independent of the ECS. The on-site care providers typically include Emergency Medical Technicians (EMTs), Law Enforcement and Fire personnel. They can also include, uniformed services medical personnel and civilian disaster medical assistance teams (DMATs). EMTs and/or on-site care providers will assess and stabilize the patients’ medical conditions, extricate them from dangerous locations, perform triage, and evacuate them to a temporary or permanent medical treatment facility (MTF) to receive emergency care. On-site care providers, typically law enforcement personnel, will make reasonable attempts on a treatment non-interference basis to positively identify patients. On-site care providers usually work outside MTFs, except in the military and Public Health Service (PHS) where they may set up and staff Battalion Aid Stations and Federal Medical Stations (FMS) respectively.

Clinical care personnel operating within an MTF provide emergency care. They usually work in an Emergency Department (ED) or equivalent military or federal facility, evaluating and or treating patients before they are discharged, transferred or admitted to an inpatient facility, or are deceased. As appropriate, clinical care personnel may also provide virtual consults. These include physicians, nurses, advanced practice nurses (e.g., nurse practitioners, nurse anesthetists), physician’s assistants, military corpsmen and all other clinical and ancillary personnel at an MTF. A major disaster may also require that urgent care, nursing homes, auxiliary care sites (ACS), surge units, and other treatment facilities shall have access to the information and information technology applications discussed herein.

Definitive care is given by non-ED clinical personnel providing acute, rehabilitative, or custodial care. They evaluate and treat patients in locations other than an ED, such as acute care hospitals, specialty hospitals, dialysis centers, nursing homes and other facilities. These personnel may include physicians, nurses, therapists, technicians, and others.

The ER-EHR Use Case requires the deployment of standardized, widely available and secure solutions for accessing and exchanging healthcare and incident information in all types of incidents (e.g., small and large scale incidents as further described above). Specifically, it requires:

1. The ability to exchange ER-EHR information (i.e., PHR, ECON, EHR) and/or Episode of Care record and the ability to access third party information about a patient/victim or an incident from the wide variety of actors that may be involved in the response to an emergency situation
2. The ability to electronically download and automatically enter patient-specific historical health information, such as Patient ID, ECON, PHR and/or EHR data into an Episode of Care record (including a pre-hospital Patient Care Report (PCR)) supporting real-time messaging of data to Emergency Department Clinicians and other authorized parties
3. The ability on treatment non-interference basis to ascertain positive patient identification, facilitate family reunification and expedite next-of-kin notification
4. The ability to document and electronically share data from the current emergency encounter or the full Episode of Care record
5. The ability for ER-EHR and PHR providing systems to support remote consults
6. The ability to provide decision support software at each step of emergency medical response, which may include algorithms, dashboards, status reports and views
7. The ability of monitoring device data to be entered automatically into a PCR and/or encounter record and provide alerts based upon triggers
8. The ability to distribute Situational Awareness Reports (or let various actors have access to the data streams about the emergency event). “Situational Awareness Reports” can be categorized as
    a. Situational centric (e.g., incident description and status)
    b. Patient centric (e.g., demographics, emergency contact information, and present episode of care)
    c. Resource centric, (e.g., hospital personnel, bed, specialty, ER status and responder resource and personnel status)
    d. Public health centric (e.g., anonymized data)

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. Note that for each action, all information exchanges shall be auditable.

Three tables are provided, one for each scenario perspective; ECS and On-Site Care, Emergency Care and Definitive Care.

Table 2.2.1-1 illustrates the mapping between the business actors and their Use Case requirements for the scenario perspective of ECS and/or On-Site Care.

Table 2.2.1-1 Mapping of Use Case Requirements to Interoperability Requirements – ECS and On-Site Care

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR		Scenario Perspective 6.1 ECS and On-Site Care	EVENT: 6.1.1 On-Site Management and Coordination	ACTION: 6.1.1.1 On-Site care providers are dispatched. Patient information from Emergency Communications Systems will be communicated to On-Site care providers. Emergency medical operations personnel coordinate response deployment. Note: Information about the incident and the patients is collected from various sources: 9-1-1 calls, third party data bases, Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR). An emergency care record is begun. On-Site care providers are dispatched based on initial triage decisions and resource information.	DATA: Patient's name, location, chief complaints, key patient-specific health information, incident information. For small scale incidents, basic information such as patient's name, location, gender, and chief complaint are gathered by the 911 telecommunicator from the individual making the emergency call when possible. Data from private sources such as automaker Telematics Service Provider (TSP) crash description information may also be available. Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) data, combined with the above, can be critical to patient identification, proper triage, and pre-arrival instructions. For larger scale incidents, dispatchers may gather less specific information about individual patients. Information provided by the caller on the size and nature of the incident, and characteristic injuries of the patients associated with the incident will allow the proper personnel/units/apparatus to be dispatched. An emergency care record is commenced and all gathered information is sent to the responding on-site care team answering the dispatch call. Note: This action is performed by the 9-1-1 and Dispatch functions, which gather as much information about the patient and the incident until the on-site units arrive, and then provide IT support to them. EMD is informed by oral questions posed by the 9-1-1 call taker; future generations of EMD will electronically accept data inputs from multiple sources. All data gathered is shared with the on-site care providers as they approach the incident. It is important to note, however, that on-site care providers may access and exchange patient-specific health information (PHR, ECON, EHR) independent of ECS. In the future, the EMD protocol of questions for 9-1-1 telecommunicators to ask emergency callers need to be able to be altered automatically by authorized public health officials to ask specific questions if threshold indicator answers have been given (e.g., “any recent foreign travel?” If “yes”, ask the following four questions”). This requires interoperability between ECS systems and public health. Dispatchers are informed about a variety of resource information with standardized data messages: for example, hospital, bed and specialty availability; closest ambulance and air transport availability. Note: Public health messaging and data systems need to be interoperable with EMD software in Dispatch entities. Data needs to be able to flow both ways. These interactions account for the other possibilities such as "discharged,” deceased, as do emergency care and definitive care with the associated patient information updates.	Data: 1,2,6,7,11,12,16 Issues: None

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	ECS	Scenario Perspective 6.1 On-Site Care	EVENT: 6.1.1 On-Site Management and Coordination	ACTION: 6.1.1.1 On-Site care providers are dispatched. Patient information from emergency dispatch center systems will be communicated to On-Site care providers. Emergency medical operations personnel coordinate response deployment.	DATA: Patient's name, location, chief complaint, other available and relevant data, including patient-specific historical health data from a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR), mechanism of injury, and situational awareness. For small-scale incidents, information such as patient's name, location, chief complaint and other patient-specific historical health data from a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) are gathered by the 9-1-1 communicator from the individual making the emergency call, and from other data sources, when possible. Decision support software such as EMD and injury predictors may act on the data on a dynamic basis throughout the response process to educate the form and type of Dispatch, the type of treatment facility, and the form and type of care. For larger scale incidents, dispatchers and others may be able to gather less information about individual patients. Information provided by the caller (or other information source to the ECS) on the size and nature of the incident, and characteristic injuries of the patients associated with the incident assist in dispatching the proper personnel/units/apparatus.	Data: 1,2,6,7,12 Issues: None
	ECS			ACTION: 6.1.1.2 Situational Awareness Report from Dispatch/EOC to ED facility and Other Providers	Gather information to keep all involved entities informed of the situation. Depending on the needs and requests of the different actors, local policies and legal requirements, this shared data and Situational Awareness Reports will differ by actor and incident type. Medical, patient, resource, incident, traffic, environmental and other information make up Situational Awareness Reports. For interoperability purposes, this means that every entity in the emergency medical response process (medical or not) needs to be interoperable with emergency messages and data from a wide variety of emergency and non-emergency sources, in addition to messages and data elements that make up the ER-EHR. This is a continuous process throughout an incident. Note: Within ECS, 9-1-1/Dispatch and an Emergency Operations Center (when it is activated in a disaster), systems monitor the number and types of patients, number of ambulances and other resources in an area, and availability of staffed beds. They receive data from individual line agencies, aggregate the information and send situational messages and reports to appropriate parties.	Data: 7,11,12 Issues: 3

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	On-Site Care Providers (often EMTs)	Scenario Perspective 6.1 On-Site Care	EVENT: 6.1.1 On-Site Management and Coordination	ACTION: 6.1.1.3 On-Site care providers assess the situation, determine the scope of required care and evacuation, notifying responding agencies of the situational assessment, and organize additional units if required.	Emergency personnel arrive on-site and perform an assessment of the incident site to determine the scope of medical care and evacuation required, and/or this is done remotely by the ECS. In certain incidents, care and evacuation will require multiple On-Site teams. If the initial On-Site team recommends that additional resources are required such as additional EMS teams, fire and rescue, police and other response units, they shall be able to convey this information back to the Emergency Communications System by voice and data messages. After On-Site assessment and communication with the Emergency Communications System, the need for an On-Site triage collection point and a medical incident command post may be established as part of the overall Incident Command System (ICS) response, if ICS has been activated. Until an incident command post is operational, the first team may serve to organize subsequent arriving units. Once the command post has become operational, the incident commander will assume command over the incident site and all assigned personnel. Depending on the type of incident, the incident commander may or may not be from a medical profession. Note: Depending upon state or local policies for a Mass Casualty Incident, first responders may be required to place a triage tag on each patient. This tag usually displays triage condition, chief complaint and an ID for each patient. It may also be a bar code identifier or RFID tag for the emergency encounter record and EHR.	Data: 12 Issues: 3 may apply
	On-Site Care Providers (often EMTs)		EVENT: 6.1.2 Continue collection of Patient information	ACTION: 6.1.2.1 Collection of patient information is for each instance of care.	On-Site crews start with the information received from the Emergency Communications System to begin collection of On-Site information. This may take several forms similar to the traditional ambulance pre-hospital Patient Care Report (PCR) or a field medical card, but the emergency care record needs to function as a dynamic continuity of care record, and provide access to the relevant information gathered to date on the victim, and decision support tools that acted on that information. The patient information is entered and verified with patient, family members, or others who may have the information at the incident scene, or from third party Personal Health Record (PHR), Emergency Contact Registry (ECON), Electronic Health Record (EHR) databases. PHR, ECON and/or EHR data and information from electronic monitors, e.g., pulse oximetry and blood pressure may be entered into the Patient Care Report (PCR) automatically. The IT systems of the responders should be capable of sending alarm messages to various parties and roles based on absolute thresholds of patient data (e.g., low blood pressure), and/or negative trends (e.g., falling Glasgow coma scores from 9-1-1 call to scene to ambulance), or falling pulse oximetry.	Data: 13 Issues: 3, 4 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
			EVENT: 6.1.3 Access additional patient health information	ACTION: 6.1.3.1 Additional patient information may be accessed and viewed from health information repositories such as existing patient electronic health records (either from an individual healthcare entity or a health information service provider), handheld storage devices, or web-hosted personal health records. Other sources such as patient registries may be accessed to view information such as emergency contact information and prescriptions. The queries for information are secondary to the stabilization and treatment of the patients. Note: Other sources of information may be accessed such as an Emergency Contact Registry (ECON) to reach persons who have knowledge about certain aspects of the patient's health, such as pre-existing conditions, allergies, medications, primary care physician, etc. ACTION: 6.1.3.1A Information from the Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) is not available (this would include jurisdictions that have not yet implemented electronic On-Site care information collection).	ECS and/or On-Site care providers, typically law enforcement, will make reasonable attempts on a treatment non-interference basis to positively identify the patient and to obtain a Patient ID. If the patient can be identified the ECS and'/or On-Site care providers send a query to receive relevant patient-specific historical health information from a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR). Both the query and retrieval are auditable. If the patient can't be identified, a patient identifier is added to the ECS and/or On-Site information. Note: The information source could also be a person at the scene or a 9-1-1 caller who has basic knowledge about the patient's health condition. Note: On a treatment non-interference basis, ECS and/or on-site care providers, typically law enforcement, in addition to attempts to positively identify patients, will also facilitate family member reunification and expedite next-of-kin notification. Note: ECS and/or on-site care providers will have the ability to electronically download and enter automatically Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) data into a pre-hospital Patient Care Report (PCR) supporting real-time messaging of Patient ID, ECON, PHR and/or EHR data to and from Emergency Department Clinicians and others. A: If information is not available from the Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR), the ECS and/or On-Site crew will enter as much information as possible in a manual mode, on a treatment non-interference basis. The information source could be the patient, family member, or friend who has knowledge about certain basic aspects of the patient's health condition, such as allergies, past episodes of care, current medications, primary care physician, etc. Note: The patient needs to be designated to a medical treatment facility; this action may be taken at any point prior to and during transportation.	Data: 1,2,3,4,5,8,9,10 Issues: 2,3,4,7 may apply (A): Issues 3,4,9 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
			EVENT: 6.1.4 Assess, triage and treat patient	ACTION: 6.1.4.1 EMTs will assess the patient's condition, develop a working diagnosis, determine triage category, and treat the patient's injuries and/or illnesses in order to stabilize the patient for transportation to the designated medical treatment facility. (Note: the patient may not have sufficient injuries to require transport) Note1: ECS may provide pre-arrival medical instructions to persons on the scene. ECS may provide Virtual Consult. Note 2: Decision support software may make predictions of likely injuries, and give appropriate protocol for response.	Based on EMD protocols, ECS may provide pre-arrival instructions. On-Site care providers perform an assessment of the patient's condition and develop a working diagnosis. Based upon predetermined triage criteria, the On-Site care team makes a decision regarding the level of care required (e.g., transport to the closest hospital or to a trauma center), the mode of transportation (ground or air) required by the patient, and the priority of movement (delayed, immediate, minimal or expectant). The On-Site team reviews the updated On-Site information to identify risks associated with the patient's pre-existing conditions, medications, allergies, and then administers basic treatment of patient injuries and/or illnesses accordingly, in order to stabilize the patient for transportation to the designated medical treatment facility. If available, they may utilize virtual consultation by a qualified clinician to assist in the assessment process. ECS shares data with ED, medical control, and other appropriate stakeholders.	Data: 2,6,13 Issues: 2,6 may apply
			EVENT: 6.1.5: Update On-Site care information	ACTION: 6.1.5.1 The On-Site care treatment team updates the On-Site care information on the treatment provided Note: Hospitals are continually reporting their bed and specialty services availability via standardized messages to ECS	The patient's destination, mode of transport and priority of movement are sent by the On-Site team to the ECS, or determined by the ECS.	Data: 2,6,13 Issues: 3,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
			EVENT: 6.1.6 Transport patient	ACTION: 6.1.6.1 Transport the patient to the designated medical treatment facility.	On-Site care information is updated with any treatment rendered en route. Any medications, changes in vital signs, etc. are updated in the Patient Care Report (PCR). This may include information feeds from automated medical devices such as blood pressure monitors. The recording of the information may take place on-site, in the transport vehicle or at the destination facility. Note: We need interoperability between the pre-hospital Patient Care Report (PCR) and electronic monitoring equipment in ambulances/aircraft and the Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) systems. We need interoperability of voice to text so that treatment at the site and enroute can be recorded in real time, without imposing additional responsibilities on EMTs, and thus is useful to the receiving facility in real time. Note: Although not stated, the patient disposition may be similar to 6.2.6.1a, c, d, e. These alternative dispositions are not significant because they do not impact the requirement for HITSP Interoperability Specifications.	Data: 2,6,13 Issues: 2,3,9 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
			EVENT: 6.1.7 Provide Information	ACTION: 6.1.7.1 The ECS and On-Site care information is made available to the receiving facility. ACTION: 6.1.7.1A Power or communication failures	Receiving facilities regularly report to the ECS their status, the numbers and types of staffed beds, and the types of staffed services available. On-Site care information is made available to the receiving facility and/or the appropriate repositories through the ECS network, or directly. In certain cases, information will be provided by On-Site providers to air ambulance services. The On-Site treatment team updates the Patient Care report (PCR) with treatment provided to the patient by the transportation team (if required). If the patient requires transport, the On-Site treatment team transmits the updated encounter record(s) to the ECS system so it can be accessed by appropriate parties. The designated receiving facility accesses the information so that appropriate resources (including clinicians) may be available at the time of patient arrival. Appropriate information is sent to (or accessed by) EOCs and public health agencies that use the information to track health resources and conduct biosurveillance respectively. The information taken from ECS systems for public health and EOC purposes is usually non-identifying or pseudonymized. Note: In this action data are likely transmitted to an EOC system, and depending on business rules, provided automatically to other appropriate actors. A: On-site systems should have backup power to avoid power interruption during patient care. Paper forms are kept in reserve so they can be used if power is lost. Once power and/or IT communications are restored, the information should be entered into the electronic health record, after the fact, possibly by scanning the record. Similarly, clinical summaries should be printed at patient handoff in the eventuality that the electronic copy is lost. In addition to the business actors describe herein, a variety of agencies may require that they receive subsets of the information collected. A commonly accessible registry for organizations needing data and the access control and identity management for those organizations must be provided. The organizations need to register the services they offer in a particular area, what incident information they want, for what geographic areas, and to what electronic address(es) they want information sent. Similarly, communicating across multiple networks and domains requires a shared, standardized, and role-based identity management and access control system, and data rights management service. These are called “core services.” NOTE: The American Red Cross reunification data base and the National Center for Missing and Abused Children (which has been given responsibility for reunification of Children with families) have been designated as national repositories.	Data: 2,6,13 Issues: 1,2,3,4,8,9 may apply A: Issues 1,2,3,4,7,8,9 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Service Providers & Other Healthcare Systems				Intermediary for 6.1.3.1 and 6.1.4.1	Intermediary for 6.1.3.1 and 6.1.4.1
Emergency Responder EHR	Facility EHR Repository (EHR)				Intermediary for 6.1.3.1	Intermediary for 6.1.3.1
Emergency Responder EHR	Emergency Contact Registry (ECON)				Intermediary for 6.1.3.1	Intermediary for 6.1.3.1
Emergency Responder EHR	Personal Health Record (PHR)				Intermediary for 6.1.3.1	Intermediary for 6.1.3.1
Emergency Responder EHR	Emergency Dept. Staff				Intermediary for 6.1.6.1	Intermediary for 6.1.6.1
Emergency Responder EHR	Public Health Agencies				Requires bidirectional interoperability with other actors (e.g., to provide protocols and collect data).	Data: 2,6,13 Issues: 1,2,3,4,8,9 may apply A: Issues 1,2,3,4,7,8,9 may apply

Table 2.2.1-2 illustrates the mapping between the business actors and their Use Case requirements for the scenario perspective Emergency Care.

Table 2.2.1-2 Mapping of Use Case Requirements to Interoperability Requirements – Emergency Care

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Emergency Communications Systems (ECS)	Scenario Perspective 6.2 Emergency Care Perspective	EVENT: 6.2.1 Emergency care site management and coordination	ACTION: 6.2.1.1 The emergency care facility is notified by the Emergency Dispatch Center regarding the in-bound patient.	ED clinical care personnel are notified by the Emergency Communications System of the in-coming patient. (Today this is often accomplished by verbal radio communication from an ambulance. In the future, this will generally be a message initiated by the EMS staff transporting the patient, which will also contain the patient encounter record. Depending on the network, this may involve human intervention at an ECS facility, or may simply pass through ECS IT services. Thus all three systems need to be interoperable). If information recorded by ECS functions and/or during On-Site care and transport is available, ED clinical care personnel receive and review the record (chief complaint, incident information, emergency contact information, demographics, diagnosis, triage outcome, trend lines for vital signs, treatment provided; decision support indications) to ensure appropriate resources are available (e.g., specialists, lab tests, blood products, radiology etc) to appropriately treat the patient upon arrival. An alert may be sent to the patient's primary care physician by the ECS or ED (if applicable), or by a private data service. Note 1: Reasonable efforts to notify the patient's immediate family or other emergency contacts are performed as soon as possible. Note 2: As appropriate, ED clinical care personnel may also access and review patient-specific historical health information from the Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) data. Note 3: The functional actors in this action will differ based on the location, nature, and size of the incident.	Data: 1,2,6,13 Issues: 2,3,4,5,6 may apply
Emergency Responder EHR				ACTION: 6.2.1.2 ECS systems send Situational Awareness Reports to all involved medical units and systems. Note: For interoperability analysis convenience, the EOC has been subsumed within the ECS. In actual environments, they may be physically separate; but, electronically linked and have the same interoperability requirements.	As information is gathered from a number of sources, ECS systems will prepare and disseminate situational awareness messages and reports keeping all involved (or interested, e.g., mutual aid partners) and authorized entities informed of the situation. Note: Throughout an incident, non-patient messages about the incident will flow among all the entities involved. These make up Situational Awareness Reports when aggregated. In a large incident the overall situational awareness reporting function is done by emergency management and the action will be performed by a CIMS system when an Emergency Operations Center is activated.	Data: 12 Issues: None

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Emergency Dept. Staff	Scenario Perspective 6.2 Emergency Care Perspective	EVENT: 6.2.2 Episode of Care Record	ACTION: 6.2.2.1 The patient is logged into the emergency care facility, thus starting the Episode of Care Record for this instance of care. ACTION: 6.2.2.1A Patient is dead on arrival. ACTION: 6.2.2.1B Power or communication failures ACTION: 6.2.2.1C Patient cannot be identified.	When the patient arrives at the ED, clinical care staff will log the patient into the system used at their facility and create a record for each patient and for each encounter. If it is still lacking, registration information (emergency contact information, patient demographics, employer, health insurance, etc.) is added to the clinical information derived from the ECS and On-Site care record. A: A new phase of the emergency care record is begun for the patient. If it was not added by ECS or by the On-Site team directly or from third party sources during those phases, registration information (emergency contact information, patient demographics, employer, health insurance, etc.) is added to the clinical and other information already in the record. Once the patient is pronounced dead by a physician, the emergency care is so annotated and the encounter record is closed. B: Devices go to generator or battery backup, and off line operation. If power outages are long term, a paper copy of the health record is begun for the patient. Once power and IT communications are restored, the information can be automatically uploaded or entered into the electronic Episode of Care Record, possibly by scanning the record. Additional sites at remote locations and redundant. Resilient links to them must be employed as backups for the primary repository in case of widespread communications and power outages caused by natural or man-made disasters. C: An emergency care record is started with a unique patient identifier as soon as any agency in the chain knows there is a patient or victim. If and when the patient's identity is established and validated, this is added to the record. This should allow access to additional sources of information about patient-specific historical health information (e.g., Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR). Note: In ACTION: 6.2.2.1c when a patient cannot be identified, a unique "temporary" patient identification number should be assigned.	Data: 1,2,6,14 Issues: 2,3,4,5,6 may apply A: Issues 4,5,6 may apply B: Issues 1,2,3,4,7,8 may apply C: Issues 1,2,3,4,7,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.2.3 Access additional patient health information Note: This can happen anywhere in the patient care chain.	ACTION: 6.2.3.1 Additional patient information may be accessed and viewed from health information repositories such as existing patient electronic health records (either from an individual healthcare entity or a health information service provider), handheld storage devices or web hosted personal health records. Other sources such as patient registries may be accessed to view information such as emergency contact information, prescriptions, and insurance claims databases (if available). Note: Other sources of information may be accessed such as emergency contact registry to reach persons who have knowledge about certain aspects of the patient's health, such as pre-existing conditions, allergies, medications, primary care physician, etc. ACTION: 6.2.3.1A Patient presents without an ECS/ On-Site care record. Note1: Additional patient information may be accessed and viewed by authorized entity in the chain of emergency medical response (i.e. ECS, On-Site, ED) Entity in the chain of emergency medical response (i.e. ECS, On-Site, ED)	As soon as the patient identity is established, a query is sent to the Healthcare Information System (HIS) for information on the patient. The local HIS utilizes available information exchange services to request, locate, and retrieve patient-specific information, such as a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) from other sources. Such information may reside within a regional RHIO/HIE, with commercial entities, with local ambulance services, and other commercial provider services. The ECS, On-Site care information and the retrieved Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) are accessible to the clinical staff and should be integrated into the Episode of Care Record. For ease of use, the information may be selected and formatted according to the clinical staff's preferences. Indeed, wherever feasible, time and expense should be saved by pre-populating fields with information that is already known about a patient (e.g., Ambulance companies often maintain data bases on persons they have previously transported) Note: The information source could also be a person at the scene who has knowledge about the patient's health condition. A: Patients who enter the emergency facility through a means other than contacting ECS or On-Site care, such as self-referral, brought in by family or friends, etc. will have their relevant emergency contact information, demographics, allergies, and past episodes of care captured by the ED staff who shall log them in and start a new emergency care encounter record. A query for the patient's health information will be sent out through the HIS and ECS. The local HIS utilizes available information exchange services to request, locate, and retrieve patient information from other sources. Note: Interactions of medical records/encounter records with decision support software may suggest what may be wrong (predictor) with the patient and suggestions on patient treatment (treatment protocol). Note: Decision support software should suggest to dispatchers and on-site personnel where to send patients by combining patient information from the encounter record with resource availability information from hospitals reported regularly using the OASIS EDXL HAVE message.	Data: 1,2,6,14 Issues: 2,3,4,5,6,7 may apply A: Issues 2,3,4,5,6,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.2.4 Assess, triage, perform tests and treat patient	ACTION: 6.2.4.1 The clinical staff reviews treatment provided by On-Site care providers and validates their initial assessment, adding any additional observations, and determining the patient's triage category. Clinical personnel treat the patient's injuries or illness. ACTION: 6.2.4.1a Access the patient's EHR via emergency facility's IT systems integrated with EHR repositories.	Based on information developing at the site or in transit to an ED (or changes by the availability of services at a medical facility), medical control within ECS may change the initial assessment and re-route the patient to another treatment facility. The clinical staff verifies and validates the On-Site care provider's initial assessment, adding any additional observations and making triage decisions as to the priority for treatment. The outcome of this activity would be a working diagnosis of the patient's conditions. If available, the clinical staff may utilize virtual specialty consultation by a qualified clinician to assist in the assessment process. The patient's injuries or illnesses are treated with the clinical staff referring to the Episode of Care Record as part of the process. A: If the treatment facility possesses an IT infrastructure with its own EHR, the demographic and clinical information contained in the Episode of Care Record will be uploaded into the facilities' repository and used to populate/update the patient's EHR.	Data: 1,2,6,10,13,14 Issues: None A: Issues 3,4,7,8 may apply
Emergency Responder EHR			EVENT: 6.2.5 Input information in emergency care record	ACTION: 6.2.5.1 As treatment progresses, information such as the results of diagnostic tests, treatment, and medications rendered, and any changes to the treatment plan are entered into the emergency care record. Information is continually sent to public health agencies for population health monitoring purposes.	Information is added to the Episode of Care Record by the clinical care staff. This will update the working diagnosis, treatment rendered, medications given, and profiles for limits to Activities of Daily Living (ADL). Diagnostic testing results are also collected and updated into the Episode of Care Record. This may include information feeds from electronic medical devices such as blood pressure monitors.	Data: 1,2,6,14 Issues: 2,3,4,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.2.6 Complete emergency disposition; Provide information	ACTION: 6.2.6.1 Once treatment is complete, the patient is directed to any follow-on care as deemed necessary. ACTION: 6.2.6.1A Patient is discharged. ACTION: 6.2.6.1B Patient is admitted to inpatient status. ACTION: 6.2.6.1C Patient is transferred to another in-patient facility. ACTION: 6.2.6.1D Patient is deceased.	Once the patient has received the needed care at the emergency facility, the patient encounter disposition summary is prepared and in action 6.2.6.2 is sent to the appropriate follow-on facility if the patient is not discharged. A: If the patient requires no further treatment, the appropriate notations are made in the emergency care record by the clinical care staff, closing the patient encounter. B: If the patient is admitted to the definitive care portion of the facility, the emergency care is so notated by the clinical care staff and is closed for that patient encounter. The emergency record is sent by the clinical care staff to the admissions office and the receiving ward. C: If the patient is transferred to another facility, the Episode of Care Record is so notated by the clinical care staff and the patient encounter is closed. The Episode of Care Record will be sent to the new facility so its staff can prepare for the patient. This may be done in the form of a notification to extract the record from the facility EHR repository. D: If the patient dies in the emergency care facility, a notation is made in the emergency care record by the clinical care staff of the time and circumstance of the death and the record is then closed for that patient encounter. Notification is sent by the clinical care staff to the Medical Examiner (currently by telephone) of the date and cause of the patient's death, and to the ECS for redistribution to appropriate stakeholders.	Data: 1,2,6,14 Issues: None A: Issues 2,3,4,6,7,8 may apply B: Issues 2,3,4 may apply C: Issues 2,3,4,5,6,7,8 may apply D: Issues None
Emergency Responder EHR			EVENT: 6.2.6 Complete disposition; Provide information	ACTION: 6.2.6.2 Once treatment is complete, information about the patient encounter will be available with other records relating to the patient, including (if they are available) any facility-based records and personal health records. It will also be available to the appropriate repositories.	Patient encounter disposition is transmitted via the HIS to the appropriate repository (or repositories). The Episode of Care Record is used to populate or update the patient's electronic health record and the PHR. Information exchanges may also occur with laboratories, pharmacies, blood banks etc. Information is sent to appropriate ECS systems and public health agencies to track health resources and conduct biosurveillance respectively. The information sent to ECS systems is generally non-identifying or anonymized/pseudo anonymized. With appropriate privacy protections, such as anonymization, patient information should be available for end to end system analysis and research.	Data: 1,2,6,11,14 Issues: 1,3,4,6,7,8 may apply
Emergency Responder EHR	Emergency Contact Registry (ECON)				Intermediary for 6.2.3.1	Intermediary for 6.2.3.1

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Service Providers & Other Healthcare Systems				Intermediary for 6.2.3.1	Intermediary for 6.2.3.1
Emergency Responder EHR	Personal Health Record (PHR)				Intermediary for 6.2.3.1	Data: 1,2,3,4,5,6,8,9 Issues: 1,3,4,6,7,8 may apply
Emergency Responder EHR	Another Facility				Receives data for own use Provides data, if requested. Bi-directional interoperability is required.	Data: 1,2,6,14 Issues: None A: Issues 2,3,4,6,7,8 may apply B: Issues 2,3,4 may apply C: Issues 2,3,4,5,6,7,8 may apply D: Issues None
Emergency Responder EHR	Medical Examiner/ fatality manager				Receives data for own use	Data: 1,3,4,5,6,8,9 Issues: None A: Issues 2,3,4,6,7,8 may apply B: Issues 2,3,4 may apply C: Issues 2,3,4,5,6,7,8 may apply D: Issues None
Emergency Responder EHR	Public health agencies				Requires bidirectional interoperability with other actors (e.g., to provide protocols and collect data).	Data: 1,3,4,5,6,8,9 Issues: 1,3,4,6,7,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Appropriate shared (HIS) repositories				Receives data for own use Provides data, if requested	Data: 1,3,4,5,6,8,9 Issues: None A: Issues 2,3,4,6,7,8 may apply B: Issues 2,3,4 may apply C: Issues 2,3,4,5,6,7,8 may apply D: Issues None

Table 2.2.1-3 illustrates the mapping between the business actors and their Use Case requirements for the scenario perspective Definitive Care.

Table 2.2.1-3 Mapping of Use Case Requirements to Interoperability Requirements – Definitive Care

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Clinical Staff	Scenario Perspective 6.3 Definitive Care Perspective	EVENT: 6.3.1 Access/Start EHR (if required)	ACTION: 6.3.1.1 Access existing facility electronic health record or start a new electronic health record if one does not already exist for this patient. ACTION: 6.3.1.1A Power or communication failures. ACTION: 6.3.1.1B Patient cannot be identified.	A query is sent by the clinical care staff to the facility database for existing information on the patient. A: If there is a general power failure, ECS entities and hospitals should shift over to generators. Devices should be able to operate without a network connection; storing and forwarding data when and if there are breaks in wireless communications with the ECS networks. A number of methods can be used to transfer data along with the patient when network access is not possible. Data can be stored on removal media. As a last resort, practitioners may resort to paper copies of the health record of the patient. Once power and IT communications are restored, the information can be re-entered into the electronic health record, possibly by scanning the record. Note: It is critical that all networks, servers, and data base systems used meet commercial best practices for redundancy and resilience, including "hot backup." B: A record is started with a patient identifier. Note: In ACTION: 6.3.1.1B when a patient cannot be identified, a unique "temporary" patient identification number must be assigned.	Data: 1,2,3,4,5,6,8,9,10,15 Issues: 1,2,3,4,7,8 may apply A: Issues 1,2,3,4,7,8 may apply B: Issues 1,2,3,4,7,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Emergency Communications Systems		EVENT: 6.3.1 Access/Start EHR (if required)	ACTION: 6.3.1.2 ECS system sends Situational Awareness Reports to all involved medical units and systems.	As information is gathered from a number of sources, ECS systems prepare and disseminate that data and Situational Awareness Reports, keeping all involved entities informed of the situation. In addition to the business actors described herein, a variety of agencies may require that they receive subsets of the information collected. Core services: A common registry for organizations needing data and the access control and identity management for those organizations must be provided. The organizations need to register the services they offer in a particular area, what incident information they want, for what geographic areas, and to what electronic address(es) they want information sent. Similarly, communicating across multiple networks and domains requires a shared, standardized, and role-based identity management and access control system, and data rights management service.	Data: 12 Issues: None
Emergency Responder EHR	Facility EHR Repository		EVENT: 6.3.2 Access additional patient health information	ACTION: 6.3.2.1 Access Electronic Health Record	The clinical staff sends a request to the HIS for patient information which may reside within its affiliated repositories. The ECS, On-Site information, emergency care record and the retrieved electric health record is accessible to the clinical staff.	Data: 1,2,3,4,5,6,8,9,10,15 Issues: 1,2,3,4,7,8 may apply
Emergency Responder EHR			EVENT: 6.3.2 Access additional patient health information	ACTION: 6.3.2.2 Where feasible, the emergency care record and any archival information (Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) should be integrated with the facility electronic health record.	The Personal Health Record (PHR), Emergency Contact Registry (ECON), and/or Electronic Health Record (EHR) data may be "view only", or if it can be integrated, it should be used by the clinical care staff to populate a patient record in the facility's patient management system. Note: It should be noted that this comment applies to all authorized business actors.	Data: 1,2,3,4,5,6,8,9,10,15 Issues: 1,2,3,4,7,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.3.3 Assess, perform tests, treat patient	ACTION: 6.3.3.1 The clinical staff reviews treatment provided in the emergency setting, makes an assessment, adding any additional observations, performs required tests, and treats the patient's injuries or illness. ACTION: 6.3.3.1A Patient notes from emergency care have been recorded in the EHR repository and clinical staff retrieves information.	While the patient is in transport or upon arrival of the patient at the treatment facility, the clinical staff reviews the emergency care record concerning treatment provided by emergency care clinicians, adding any additional observations. The outcome of this activity would be an updated working diagnosis of the patient's conditions. The patient's injuries or illness are treated with the clinical staff referring to the electronic health record as part of the process. A: The clinical staff sends a query via the in-house system (if applicable) requesting the Episode of Care Record health information for the patient. The information is received and the clinical staff combines this information with that from the electronic health record.	Data: 1,2,3,4,5,6,8,9,10 ,15 Issues: 6 may apply A: Issues 2,4,6 may apply
Emergency Responder EHR			EVENT: 6.3.4 Input informatio n in EHR	ACTION: 6.3.4.1 Information related to diagnosis, tests, and treatment is recorded in the patient's EHR and PHR. Information is continually sent to public health agencies for population health monitoring purposes.	Clinical care staff updates information to the electronic health record. The EHR is updated with the working diagnosis, treatment rendered, medications given, and profiles. Diagnostic testing results are updated into the electronic health record, ideally without additional entry requirements being placed on the clinical care staff. This should also include information feeds from automated lab systems and automated electronic medical devices.	Data: 1,2,3,4,5,6,8,9,10 ,15 Issues: 2,3,4,5,6,7,8 may apply

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.3.5 Complete disposition ; Provide informatio n	ACTION: 6.3.5.1 Patient disposition occurs. ACTION: 6.3.5.1A The patient is discharged. ACTION: 6.3.5.1B The patient is transferred to inpatient status at another facility. ACTION: 6.3.5.1C The patient is discharged with outpatient follow-up. ACTION: 6.3.5.1D The patient is transferred to another facility. ACTION: 6.3.5.1E The patient is deceased. ACTION: 6.3.5.1F The patient is discharged against medical advice.	Patient care information is available for access by authorized clinical care staff in other facilities via the HIS. A: If the patient requires no further treatment, the appropriate notations are made by the clinical care staff in the electronic health record, closing the patient encounter. The updated electronic health record information is sent by the clinical care staff via the HIS to the appropriate repository(ies) to be combined with the patient's electronic health record. B: The electronic health record is sent directly to the receiving facility. It is also available to the clinical care staff via query through the HIS. C: The updated electronic health record information is available to clinical care staff via query through the HIS. D: The updated electronic health record information is sent directly to the receiving facility and is also available to clinical care staff through query via HIS. E: If the patient expires in the definitive care facility, a notation is made in the electronic health record by clinical care staff of the time and circumstance of the death and the record is then closed for that patient encounter. Notification is sent by clinical care staff to the Medical Examiner (currently by telephone) of the date and cause of the patient's death and to the ECS for redistribution to appropriate stakeholders. F: A notation by clinical care staff is made and signed in the electronic health record, closing that patient encounter.	Data: 1,2,3,4,5,6,8,9,10 ,15 Issues: 2,3,4,6,7,8 may apply A: Issues 4,7,8 may apply B: Issues 1,2,3,4,5,6,7,8 may apply C: Issues 1,2,3,4,5,6,7,8 may apply D: Issues 1,2,3,4,5,6,7,8 may apply E: Issues None F: Issues None

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR			EVENT: 6.3.5 Complete disposition ; Provide information	ACTION 6.3.5.2 Release of information.	Information on the patient's present episode is sent by clinical care staff to the HIS where it is to be located with existing patient health information in the electronic health record. Appropriate information is sent to ECS systems and public health agencies that use the information to track health resources and conduct biosurveillance respectively. The information sent to ECS systems is non-identifying or anonymized. Note: A subset of the information (typically only name, location and emergency contact information) should be sent to the American Red Cross' server for its family reunification responsibilities and to the National Center for Missing and Exploited Children for its child reunification responsibilities.	Data: 1,2,3,4,5,6,8,9,10 ,12,15 Issues: 1,2,3,4,7,8 may apply
Emergency Responder EHR	ECS				Intermediary for 6.3.2.2	
Emergency Responder EHR	Service Providers & Other Healthcare Systems				Receives data for own use	Data: 1,2,3,4,5,6,8,9,10 ,12,15 Issues: None
Emergency Responder EHR	Emergency Contact Registry (ECON)				Intermediary for 6.3.2.2	Data: 1
Emergency Responder EHR	Personal Health Record (PHR)				Intermediary for 6.3.2.2	Intermediary for 6.3.2.2
Emergency Responder EHR	Appropriate Shared (HIS) repositories				Intermediary for 6.3.2.2	Intermediary for 6.3.2.2
Emergency Responder EHR	Other Third Party Data				Intermediary for 6.3.2.2. Requires bidirectional interoperability with other actors (e.g., to provide protocols and collect data).	

Use Case	Perspective/ Business Actor	Scenario	Event	Action	Interoperability Requirement(s)	Data Requirement Number & Issues
Emergency Responder EHR	Another Facility				Receives data for own use. Requires bidirectional interoperability with other actors (e.g., to provide protocols and collect data).	Data: 1,2,3,4,5,6,8,9,10 ,15 Issues: 2,3,4,6,7,8 may apply A: Issues 4,7,8 may apply B: Issues 1,2,3,4,5,6,7,8 may apply C: Issues 1,2,3,4,5,6,7,8 may apply D: Issues 1,2,3,4,5,6,7,8 may apply E: Issues None F: Issues None
Emergency Responder EHR	Public health agencies				Requires bidirectional interoperability with other actors (e.g., to provide protocols and collect data).	Data: 1,2,3,4,5,6,8,9,10 ,15 Issues: 1,2,3,4,7,8 may apply

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

Data Requirement Number	Description	Scenario
Data Requirement 1	Emergency Contact Information is provided, including (but not limited to): Emergency Contact Information	1,2,3
Data Requirement 2	Patient data are provided, including (but not limited to): Patient Demographics (Identity)	1,2,3
Data Requirement 3	Allergy data are provided, including (but not limited to): Allergy Information	1,2,3
Data Requirement 4	Medication History is provided, including (but not limited to): Medication History	1,2,3

Data Requirement Number	Description	Scenario
Data Requirement 5	Problem List is provided, including (but not limited to): Problem List	1,2,3
Data Requirement 6	Patient Location is provided, including (but not limited to): Patient Location	1,2,3
Data Requirement 7	Triage Category is provided, including (but not limited to): Triage Category	1,2,3
Data Requirement 8	Advance Directives information is provided, including (but not limited to): Advance Directives	2,3
Data Requirement 9	Previous Immunizations information is provided, including (but not limited to): Previous Immunizations	1,2,3
Data Requirement 10	Treatment History is provided, including (but not limited to): Prior emergency transport or ED visits (HITSP Gap) Treatment Histories (previous episodes of care)	2,3
Data Requirement 11	Resource Utilization is provided, including (but not limited to): Resource Utilization	1,2,3
Data Requirement 12	Situational Awareness information is provided, including (but not limited to): Situation, patient(s), resources	1,2,3
Data Requirement 13	Present Episode of Care – ECS and On-Site information is provided, including (but not limited to): Present Episode of Care – ECS and On-Site Complaint (current problem) Mechanism or cause of injury or illness (Chemical spill data, car crash data) Assessments and Trends - Vital signs - Pain status - Glasgow Coma Scale - Triage Category - Testing - Other Decision Support Predictive Scores - URGENCY - Other Treatment - Meds Administered - Procedures - Other Outcomes Disposition/Plan of Care	1

Data Requirement Number	Description	Scenario
Data Requirement 14	Present Episode of Care – Emergency Care information is provided, including (but not limited to): Present Episode of Care – Emergency Care Complaint (current problem) Assessments and Trends of them - Vital signs - Pain status - Glasgow Coma Scale - Triage Category - Testing - Other Decision Support Predictive Scores - URGENCY - Other Treatment - Meds Administered - Procedures - Other Outcomes Disposition/Plan of Care	2
Data Requirement 15	Present Episode of Care – Definitive Care information is provided, including (but not limited to): Present Episode of Care – Definitive Care Facility Complaint (current problem) Assessments and Trends of them - Vital signs - Pain status - Glasgow Coma Scale - Triage Category - Testing - Other Decision Support Predictive Scores - URGENCY - Other Treatment - Meds Administered - Procedures - Other Outcomes Disposition/Plan of Care	3
Data Requirement 16	Incident Information from Third Party Service is provided, including (but not limited to): Automaker Telematics Service Provider (TSP) data (e.g., General Motors' OnStar, Mercedes-Benz TeleAid) Sensors (e.g., Insulin monitor, Heart Monitor)	1

2.2.2.1 Data Issues Identified in Use Case

Inherent in the ER-EHR Use Case is the premise that some of the issues and obstacles in today's environment will be addressed through health information technology, message and taxonomy standardization and harmonization activities, policy development, establishment of interoperability policy

making bodies at all levels of government representing the full range of safety professions, and other related initiatives. This is not an all-inclusive attempt to cross reference every issue to an information flow. The goal is to point out some practical situations in which an issue or obstacle would arise.

How these issues are related to the Use Case scenario perspectives (On-Site, Emergency Care and Definitive Care) are specified in Tables 2.2.1-1, 2.2.1-2 and 2.2.1-3.

Regulatory or Policy

1. Current policies and regulations are not always considerate of emergency care. As an example, the disaster response to Hurricane Katrina showed some of the policy issues that impact accessing and sharing patient-specific health information, such as a Personal Health Record (PHR), in an emergency. Some issues include:

- The need for the timely development of business associate or other agreements by entities wishing to share patient-specific health information during an emergency can be challenging
- This should include the sharing of License, Credentials and or Privileges across geo-political boundaries and healthcare facilities. In many cases, depending on the scale of the event, these can or will be contained on or in the badge
- This should include the establishment long before a disaster event of standardized, shared core services, including registry of organizations, identity management/access control, and data rights management. Because of the impossibility of negotiating rights on a reciprocal basis between the tens of thousands of organizations that form the pool from which interoperability is required, rights should instead be based on standardized roles (e.g., hospital emergency department, 9-1-1, EOC, EMS unit responding to the incident, EMS in mutual aid area, law enforcement responding to the incident, etc)
- Variations in local policies and state security and privacy regulations impact the ease of cross-jurisdictional sharing of protected health information. The core services affecting rights therefore need to allow policy making entities to record differences based on jurisdiction as well as incident type

2. There is widespread and fundamental misunderstanding by emergency practitioners of HIPAA's treatment of medical information in general, and emergencies in particular. For example, most are not aware there is a complete exemption in HIPAA for care providers treating a patient involved in an emergency situation. HIPAA was designed to stop abuses, not to be a barrier to providing care to patients in emergencies. There is widespread misunderstanding of how data sharing systems can and should improve patient privacy over today' voice and paper-based methods.

Patients may have concerns about privacy if information about their care in an emergency situation is shared inappropriately. However, ECS and on-site care providers (EMS, Law Enforcement and Fire) and clinical care personnel involved in emergency care activities may need to have the capability to "break the glass" in order to gain access to patient-specific historical health information, such as a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR). This has immediate relevance to the clinician's decisions about the care needed or to facilitate family member reunification and expedite next-of-kin notification to reach emergency contacts who have knowledge

about certain basic aspects of the patient's health, such as pre-existing conditions, allergies, past episodes of care, current medications, primary care physician, etc. HIPAA allows this, but many practitioners are not aware, or are governed by excessively conservative institutional policies.

Data

3. Data exchanges are hampered by lack of harmonization of the data sets needed to support emergency response, the underlying data definitions, the minimum data required, and inconsistent implementation of existing data standards. This is particularly true between functions (e.g., Law Enforcement to EMS, EMS to Definitive Care; 9-1-1 to EMS to EOC). Likewise, many existing systems currently supporting emergency responses have not developed interfaces to convert their internal, proprietary coding into standard formats and terminology. This issue applies to emergency messaging in general, and to specific substantive areas such as patient information, situational awareness messages, and information describing the resources available to support an emergency response effort (e.g., clinician availability, stockpile inventory, pharmacy inventory, and hospital bed availability).

4. Methodologies for identifying and unambiguously matching patients and their information may vary from system to system, resulting in incomplete access to information at various points in the information exchange.

Authentication and Authorization

5. The lack of technologies to provide core services for inter-organizational interoperability (specifically access control/identity rights management, organizational registry, and data rights management) and the lack of standards for them impose significant costs in money and inefficiency. We lack the technical core service tools, but that is just the first part. Those software core services need to be populated with policies and rules based on the roles of organizations in emergency response. In many areas we still need to establish interoperability policy making bodies at all levels of government representing the full range of safety professions.

We then need ways to enforce those policies. Mechanisms to audit access to patient-specific historical health information, such as a PHR, ECON, and/or EHR data across multiple organizations, geographic regions or health information service provider markets are not available. While a local market health information service provider will have the audit data for their own market, mechanisms to create an integrated view of who has accessed patient-specific information across multiple markets will be challenging. Agreed upon standards for audit-related data and standards for exchanging audit information among networks are needed. This need emerges in larger scale incidents during which patients are transported across market boundaries.

Similarly, mechanisms to verify the license, credentials and privileges of a clinical care provider at the scene of an incident or medical treatment facility may not be available to incident control personnel. This becomes most relevant in larger-scale incidents during which personnel from out-of-region arrive on-scene to provide medical care and need to be quickly identified and given permission to enter the scene.

6. Even if a clinical care provider has been issued authentication credentials by a local market health information service provider to access network resources, mechanisms to disseminate those authentication and authorization credentials to all health information service providers in an emergency may not be available.

Technology

7. In general, the emergency response professions have not been focused on sharing data in their response to emergencies. At the present time, real time communications to and from 9-1-1, and to and from Law Enforcement and EMS, are primarily voice transmissions. Information technology has typically been restricted to internal use and after the fact record keeping and reporting. Therefore it is often the case that agencies do not have broadband connections; their software applications (e.g., Computer Aided Dispatch) are unlikely to be set up to exchange data with external parties, much less have interfaces to and use the new standardized message sets.

As the costs of information and communications technology are typically borne by each individual agency or profession (rather than shared networks and applications), replacement of technology is slow and relatively expensive. Perhaps more importantly, this balkanization means there is no “single place”, single agency, charged with building, owning and operating an integrated overall emergency medical system. Therefore there is no single agency or place where systemic financial and service delivery advantages of interoperability and shared systems, such as an expected lower total cost of ownership, can be envisioned, planned and deployed, much less measured.

8. There are likely to be varying levels of technical infrastructure available to those participating in an emergency response situation. This could be a consequence of the nature of the incident (e.g., electrical power failure) in which certain capabilities are degraded, or the absence of certain capabilities in the infrastructure supporting a specific response group (e.g., no wireless infrastructure capability), or a variance in the ability of agencies to acquire new technology.

Workflow and Ease of Use

9. The scale and complexity of an incident may impact the ability of a provider to effectively utilize patient-specific historical health information (i.e., PHR, ECON and/or EHR) without adversely affecting the pace of providing patient care. There could be situations in which some steps in the Use Case information flow may be difficult or even impossible to perform, resulting in the clinical care providers utilizing alternative information gathering and communication mechanisms which may not be readily integrated with these information tools.

Stand alone EMS-only, or mass casualty-only emergency patient record systems have had limited acceptance. Initial field experience with field information technology systems has shown that adoption and use will be greatest if patient information systems are used and have value in day to day emergency medical events, not just disasters. And, in addition, (a) there is a strong focus on user needs, especially ease of use; (b) information useful to the user is pre-populated from 9-1-1, PHR, ECON and/or EHR, and other sources (such as prior ambulance transports of that patient); (c) physical entry requirements for

responders who need to use their hands for patient care are minimized (maximizing use of voice to text technology and automatic integration of sensor data, such as data from blood pressure and pulse ox devices); and (d) economic and financial benefits are achieved, not just care improvements.

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
Emergency Communications System (ECS) • 9-1-1 • Dispatch • Emergency Management • Private sources of information (e.g., OnStar) • Supporting IT systems	This term is a technical and architectural convenience representing four primary functions: the 911/Public Safety Answering Points (PSAP), Dispatch, and Emergency Operations Centers within the scenarios, along with the external public and private information sources to which they have access, or which access them. In some jurisdictions the location and staff of these functions may be the same. For example, the 911 call center and dispatch are very often co-located, and in small communities often also functions as the EOC in disasters. 911 Call Center/PSAP is the location where a call is received and processed by a telecommunicator. Data about the incident, patient, and care information is collected from multiple sources, including a Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) in a Computer Aided Dispatch (CAD) system. Dispatch is the allocation and sending of the proper resources and personnel to the scene. Emergency Medical Dispatch (EMD) is a protocol for determining what care to send, generally administered through oral questions posed by the telecommunicator. With ER-EHR interoperability, the next generations of EMD can be far "smarter," taking advantage of data from multiple sources. An Emergency Operations Center (EOC) is the physical location where various organizations come together under the direction of the Emergency Management staff during a larger scale emergencies or incidents to coordinate response and recovery actions and resources. Increasingly, ECS also refers to the IT and communications systems that support the above and other actors, especially On-Site Care Providers, during emergencies.	1,2,3

Business Actor	Description	Use Case Scenario
On-Site Care Providers / Incident Commander	On-Site Care Providers: These are primarily Emergency Medical Services (EMS) staff, such as paramedics and EMTs. They may also include law enforcement, fire, and other medically trained emergency responders who provide care while at, or in transport from, the site of an emergency. Incident Commander: The officer in charge of the overall management of an incident at the incident site. He or she is responsible for building a management organization according to ICS rules. There is only one incident commander per incident.	1,2,3
Patient ID Cross-Referencing Service (PIDs)	An application that references a patient data base for the purpose of identifying a particular patient based on one of many IDs or by matching patient demographics.	1,2,3
Network Service Providers and Other Healthcare Systems	A network service provider that enables or oversees the access to and exchange of health and related information, in a secure manner, for the purpose of supporting responder, clinician, and consumer needs. Other healthcare facilities, such as record repositories, organ recovery organizations, etc.	1,2,3
Electronic Health Record (EHR)	The Electronic Health Record (EHR) is a secure, real-time, point-of-care, patient-centric information resource for clinicians and other responders.	1,2,3
Clinician	Healthcare providers located at a Medical Treatment Facility (MTF) with responsibility for treating emergency incident victims. This includes emergency physicians, emergency nurses, and all other clinical and ancillary personnel at the MTF.	2
Emergency Contact Registry (ECON)	An organized system for the registration, storage, retrieval, and dissemination of emergency contact information for individual persons. The registry contains a person's emergency contact name(s) and contact phone number(s) to assist with unidentified person identification, facilitate family member reunification and expedite next-of-kin notification. The registry responds to unique identifier (e.g., motor vehicle VIN#) queries for emergency contact information. The emergency contacts may provide additional knowledge about certain aspects of a person's health, such as pre-existing conditions, allergies, medications, last meals, primary care physician, etc. The registry may also provide an electronic 'pointer' to the availability and location of a person's Personal Health Record (PHR)	1,2
Emergency Dept. Staff	Emergency care is provided by clinical care personnel operating in a MTF. They usually work in an ED or equivalent military facility, evaluating and or treating patients before they are discharged, admitted to an inpatient facility, or deceased. They may include physicians, advanced practice nurses (e.g., nurse practitioners, nurse anesthetists), emergency nurses, physician's assistants, and military corpsmen.	1,2,3
ED Staff System	The IT system containing the ED encounter record and supporting the ED staff.	2

Business Actor	Description	Use Case Scenario
ECS/On-Site Systems (e.g., 911, EOC, Dispatchers, EMS, Police, Fire)	The IT systems containing the encounter records and supporting the ECS and first responders. Generally, the ECS and on-site systems are separate; but, have similar ER-EHR interoperability requirements.	
Public Health Agencies	Those agencies of local, state and federal government charged with the health of their populations.	1,2,3
Appropriate Shared (HIS) repositories	Repositories from "Other Health Information Providers", which may include medical device manufacturers, medical registries, emergency contact registry etc.	2,3
Another Facility	"Other" medical facilities	2,3
Medical Examiner/ Fatality Manager	Medical Examiner/ Fatality Manager: Those charged with investigation of the cause of death where the death is under suspicious circumstances. Medical Examiner: A physician officially authorized by a governmental unit to ascertain the cause of death. Unlike a coroner, the medical examiner is always a physician. Medical Examiners/Fatality Managers investigate by inquest any deaths thought to be of other than natural cause. They may perform autopsies or inquests, usually in morgues. They may include Medical Examiners, Coroners, and Disaster Mortuary Operational Response Teams (DMORTs).	2
Personal Health Record (PHR):	A health record that can be created, reviewed, annotated, and maintained by the patient or the care giver for a patient. The health record may include any aspect(s) of their health condition, medications, medical problems, allergies, vaccination history, visit history, or communications with their healthcare providers.	1,2,3
Core Services	A collection of standardized, shared services that help ensure security during the sharing of patient information and accurate data routing. These include but are not limited to: access control/identity management, data rights management, and location and other information about emergency agencies.	1,2,3

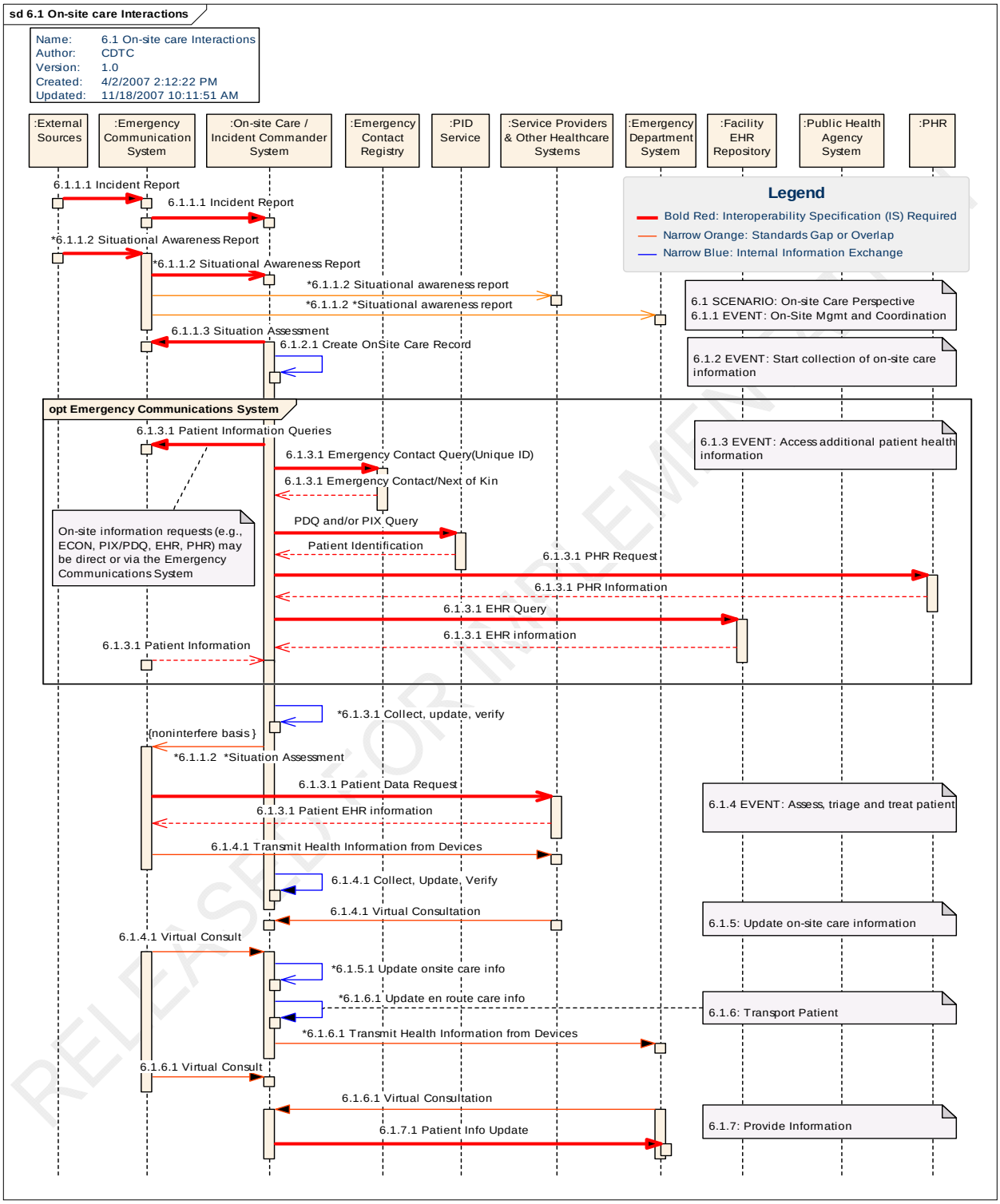
2.2.4 HIGH-LEVEL UML BUSINESS SEQUENCE DIAGRAMS

This section contains an explanation of the relationship between the business actors and data interactions between the primary actors and alternative actors for each Use Case scenario. The diagrams that follow illustrate each scenario with a representation of a normal sequence of exchange between the primary actors. Note that all ER-EHR Clinical Summary exchanges use the HITSP/C32 -Summary Documents Using HL7 Continuity of Care Document (CCD) Component.

2.2.4.1 On-Site Care Scenario Perspective Business Sequence Diagram

Figure 2.2.4.1-1 illustrates the UML interaction diagram from the scenario perspective of On-Site Care.

Figure 2.2.4.1-1 On-Site Care Scenario Perspective Business Sequence Diagram



This following narrative provides a high level walk though of the flow depicted in the UML diagram in Figure 2.2.4.1-1 On-Site Care Scenario Business Sequence Diagram. A response to a motor vehicle

crash involving a single vehicle is utilized as the incident example. It is fictitious and only one simple example of the scenario. The goal is to provide a better understanding of the actions involved regarding 1) ECS access and exchange of patient-specific and incident information with on-site care providers (EMS, Law Enforcement, Fire), and; 2) on-site care provider (EMS, Law Enforcement, Fire) access and exchange of patient-specific health information, such as a Personal Health Record, Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR), with or independent of the ECS.

An Emergency Communications System (ECS) is notified of a motor vehicle crash. The 9-1-1 telecommunicator attempts to collect data such as victim's name, location, gender, and chief complaint. Vehicular incident data from automaker Telematics Service Providers (e.g., General Motors' OnStar, Mercedes-Benz TeleAid) may also be available. Other external incident data may be transmitted to, or accessed by the ECS (and other actors depending on specific agency desires and local business rules entered into the core services.). The ECS begins an emergency care record on the victim and supplements it with information derived from questioning the caller that may be relevant (age, gender, partial Glasgow coma scale measurements). Victim-specific historical health information, such as PHR, ECON and/or EHR may be available. From the ECS, the 9-1-1 Telecommunicator/Dispatcher provides the initial patient assessment in deciding what care to dispatch to the scene. These decisions are usually made according to Emergency Medical Dispatch (EMD) protocols. In the future, we expect these to be enhanced by the application of new predictive decision support tools which take advantage of the data sources discussed herein. The same data may indicate the need for additional resources from a different profession (e.g., an extrication team from fire services). In some cases, trained telecommunicators may provide telephone pre-arrival treatment instructions of the patient(s) prior to arrival of the first on-site care providers on the scene. All patient, incident, and care information collected by the ECS is entered into an Episode of Care Record in a Computer Aided Dispatch (CAD) system prior to dispatch of personnel to the scene.

On-Site care providers, such as Fire, Police, EMS, or Air Transport are dispatched based upon the above information. [6.1.1.1 – HITSP Gap]. All gathered information is sent from the ECS to the responding on-site care team answering the dispatch call (or available to them), and other involved organizations as appropriate (with data access rights governed by the core services). The fire services extrication team accesses automotive design data on the way to the incident to learn where to cut into this particular vehicle without triggering a side airbag or hitting an electrical cable.

The Emergency Communications System [Emergency Operations Center in a large scale emergency] provides continuous updates about the incident (such as location, situation, patients, etc) by sharing a flow of incident messages and creating Situational Awareness Reports from time to time. These messages and reports are sent to incident stakeholder locations such as EMS, Emergency Department, Incident command, state health department, state EOC, HHS, depending on the incident. etc. [6.1.1.2 - HITSP Gap]. If the Incident Command System (ICS) is invoked, there are a large number of standard ICS forms, but there has not been an electronic standardization of the forms or all of their taxonomy.

On-Site care providers (EMS, Law Enforcement, and Fire) arrive at the scene. Police or transportation officials begin traffic diversion. Fire Services staff successfully extricate the victim. The Emergency Medical Technician (EMT) begins treatment of the patient and begins contributing to the pre-hospital Patient Care Report (PCR) [6.1.2.1], adding to the data already transmitted from the ECS.

The crash victim is unconscious and not identifiable. In order to keep the focus of the EMT on delivery of emergency medical services, law enforcement is typically responsible for the identification of unidentified crash victims and/or obtaining the vehicle owner emergency contact information to assist in the identification of unidentified crash victims, facilitate family member reunification and expedite next-of-kin notification. Law Enforcement may accomplish these tasks on a treatment non-interference basis by utilizing the Vehicle Identification Number (VIN) as a unique identifier to query an Emergency Contact Registry (ECON) [6.1.3.1 – HITSP Gap] to obtain the vehicle owner emergency contact name(s) and phone number(s). The vehicle owner emergency contacts may provide assistance in identifying unidentified crash victims, as well as, providing additional knowledge about certain aspects of victim-specific health information, such as pre-existing conditions, allergies, medications, primary care physician, etc.

Law Enforcement electronically passes the gathered patient-specific historical health information to EMS and other authorized parties, specifically positive victim identification and emergency contact information. This information may include an electronic ‘pointer’ to the availability and location of a PHR. EMS electronically records the Patient ID (demographics) and PHR ‘pointer’ information in the pre-hospital PCR system, enabling authorized EMS personnel to send a query (or automatically querying a Patient Identification Service) to determine the location of the PHR and/or EHR data. [HITSP/TP22 - Patient ID Cross-Referencing (IHE PIX Query)] (see note). This allows a query or retrieval of the needed documents [6.1.3.1 – HITSP/TP13 - Manage Sharing of Documents (IHE XDS), with the document defined by HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)]. On-site care providers at times will need access to parts of the patient–specific historical health data in a PHR, ECON and/or EHR, as opposed to the documents or parts of the documents themselves.

On-site EMS gathered patient specific historical health information gathered by EMS, including PHR, ECON and/or EHR data are electronically downloaded and entered automatically merged into the pre-hospital PCR. This supports real-time messaging of patient-specific historical health information (i.e., Patient ID, ECON, PHR and/or EHR data) to Emergency Department Clinicians and other authorized parties.

This information enhances the Dispatch, Virtual and/or on-site care of the patient [6.1.4.1, 6.1.5.1, 6.1.6.1]. EMS personnel perform tests on the patient requiring medical devices, such as EKG, blood pressure monitors, etc. This device information is automatically added to the pre-hospital Episode of Care Record (including Patient Care Report), which is now available through the ECS to the ED where the patient is being sent based on a matching of hospital resource availability and the needs of the patient. A decision support software application meshes relevant parts of the Episode of Care Record with on-going reports from hospitals on ED, specialty care, operating room and bed availability [6.1.4.1 – HITSP Gap].

The simultaneous receipt of this data, and of trend lines in patient vitals, allows virtual consultation by more expert practitioners at the ED or trauma center. In some cases, the ED may be skipped altogether as the victim is delivered directly to the cardiac unit, operating room, etc.

Before the patient arrives at the ED, the hospital's ED information system has been pre-populated with information about the victim. This includes all the identity, emergency contact information, incident and care information discussed above, and also organ donor and insurance billing information.

The traditional task of creating an EMS ambulance "run report" or PCR is made simpler as most of the information is already in the ECS or EMS system and can be directly printed and/or electronically reported. While the run report may need further editing, EMS should find that this new approach saves report writing time. Some portions of the Encounter Record need to be extracted to update the patient's PHR and/or EHR [6.1.7.1 HITSP/TP13 - Manage Sharing of Documents (IHE XDS), with the document yet to be defined – HITSP Gap].

Note: Another example is where law enforcement was not able to ascertain the victim's identity from the emergency contacts in ECON, but was able to obtain patient demographics and locations of PHR and/or EHR data. For this example, the PIX query would not work because a Patient ID is not known. Therefore, a patient demographics query to obtain the Patient's ID from the known PHR/EHR would be required [HITSP/T23 - Patient Demographics Query].

Note: "HITSP Gap" means that there is no existing HITSP construct with transport data and vocabulary standards. The HITSP Gap road map, in Section 3.0, addresses candidate standards and/or duplicate or overlapping standards which are being suggested or matured to satisfy this need.

2.2.4.2 Emergency Care Scenario Perspective Business Sequence Diagram

Figure 2.2.4.2-1 illustrates the UML interaction diagram from the scenario perspective of Emergency Care.

Figure 2.2.4.2-1 Emergency Care Scenario Perspective Business Sequence Diagram

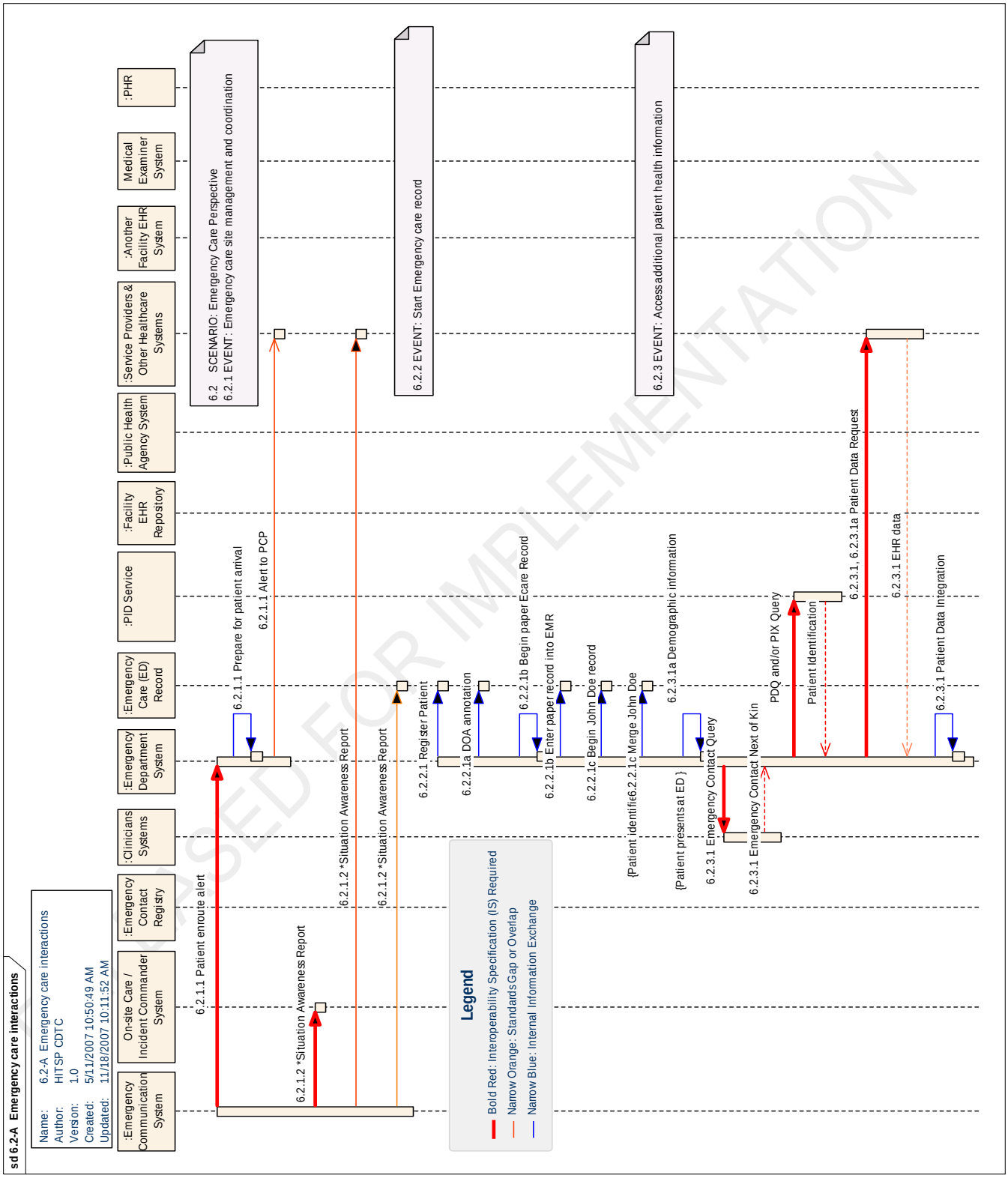
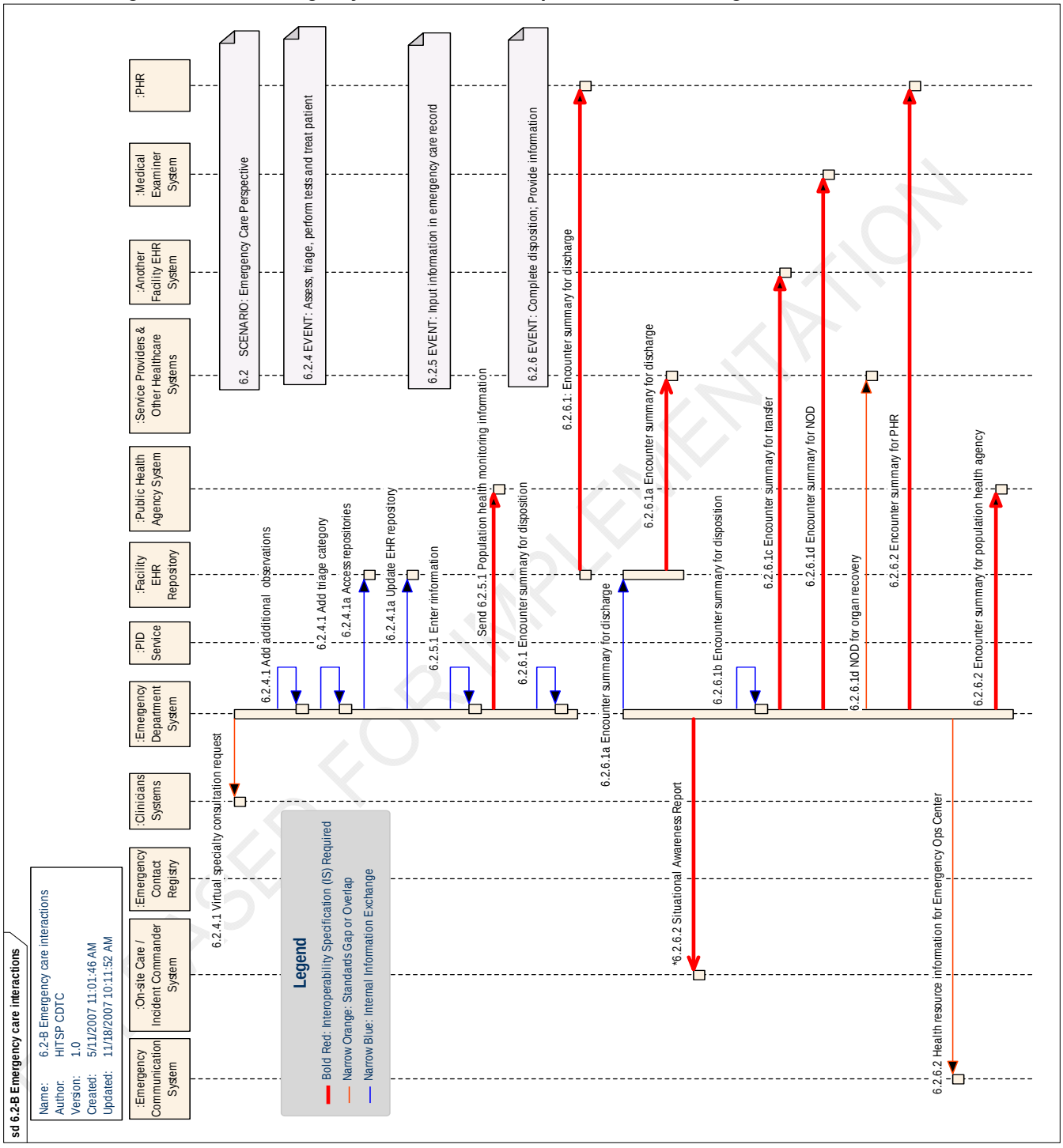


Figure 2.2.4.2-1 Emergency Care Scenario Perspective Business Diagram Continued



This following narrative provides a high level walk through of the flow depicted in the UML diagram in Figure 2.2.4.2-1 Emergency Care Scenario Perspective Business Diagram. It is fictitious and only one

simple example of the scenario. The goal is to provide a better understanding of the scenario and to map standard electronic communications to HITSP Transactions.

Initially, all facilities in the immediate area are alerted about an incident and updates are made regarding current resource availability. An Emergency Department receives a notification from the Emergency Communications System [On-Site responders and/or Medical Control functions] about a patient being transported to their facility [6.2.1.1 – HITSP Gap]. The Emergency Communications System [often the Emergency Operations Center in a large scale emergency] provides continuous updates about the incident (such as location, situation, patients, etc.) which from time to time are collected in Situational Awareness Reports. These are formalized as ICS reports if ICS has been activated. These messages and reports are sent to incident stakeholder locations that have registered to receive it such as EMS, Emergency Department, higher level EOCs, etc. [6.1.1.2 - HITSP Gap].

If there is no power or communications, the Emergency Department begins a paper record for the patient [6.2.2.1 – no electronic communications]. Patient arrives at ED and the department attempts to obtain patient-specific historical health information via many possibilities, ECON, EHR, PHR, other facilities – If that data has not already been accessed and, where relevant, added to the Emergency Care Record by either the ECS or On-Site care earlier in the response process, the ED queries the various ECONs to determine the patient's contact information [6.1.3.1 – HITSP Gap].

A query to a Patient Identification Service (PID Service) is required to determine the Patient's ID for the PHR and/or EHR [HITSP/T22 - Patient ID Cross-Referencing (IHE PIX Query)] (see note in Section 2.2.4.1). After obtaining the proper ID for the PHR/EHR, the ED query/retrieve the needed data [6.2.3.1 – HITSP/TP13 - Manage Sharing of Documents (IHE XDS), HITSP/C32 – Summary Documents Using HL7 Continuity of Care].

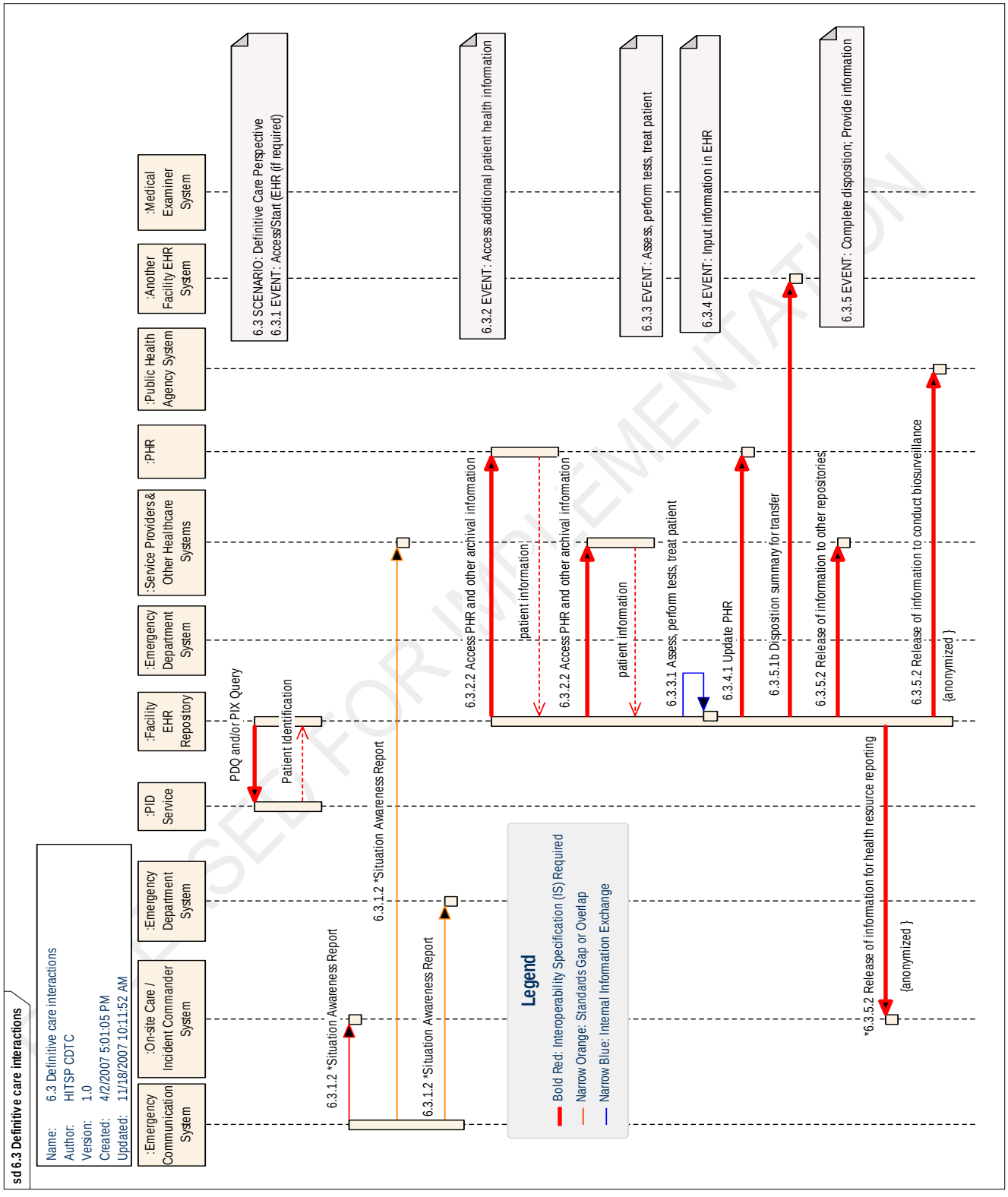
The ED personnel (i.e. nurses, doctors, etc.) perform various tests, collect data and build a report [6.2.4.1, 6.2.5.1, - internal ED events]. The output of this effort is an ED summary document that can be transmitted to many different authorized entities [6.2.6.1 HITSP/TP13 - Manage Sharing of Documents (IHE XDS), with the document defined in HITSP/C28].

The Situational Awareness messages and/or report are updated by the ED and sent to the Incident Commander and the Emergency Communications System [often the Emergency Operations Center in a large scale emergency] is updated with ED and hospital resource information [6.2.6.2 – HITSP Gap].

2.2.4.3 Definitive Care Scenario Diagram

Figure 2.2.4.3-1 illustrates the UML interaction diagram from the scenario perspective of Definitive Care.

Figure 2.2.4.3-1 Definitive Care Scenario Perspective



This following narrative provides a high level walk though of the flow depicted in the UML diagram in Figure 2.2.4.3-1 Definitive Care Scenario Perspective. It is fictitious and only one simple example of the scenario. The goal is to provide a better understanding of the scenario and to map standard electronic communications to HITSP Transactions.

The Emergency Communications System [Emergency Operations Center in a large scale emergency] provides continuous updates about the incident (such as location, situation, patients, etc) by sending messages about the incident and from time to time creating a Situational Awareness or ICS Report. These messages and reports are sent to incident stakeholder locations such as EMS, Emergency Department, etc. [6.3.1.2 - HITSP Gap].

Where feasible and appropriate the emergency care record, or parts of it (including information from ECON) are transferred to others (Virtual consultations, EHR, PHR, etc). A query to a Patient Identification Service (PID Service) is required to determine the Patient's ID for the PHR and/or EHR [HITSP/T22 - Patient ID Cross-Referencing (IHE PIX Query)] (see note). After obtaining the proper ID for the PHR/EHR, the EMS query/retrieve the needed documents [6.3.2.3, 6.2.4.1 – HITSP/TP13 - Manage Sharing of Documents (IHE XDS), with the document defined by HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)] (see note).

The ED discharges the patient with a medical summary document and transfers to other facilities [6.3.5.1 – HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) and HITSP/C39 - Encounter Message. If appropriate, The Red Cross is notified of the name and location of the patient. It may also be that a Red Cross facility is the recipient of the patient.

Note: Event 6.3.2.2 is identified as "Access PHR other Archival Information." This specification only defines the PHR summary document to retrieve (HITSP/C32). Other archival information may be accessible to the EHR but that is an internal function outside the scope of this Interoperability Specification.

3.0 DESIGN

The design for the ER-EHR 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.

Sharing of data across medical and non-medical professions requires agreement and use of a set of messaging standards, common terminology, messaging protocols and core services between medical, EMS, public health, 9-1-1, emergency management, fire services, law enforcement and other actors at local, state and federal levels. Some of these messaging standards and common terminology exist today, but have not been widely adopted. The rest need to be developed and/or deployed outside as well as inside the healthcare domain. This may require cross domain translation services among standardized healthcare transport and vocabulary and other domains' standardized transport and vocabulary. This IS does not address the standardization of non-healthcare domains.

All ER-EHR exchanges of clinical summary information use the HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD). HITSP has identified the key capabilities (new or modified HITSP constructs) that are necessary to support this version of ER-EHR requirements of the Use Case. These capabilities have been identified out of the pool of considerations as the minimum necessary to effectively support the listed perspectives and events of the Use Case.

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
HIPAA policy compliance is maintained by all organizations handling patient data	1, 2, 3

Assumption	Use Case Scenario
Situation reports and patient information are periodically sent to public health agencies, ECSs and appropriate other actors and locations, whenever that information is available and/or needed.	1, 2, 3
Event 6.3.2.2 is identified as "Access PHR other Archival Information." This specification only defines the PHR document to retrieve (HITSP/C32). Other archival information may be accessible to the EHR but that is an internal function outside the scope of this Interoperability Specification.	3
As appropriate, education may be part of Treatment for Data requirement 13, 14, and 15	1, 2, 3
Systems store patient data as an encounter. A patient has 1 to many encounters linked into episodes of care. Each encounter holds documents. Each document holds data. This is analogous to each encounter being a report holding many paper document sections and each document section containing many data pieces. An episode of care contains many reports on the same incident. The file folder also contains incident information on the same topic (e.g., patient). We assume data are communicated in both document and message forms.	1, 2, 3
Individual and organizational communications modalities other than telephone and public safety radio exist. These include personal devices such as PDA, IM, P25 and/or, 2G, 3G and 4G wireless data devices, as computers linked by broadband between organizations These devices can be used to exchange information when implementing the Use Case. The various headquarters and offices of the emergency response professions (e.g., ECS, EMS, hospitals, public health) will need to be linked to broadband backbones – as most are not today. The key to success rests on making the systems and software of various professions interoperable with each other and the private sector at the TCP/IP transport level, at the transaction level, at the data level and at the vocabulary level. Communications modalities are out of scope of the ER-EHR. We assume the TCP/IP transport level is universally provided.	1, 2, 3
A wide variety of actors need access to some or all of the data generated by an incident. First, organizational actors need to be able to register their desire to receive/have access to certain kinds of incidents and portions of the total data (patient, situational awareness, etc). Then there need to be role-based access control and data rights management core service applications to govern that access. These core services need to be standardized, and separated from proprietary systems, so they can be shared: i.e. a common rights management system for each community.	

3.1.2 CONSTRAINTS

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

Table 3.1.2-1 Constraints

Constraint	Use Case Scenario
Discharge messages and documents are not anonymized for transfer of patients (unless to Public Health facilities or the ECS).	1,2,3

3.1.3 PRE-CONDITIONS

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

1. The transport network infrastructure is TCP/IP: The actors' systems are all connected to Internet protocol broadband networks. Organizations have network gateways; individuals may have appropriate networked mobile devices. All non-IP devices or communications systems have gateways to convert those communications into IP

2. Those networks are governed by industry standards-based, open, service-oriented architectures that are network-centric

3. Within the networks there are standardized and shared services that enable secure, appropriate, and accurate information exchange across data sources and systems to view and use the data. These are functionally external to proprietary messaging or customer premises applications. They include, but are not limited to a variety of enterprise services, including core services:

a. to identify and authenticate users
b. to identify and determine providers of care
c. to record and enforce access control and data access policies
d. to ensure that the data are true copies of the data as attested by the source
e. to correctly match patients with data about them across systems
f. to log transactions and provide an audit trail
g. to identify data sources, including but not limited to patient-specific historical health information provider (i.e., Personal Health Record (PHR), Emergency Contact Registry (ECON) and Electronic Health Record (EHR) systems
h. for organizations to register their interest in receiving various kinds of incident data, including patient information

4. Appropriate standards are developed, approved, and widely adopted supporting data content and structure, allowing universal access by compliant systems to:

a. Situational awareness messaging and taxonomy (all emergency response professions)
b. Patient messaging and taxonomy (primarily medical and 9-1-1 communities)
c. Conversion interface between NEMSIS and hospital data standards if these remain distinct

5. Core pre-hospital datasets are standardized and adhered to

6. Other organizations may be queried for data and matching to the patient

a. Emergency response organizations
b. Individual medical sources

c. Private sector sources

7. System transactions will be logged

8. Security and privacy policies, procedures and practices are commonly implemented through core services to support acceptable levels of patient security and privacy

9. Appropriate standards protocols, patient identification methodology, consent, security and privacy procedures, will be agreed to by all relevant participants

10. Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect

11. Business, billing, insurance, and related economic issues are resolved in ways that support the sharing of information as described herein

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

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/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 Directives – Capture/Request consent directive HITSP/TP20 - Access Control – Access control request	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
The ECS system and On-Site care team (EMT, Law Enforcement, Fire) receive incident and patient-specific historical health information that allows them to provide more informed and rapid response; the Emergency Department receives incident and patient data before arrival (i.e. traditional ambulance Patient Care Report (PCR) enhanced as described herein) that allows ED to provide more informed and rapid response. All actors save money by avoiding duplicative entry of the same data, and errors that result from that.	1, 2, 3
On-Site care team (EMT, Law Enforcement, Fire) directly access and exchange patient-specific historical health information (i.e., Personal Health Record (PHR), Emergency Contact Registry (ECON), and/or Electronic Health Record (EHR) data) relating to the assessment, stabilization and treatment of the victims of emergency incidents, as well as, on a treatment non-interference basis, facilitate family member reunification and expedite next-of-kin notification following such incidents.	1,2,
The Emergency Department and definitive care facility creates timely care and outcome summaries for the patient (e.g., clinical disposition reports).	2, 3
The patient is discharged from the ED or definitive care facility and the summary records are transferred to appropriate locations, including anonymized end-to-end data for overall research purposes,	2, 3

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
An emergency incident occurs	1, 2, 3
A private sector sensor or source of information alerts ECS of an emergency and provides data about it.	1, 2, 3

3.2 DETAILED DESIGN

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

3.2.1 TECHNICAL ACTOR ROLE DESCRIPTIONS

This section contains technical actor role descriptions for all scenarios. Note that a business actor is a representation of a person, IT system, organization or any combination that is engaged, and benefits from the real world information interchange defined by a business Use Case, while a technical actor represents an entity internal to a software application, which is engaged in one or more specific Transactions to support a specific aspect of a real world information interchange (e.g., set of message exchanges). The table below describes the technical actor roles involved and the correlation between active actors.

Table 3.2.1-1 Technical Actor Role Descriptions

Technical Actor(s)	Actor Role
Access Control Service Consumer	The Access Control Service User accesses the Access Control Registry to determine if it may send, receive or review messages and/or data.
Access Control/Authorization Registry (core service)	This registry maintains data about the rights of each Actor to send, receive and access data. It is paired with an identity management/authentication service.
Agency Registry (core service)	This registry maintains metadata about each organization, and the alerts and messages it wishes to receive.
Audit Record Repository	This actor provides a repository for audit events. IHE does not specify what analysis and reporting features should be implemented for an audit repository
Audit Record Source	The actor that, on behalf of another actor that performs an action requiring logging, creates and communicates an Audit Record to the Audit Record Repository
Consent Directive Requester	The Consent Directive Requester access consent directive located through a Consent Registry from Consent Repositories.
Consent Originator	The Consent Originator captures consent directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry.
Consent Repository	The Consent Repository is responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns a Uniform Resource Identifier (URI) and Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point.
Content Consumer	A Content Consumer Actor is responsible for viewing, import, or other processing of content created by a Content Creator Actor.
Content Creator	The Content Creator Actor is responsible for the creation of content and transmission to a Content Consumer.
Document Consumer	The Document Consumer queries a Document Registry for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors.
Document Registry	The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration.
Document Repository	The Document Repository is responsible for both the persistent storage of documents as well as for their registration with the appropriate Document Registry. It assigns a URI to documents for subsequent retrieval by a Document Consumer. The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration.

Technical Actor(s)	Actor Role
Document Source	The Document Source is the producer and publisher of documents and information. It is responsible for sending documents to a Document Repository. It also supplies metadata to the Document Repository for subsequent registration of the documents with the Document Registry Actor.
Identity Provider	The Identity Provider receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider).
Message/Alert Consumer	The Message/Alert Consumer queries a Message/Alert Registry for Messages or alerts meeting certain criteria, and retrieves selected Messages or alerts from one or more Message Repository actors.
Message/Alert Registry	The Message and Alert Registry maintains metadata about each registered Message and alert in a Message or alert entry. This includes a link to the Message or alert in the Repository where it is stored. The Message Registry responds to queries from Message Consumer actors about Messages or alerts meeting specific criteria. It also enforces some healthcare specific technical policies at the time of Message/alert registration. Some call this an intelligent message broker, or messaging service.
Message/Alert Source	The Message Source is the producer and publisher of messages/alerts and information. It is responsible for sending messages to a Message/Alert Queue. It also supplies metadata to the Message Queue for subsequent registration of the messages and alerts with the Message Registry Actor.
Node	The originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the *Secure Node* in the IHE ATNA Transaction.
Patient Demographics Consumer	The Patient Demographics Consumer 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 Supplier	The Patient Demographics Supplier receives patient registration and update messages from other systems in the enterprise (e.g., ADT Patient Registration or Health Plan Membership Management systems), which may or may not represent different Patient ID Domains. It responds to queries for information.
Patient Identity Source	Sends patient demographic information to the Patient Identifier Cross-Reference Manager
PIX Consumer	The Patient Identifier Cross-Reference Consumer either queries for sets of cross-reference patient identifiers. It may also receive notifications about cross-reference changes.
PIX Manager	The Patient Identifier Cross-Reference Manager Actor is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains.
Service Provider	The Service Provider represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion.
Service User	The entity represents any individual entity (such as a clinician or an EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transaction.
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).

Note: The Document Registry and Document Repository technical actors may reside in many different real world business actors. For this table they are shown in the Personal Health Record (PHR) but could reside in other business actors also (such as, ECS, ECON, EHR, RHIO/HIE, Other Facilities, etc). Similarly, the standardized core services can exist independently or as part of a messaging or document provider or message broker service. It is not the intent of this document to illustrate the possible architecture variants, see the HITSP/IS 03 - Consumer Empowerment and Access to Clinical Information

via Networks for real world examples.

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 interactions (encapsulated in HITSP constructs). The detailed actor interactions 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.

Each Use Case scenario is shown in the Use Case sequence diagrams in Figures 2.2.4.1-1, 2.2.4.2-1 and 2.2.4.3-1. The detailed actor interactions are described in the HITSP constructs or referenced IHE Technical Framework specifications which show how the HITSP constructs are used to support the Interoperability Specification. These technical actor interactions are also shown in Figure 3.2.2. The level of detail of data exchanged between two PHRs, EHRs or between PHR and EHR systems depends upon information contained in these systems. The specification of the format and the content of the information to be exchanged are as specified in HITSP constructs for content summarized below. Despite this detailed specification of data elements, some information exchanged may still require the personal assessment of the individuals conducting this information exchange which is pertinent to achieve semantic interoperability but is out of scope of this IS, e.g., the definition of problems as major medical conditions depends upon the clinical judgment of the consumer's trusted healthcare providers.

In order to initially populate the encounter record, we can either begin the entry of personal demographics and share that with the healthcare providers, or request information, which can then be imported into the encounter record from a portable PHR or from one or more EHRs/ECONs/PHRs service providers. The exchange between any PHRs would be accomplished via the same process as that accomplished with EHRs.

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

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

NOTE: We are not describing the content of the EHRs/ECONs/PHRs, but the exchange of information among EHR/ECON/PHR systems.

The HITSP/C32 document consists of Content Modules that contain multiple data elements. The list of content modules is:

- Personal Information

- Languages Spoken
- Support
- Healthcare Provider
- Insurance Provider
- Allergies and Drug Sensitivity
- Condition
- Medications – Prescription and Non-Prescription
- Results – Laboratory
- Immunizations
- Encounters
- Vital
- Pregnancy
- Information Source
- Comments
- Advance Directives

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

Laboratory Report Document

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

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

Figure 2.2.4.1-1 gives the On-Site Care Scenario Perspective Business Sequence Diagram. Figure 2.2.4.2-1 gives the Emergency Care Scenario Perspective Business Sequence Diagram and Figure 2.2.4.3-1 gives the Definitive Care Scenario Perspective Business Sequence Diagram. The supporting technical actor interactions are shown in Figures 3.2.2-1, 3.2.2-2, 3.2.2-3, and 3.2.2-4.

Figure 3.2.2-1 On-Site Care Detailed Design Diagram

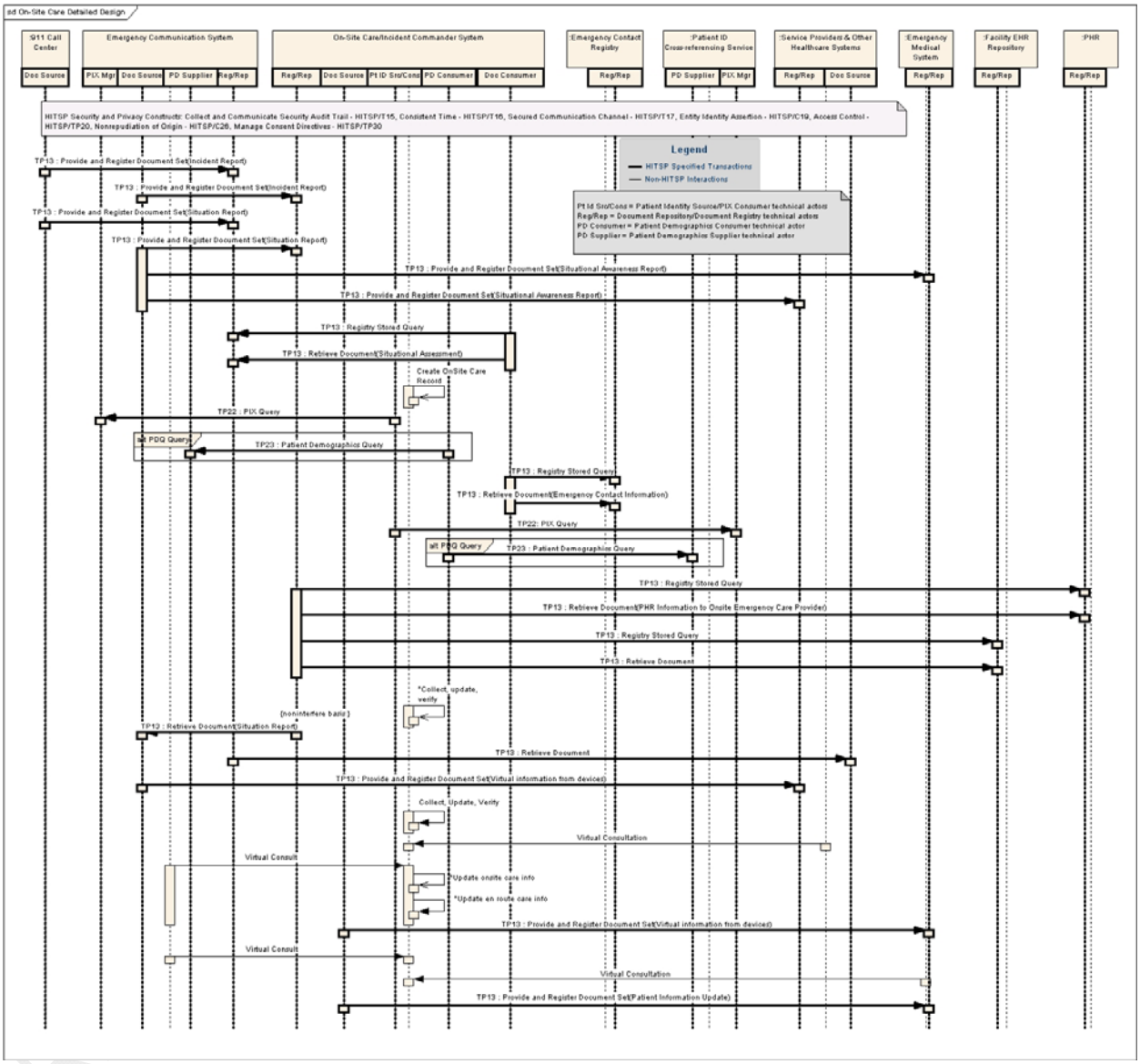


Figure 3.2.2-2 Emergency Care Detailed Design Diagram – Part A

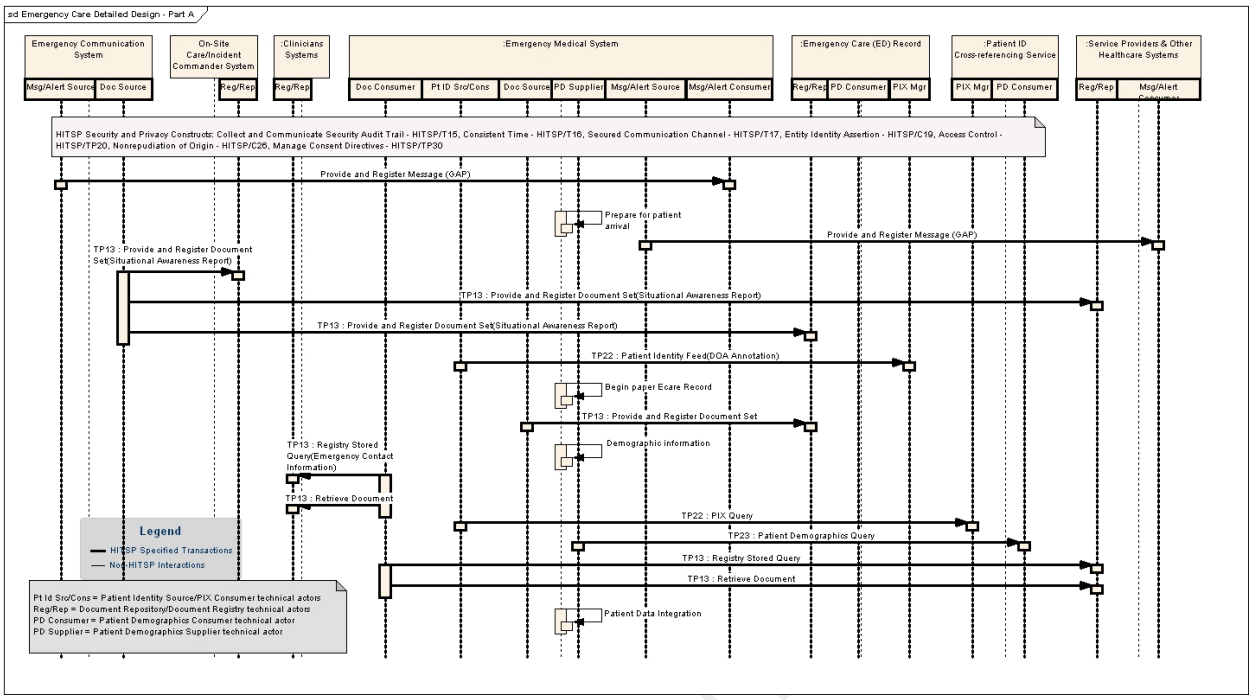


Figure 3.2.2-3 Emergency Care Detailed Design Diagram – Part B

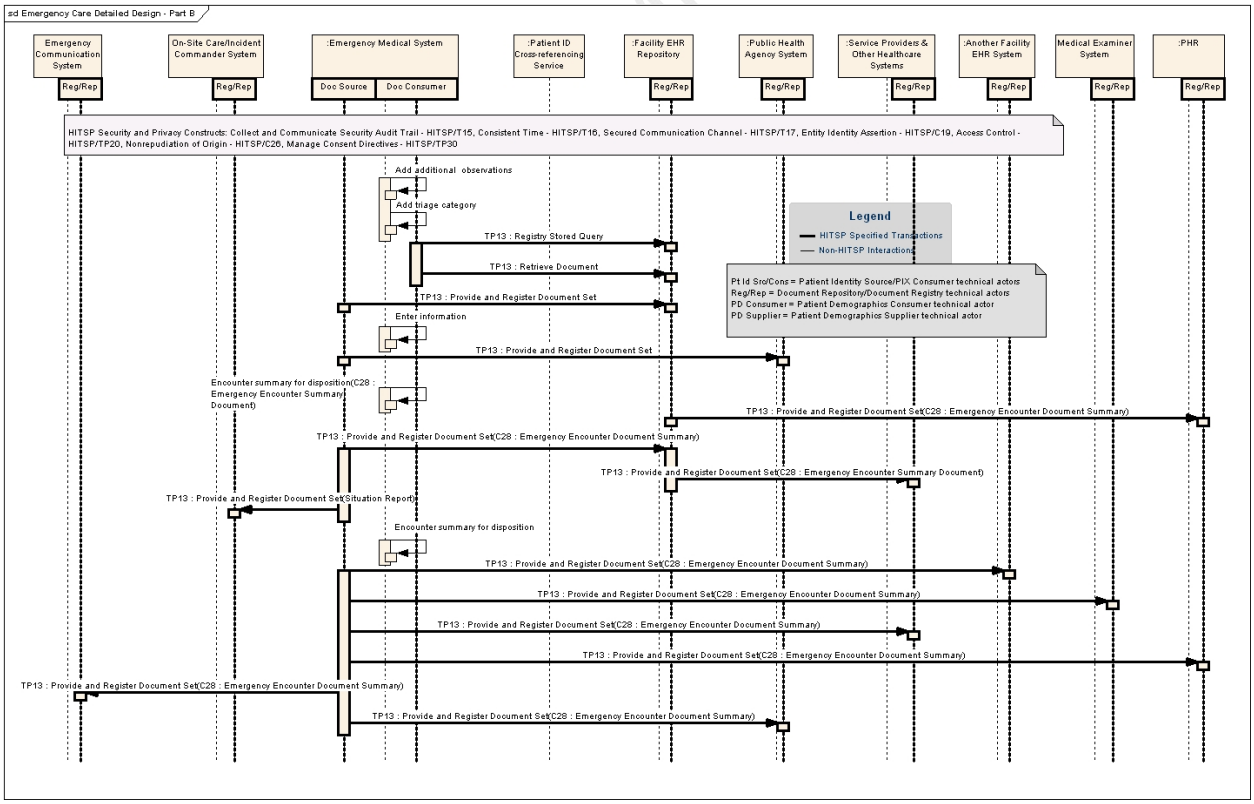
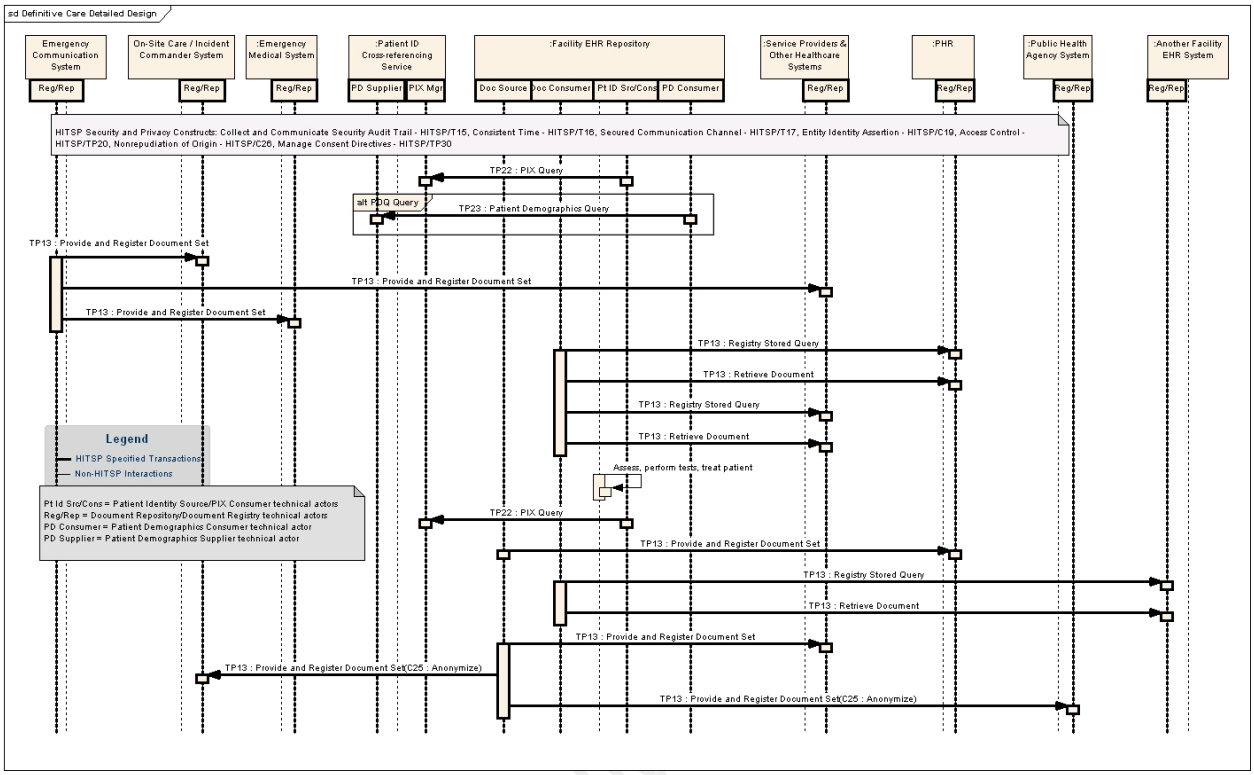


Figure 3.2.2-4 Definitive Care Detailed Design Diagram



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

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

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

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

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

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
Another Facility	Same as Facility EHR Repository				
Appropriate shared (HIS) repositories	Same as Facility EHR Repository				
Automated Medical Device	GAP, covered in separate '2008 Use Case.				
Clinical Staff	No technical actors				
Clinical Staff System	Same as Facility EHR Repository				
Clinician	No technical actors				
Core Services	Security & Privacy constructs are specified under business actors, which use them.				
Emergency Communications System • 9-1-1 • Dispatch • Emergency Operations Management • EMS • Police, Fire • Private sources of information (e.g., telematics service provider)	Patient Identity Source	C [101]	HITSP/T23	Patient Demographics Query	R
	PIX Consumer	C [101]	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/TP23	Patient Demographics Query	R
	Document Consumer	R	HITSP/TP13	Query Registry	R
				Retrieve Documents	R
	Message/Alert Consumer	R	GAP	Retrieve Message	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Documents Set	R
				Provide & Register Document Set	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set	R
	Message/Alert Source	R	GAP	Provide & Register message	R
	Content Creator	R	HITSP/C32	Creator-Registration Subset (See Section 3.2.3.1)	C[201]
				Creator-Registration-Coded Subset (see Section 3.2.3.2)	C[201]
				Creator-Medication and Immunization History Subset (See Section 3.2.3.3)	C[201]
				Creator-Medication and Immunization History - Coded Subset (See Section 3.2.3.4)	C[201]
				Creator-Conditions and Allergy Subset (See Section 3.2.3.5)	C[201]
				Creator-Conditions and Allergy -Coded Subset (See Section 3.2.3.6)	C[201]

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

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Consent Originator	R	HITSP/TP30	Provide Document Set	R
				Register Document Set	R
	Consent Repository			Register Document Set	R
				Stored Query	R
	Consent Registry			Provide Document Set	R
				Register Document Set	R
	Consent Directive Requester			Stored Query	R
				Retrieve Document Set	R
Emergency Contact Registry (ECON)	Document Source	R	GAP	Provide & Register Document Set	R
	Content Creator	R	GAP	Emergency Contact data set Content Component	R
Emergency Dept. Staff	No technical actors				
Emergency Dept. Staff System	Same as Facility EHR Repository				
Facility EHR Repository (EHR)	Patient Identity Source	C [101]	HITSP/T23	Patient Demographics Query	R
	PIX Consumer	C [101]	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/TP23	Patient Demographics Query	R
	Document Consumer	R	HITSP/TP13	Query Registry	R
				Retrieve Documents	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Documents Set	R
				Provide & Register Document Set	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set	R
	Content Creator	R	HITSP/C32	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
				Consumer-Document Display Subset (See Section 3.2.3.9)	R

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

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Consent Originator	R	HITSP/TP30	Provide Document Set	R
				Register Document Set	R
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Stored Query	R
	Consent Registry	O	HITSP/TP30	Provide Document Set	R
				Register Document Set	R
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
Medical Examiner / fatality manager	Same as Facility EHR Repository				
Network Service Providers and Other Healthcare Systems	Same as Facility EHR Repository				
On-Site Care Providers / Incident Commander	Patient Identity Source	C [101]	HITSP/T23	Patient Demographics Query	R
	PIX Consumer	C [101]	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/TP23	Patient Demographics Query	R
	Document Consumer	R	HITSP/TP13	Query Registry	R
				Retrieve Documents	R
	Alert Consumer	R	GAP	Retrieve Alert	R
	Message Consumer	R	GAP	Retrieve Message	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Documents Set	R
				Provide & Register Document Set	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set	R
	Alert Source	R	GAP	Provide & Register Alert	R
	Message Source	R	GAP	Provide & Register Message	R
	Content Creator	R	HITSP/C32	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
				Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
		R	HITSP/C37	Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
				Consent Document Component	R
				Consumer-Document Display Subset (See Section 3.2.3.9)	R
		R	HITSP/TP30	Consumer-Document Import Subset (see Section 3.2.3.10)	O
		R	GAP	Situation Report/Message Component	R
		R	GAP	Incident Report/Message Component	R
	Content Consumer	R	HITSP/C32	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
		R	HITSP/C37	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
		R	HITSP/TP30	Consent Document Component	R
		R	GAP	Situation Report/Message Component	R
		R	GAP	Incident Report/Message Component	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
	Service User	R	HITSP/C19	Convey Assertion	R
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Consent Originator	R	HITSP/TP30	Provide Document Set	R
				Register Document Set	R
	Consent Repository	O	HITSP/TP30	Register Document Set	R
				Stored Query	R
	Consent Registry	O	HITSP/TP30	Provide Document Set	R
				Register Document Set	R
	Consent Directive Requester	O	HITSP/TP30	Stored Query	R
				Retrieve Document Set	R
Other Third Party Data	Same as Facility EHR Repository				
Patient ID Cross-Referencing Service (PIDs)	PIX Manager	R			
	Patient Demographics Supplier	R			
	Patient Identity Source	R			
Personal Health Record (PHR) Service Provider	Patient Identity Source	C [101]	HITSP/T23	Patient Demographics Query	R
	PIX Consumer	C [101]	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
	Patient Demographics Consumer	C [101]	HITSP/TP23	Patient Demographics Query	R
	Document Repository	O	HITSP/TP13	Retrieve Document	R
				Retrieve Documents Set	R
				Provide & Register Document Set	R
	Document Source	R	HITSP/TP13	Provide & Register Document Set	R
	Document Consumer	R	HITSP/TP13	Query Registry	R
				Retrieve Documents	R
	Content Creator	R	HITSP/C32	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
				Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
				Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
		R	HITSP/C37	Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
				Consent Document Component	R
				Consumer-Document Display Subset (See Section 3.2.3.9)	R
		R	HITSP/TP30	Consumer-Document Import Subset (see Section 3.2.3.10)	O
	Content Consumer	R	HITSP/C32	Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
				Consumer-Registration Discrete Data Import Subset (see Section 3.2.3.11)	O
				Consumer-Medication and Immunization History Discrete Data Import Subset (see Section 3.2.3.12)	O
				Consumer-Conditions and Allergy Discrete Data Import Subset (see Section 3.2.3.13)	O
		R	HITSP/C37	Consumer-Laboratory Discrete Data Import Subset (see Section 3.2.3.14)	O
				Consumer-Document Display Subset (See Section 3.2.3.9)	R
				Consumer-Document Import Subset (see Section 3.2.3.10)	O
		R	HITSP/TP30	Consumer-Lab Report Discrete Data Import Subset (see Section 3.2.3.15)	O
	Audit Record Source	R	HITSP/T15	Consent Document Component	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content (T/C)	T/C Optionality*
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
Service Providers & Other Healthcare Systems	Same as Facility EHR Repository				
Public Health Agencies System	Same as Facility EHR Repository				
Information Service Provider (Telematics Service Provider (TSP))	Document Source	R	GAP	Provide & Register Document Set	R
	Content Creator	R	GAP	Vehicle crash data set Content Component	R
	Message Source	R	GAP	Provide & Register message	R

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

Actor Optionality Conditions

- C [101] - Shall support (Patient Identity Source plus PIX Consumer) and/or Patient Demographics Consumer
- C [102] - Required if Access Control Request Transaction is not supported
- C [103] - Required when a Document Repository and/or a Document Registry is supported

Transaction/Content (T/C) Optionality Conditions

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

3.2.3.1 C32 "Creator-Registration Subset"

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

Table 3.2.3.1-1 Creator Registration Subset Content Modules

Content Modules
Person Information
Language Spoken
Support

Content Modules
Healthcare Provider
Insurance Provider
Pregnancy
Information Source
Comments
Advance Directives

Note: HITSP/C32 Required Content Modules that are not listed above shall contain “unknown”.

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

3.2.3.2 C32 “Creator-Registration-Coded Subset”

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

3.2.3.3 C32 “Creator-Medication and Immunization History Subset”

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

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

Content Modules
Person Information
Healthcare Provider
Medications – Prescription and Non-Prescription
Information Source
Comments

Note: HITSP/C32 Required Content Modules that are not listed above shall contain “unknown”.
The medication entry may contain the concepts but without an associated code.

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

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

3.2.3.5 C32 “Creator-Conditions and Allergy Subset”

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

Table 3.2.3.5-1 Creator Conditions and Allergy Subset Content Modules

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

Note: HITSP/C32 Required Content Modules that are not listed above shall contain “unknown”.
The condition and allergy entries contain the concepts but without the HITSP/C32 specified code set.

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

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

3.2.3.7 C32 “Creator-Laboratory Section Subset”

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

Table 3.2.3.7-1 Creator Laboratory Subset Content Modules

Content Modules
Person Information
Healthcare Provider
Results
Information Source
Comments

Note: HITSP/C32 Required Content Modules that are not listed above shall contain “unknown”. The results entries contain the concepts but without the HITSP/C32 specified code set.

3.2.3.8 C32 “Creator-Laboratory Section-Coded Subset”

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

3.2.3.9 Consumer-Document Display Subset

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

3.2.3.10 Consumer-Document Import Subset

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

3.2.3.11 C32 “Consumer-Registration Discrete Data Import Subset”

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

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

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

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

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

3.2.3.14 C32 “Consumer-Laboratory Discrete Data Import Subset”

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

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

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

3.2.4 CONSTRUCT DEPENDENCIES

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

Table 3.2.4-1 Construct Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
none	Not applicable	Not applicable	Not applicable

3.2.5 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

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

Table 3.2.5-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
All	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) Component	Create this document as defined, except the document shall NOT be anonymized unless being sent to a Public Heath Facility or Emergency Operations Center	General	Need to transfer real patient data for patient care; other actors need aggregate or trend data, but do not usually need to know individual identities
All	HITSP/C39 - Encounter Message Component	Create these messages as defined, except the messages shall NOT be anonymized unless being sent to a Public Heath Facility or Emergency operations center	General	Need to transfer real patient data for patient care

4.0 STANDARDS SELECTION

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

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

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

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

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

4.1 TABLE OF SELECTED STANDARDS

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

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

4.1.1 REGULATORY GUIDANCE

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

Table 4.1.1-1 Regulatory Guidance

Standard	Description
No applicable regulatory guidance	

4.1.2 SELECTED STANDARDS

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

Table 4.1.2-1 Selected Standards Linked to HITSP Constructs

Standard Name	HITSP Construct	Remarks/ Minor HITSP GAPs
CDC Race and Ethnicity Code Sets	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Federal Information Processing Standards (FIPS) Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas Publication # 5-2, May, 1987	HITSP/C39 - Encounter Message	
Federal Medication Terminologies	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Health Care Provider Taxonomy	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Health Level Seven (HL7) Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD), April 01, 2007	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/TP20 - Access Control	
Health Level Seven (HL7) Version 2.5	HITSP/C39 - Encounter Message HITSP/TP22 – Patient ID Cross-Referencing	
Health Level Seven (HL7) Version 2.5/2.5.1	HITSP/T23 - Patient Demographics Query	
Health Level Seven (HL7) Version 3.0 Clinical Document Architecture (CDA/CDA R2)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	HITSP/T15 - Collect and Communicate Security Audit Trail HITSP/T17 - Secured Communication Channel	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Consistent Time (CT) Integration Profile	HITSP/T16 - Consistent Time	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	HITSP/C19 - Entity Identity Assertion	

Standard Name	HITSP Construct	Remarks/ Minor HITSP GAPs
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Demographics Query (PDQ) Integration Profile	HITSP/T23 - Patient Demographics Query	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) - Emergency Department Encounter Summary (EDES), Technical Framework Supplement, Volume I, Revision 3.0, 2007-2008.	HITSP/C28 - Emergency Care Summary Document Using IHE Emergency Department Encounter Summary (EDES)	
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	

Standard Name	HITSP Construct	Remarks/ Minor HITSP GAPs
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	HITSP/C39 - Encounter Message	
International Classification of Diseases, 10th Revision, Related Health Problems (ICD-10-CM)	HITSP/C39 - Encounter Message HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
International Classification of Diseases, 9th Revision, Clinical Modifications (ICD-9-CM)	HITSP/C39 - Encounter Message HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C39 - Encounter Message HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF), The mailto URL (Uniform Resource Locators) scheme (RFC 2368) Proposed Standard	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Internet Engineering Task Force (IETF), The tel URI (Uniform Resource Identifier) for Telephone Numbers (RFC 3966) Proposed Standard	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
Logical Observation Identifiers Names and Codes (LOINC®)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C35 - Lab Result Terminology HITSP/C39 – Encounter Message HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
National Library of Medicine (NLM) Unified Medical Language System (UMLS) RxNorm	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD)	
National Uniform Billing Committee (NUBC) Uniform Bill Version 1992 (UB-92) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	HITSP/C39 - Encounter Message	

Standard Name	HITSP Construct	Remarks/ Minor HITSP GAPs
National Uniform Billing Committee (NUBC) Uniform Bill Version 2007 (UB-04) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS-Federation), Version 1.1, December 2006	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/TP20 - Access Control	
Unified Code for Units of Measure (UCUM)	HITSP/C32 - Summary Documents Using HL7 Continuity of Care Document (CCD) HITSP/C39 - Encounter Message HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	

4.1.3 INFORMATIVE REFERENCE STANDARDS

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

Table 4.1.3-1 Informative Reference Standards

Standard Name	Description/Reason for Use
American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), #359-2004	This standard describes RBAC features that have achieved acceptance in the commercial marketplace. It includes a reference model and functional specifications for the RBAC features defined in the reference model. It is intended for (1) software engineers and product development managers who design products incorporating access control features; and (2) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional. For more information visit http://www.ansi.org

Standard Name	Description/Reason for Use
American Society for Testing and Materials (ASTM) Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org
American Society for Testing and Materials (ASTM) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1)." For more information visit www.astm.org
Council for Affordable Quality Health Care (CAQH) Committee on Operating Rules for Information Exchange (CORE) Phase I Operating Rules	Provide agreed-upon business rules and guidelines for using and processing eligibility inquiry and response transactions between providers and health plans; in particular those that have been adopted under HIPAA. For more information visit www.caqh.org
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org

Standard Name	Description/Reason for Use
Health Level Seven (HL7) Version 3.0	The HL7 Version 3.0 Messaging Standard is an application protocol for electronic data exchange in healthcare. Version 3.0 is based on a Reference Information Model (RIM); which is used to instantiate various message formats. Value sets / code tables are contained in the standard. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) Technical Framework Revision 1.0	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross-Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross-Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net

Standard Name	Description/Reason for Use
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	The International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS), describes the classification of inpatient procedures for statistical purposes and for the indexing of healthcare records by procedures. ICD-10-PCS is a procedural coding system managed by the Centers for Medicare and Medicaid Services (CMS). For more information visit www.cms.hhs.gov Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Organization for Standardization (ISO) Health informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992	Establishes user requirements for the service definition needed to support the security alarm reporting function, defines the service provided by the security alarm reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics -- Information technology -- Text and office systems - Office Document Architecture (ODA) and interchange format, Technical Report on ISO 8613 implementation testing, Technical Specification # ISO/IEC CD 10183 -- Part 3: Testing procedure.	Specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics -- Privilege management and access control(PMAC), Technical Specification #22600 -- Part 1: Overview and policy management, July 2006	Supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics – Functional and Structural Roles (ISO SF Roles), Technical Specification #21298 , Draft May, 2007	This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare actors Directory services: structural roles are usefully recorded within directories of health care providers (see for example, ISO TS 21091 Health Informatics – Directory services for security, communications, and identification of professionals and patients). Audit trails: functional roles are usefully recorded within audit trails for health information applications Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary. For more information visit www.iso.org

Standard Name	Description/Reason for Use
National Cancer Institute (NCI) Thesaurus: Route of Administration	Route of Administration is the path by which a particular drug product is introduced on or into the body. The medication terminology is maintained by the NCI Thesaurus, a reference terminology and biomedical ontology used in a growing number of NCI and other systems. It covers vocabulary for clinical care, translational and basic research, and public information and administrative activities. The NCI Thesaurus provides definitions, synonyms, and other information on nearly 10,000 cancers and related diseases, 8,000 single agents and combination therapies, and a wide range of other topics related to cancer and biomedical research. It is part of the Federal Medication Terminologies. For more information, visit www.cancer.gov
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security SOAP Message Security Version 1.0	Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e.. support multiple security token formats. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Simple Object Access Protocol (SOAP) Version 1.1	SOAP is a protocol specification for invoking methods on servers, services, components and objects. SOAP codifies the existing practice of using XML and HTTP as a method invocation mechanism. The SOAP specification mandates a small number of HTTP headers that facilitate firewall/proxy filtering plus an XML vocabulary that is used for representing method parameters, return values, and exceptions." {DevelopMentor} SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. For more information visit www.oasis-open.org
Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity	This classification provides a minimum standard for maintaining, collecting, and presenting data on race and ethnicity for all Federal-reporting purposes. The categories in this classification are social-political constructs and should not be interpreted as being scientific or anthropological in nature. The standards have been developed to provide a common language for uniformity and comparability in the collection and use of data on race and ethnicity by Federal agencies. For more information visit www.census.gov

There are a number of standards that will be considered as part of the Gap/Overlap Road Map work group effort described in the next sections. The organizations and standards to be evaluated include, but are not limited to those listed in the following table.

Table 4.1-2 Candidate Standards Linked to HITSP Constructs

Standard Name	HITSP Construct	Remarks/ Minor HITSP GAPs
OASIS Emergency Data Exchange Language Distribution Element (EDXL DE)	Routing of wide variety of data payloads as noted above in text for both Situational Awareness and patient care	Candidate Standard
OASIS Common Alerting Protocol 1.1	Alert and warning portions of Situational Awareness	Candidate Standard
OASIS EDXL HAVE	Provisional (now in second round public comment). Payload distributed by EDXL DE. Provides hospital bed, staffed services and related information for use by ECS and other actors.	Candidate Standard
OASIS EDXL Resource Messages	Intended for Use. A series of situational awareness messages about the seeking, committing, deploying and returning any form of non-human resource. In final stages of resolution of public comment. Balloting expected in next couple of months.	Candidate Standard
Vehicular Emergency Data Set (VEDS)	Intended for Use. Incident and vehicular telematics data. To be combined, as appropriate, with other data and standards as they emerge such as identity, patient-specific health information and emergency contact information.	Candidate Standard
National Highway Traffic Safety Administration NEMSIS Data Set	Intended for Use. Standardized pre-hospital patient and scene data collected by EMS during a patient encounter	Candidate Standard

4.2 HITSP GAPS WHERE THERE ARE NO STANDARDS

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

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

The HITSP Gap is only relative to the specific Emergency Responder event. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross team validation of the HITSP Gap, provisional recommendations and peer review.

In October, 2007 the ER-EHR Work Group reviewed the identified gaps in a special session with Emergency Medical Service and Law Enforcement Subject Matter Experts. The intent of the session was to: 1) ensure that all gaps had been identified, 2) ensure that the identified gaps have been appropriately framed/described and included on the "Road Map" for closure/resolution, and 3) Identify the appropriate groups or individuals that would help lead an effort to effectively "Close the Gap". During that session, four specific, although related, "gap closing projects" were identified and/or proposed by participants.

The Work Group agreed that the National Emergency Medical Services Information Systems (NEMSIS) Technical Support Center and the National Trauma Data Bank (NTDB) Technical Center would chair a work group to develop a draft plan which defines a process for closing the gaps at least for these specific four issues. Different organizations will take the initial lead on drafting suggested plans as to how to address some of these issues, subject to NEMSIS' coordination and leadership. The overall plan will be presented to the TC. The plan shall specifically address a process which can be used to reach a collaborative and transparent approach for:

- Identification of and harmonization of current data taxonomies and messaging standards that are/have been in use by the different organizations that operate in the pre-hospital and ED domain and, if necessary, their mapping to standard terminologies and data structures
- Identification of and strategy for involving all the significantly affected stakeholders both in development and in the maintenance of these standards. This will include at a minimum groups such as NEMSIS, NHTSA, HL7, DHS-DM, IHE, NTDB, NASEMSO, APCO, COMCARE, HIMSS, NENA and others
- Identification of and strategy for involving stakeholders both in development and in the maintenance of the messaging/exchange standards
- Plan to develop criteria for SDO selection based on the HITSP Tier 2 Criteria
- How and when SDO approved messaging/exchange standards will be included in a subsequent iteration of HITSP/IS04

The four planned projects for which the NEMSIS chaired Work Group will report back to the TC are:

- Finding a method of assigning and adopting unique identifiers for both incidents and patients so data from heterogeneous systems can be linked
- Exploring common approaches of delivering third party incident information such as telematics data to the ECS and other emergency responders
- Reaching agreement between healthcare and other emergency responders on a common terminology ("Managed List") for incident types
- Harmonizing the data taxonomies of hospital, EMS, and other emergency responders to the extent necessary to implement the ER-EHR

In addition to the four projects above, there are four additional gap area projects, which are:

- Decision Support Tools
- Core Services
- Situation Awareness Messaging
- Emergency Contact Registry (ECON)

Details on each of these are discussed in the following table. The table below identifies the Use Case events and known associated HITSP Gaps, along with the recommended resolutions.

Table 4.2-1 Use Case Events and Associated HITSP Gaps

Event Code	Event Description	Identified HITSP Gaps	Recommended Resolution
6.1.1.1	ECS Gathering of Information	There are three levels of standardization needed at the ECS level: • System (middleware) level: for routing, security (Covered within SPWG) • Payload: for individual incident and patient type • Interface with decision support tools Information about incidents and patients will come from multiple sources at multiple times during a response. There needs to be a way to link informational inputs to a patient and the patient to an incident. Gathering information is mostly verbal today providing data such as incident location, chief complaint, patient info etc. Data sources and services for various types of incidents are beginning to develop (e.g., telematics, heart monitors, medical panic buttons). Typically these involve a commercial call center service to which the initial alarm goes, and which in turn contacts 9-1-1. Outputs from such call centers to the emergency response community need to be standardized. Each of these has the ability to send data to the ECS, On-Site Care and ED, and that process needs to be accelerated. However, for small scale incidents involving motor vehicles there is the ability to transmit vehicle incident severity data. To ensure appropriate routing of information about incidents, there needs to be a standardized list of incident types that all emergency domains subscribe to. This is not necessarily a standard. It is referred to as a "Managed List" in the OASIS EDXL Distribution Element Standard. Similarly, there are a growing number of private PHR services of various kinds. Queries to and outputs from such services need to be standardized.	Identifier Project: Identify and assemble 'topic experts' to address resolution of identified HITSP Gap which at least include NEMSIS (in their lead role), NHTSA, HL7, DHS-DM, IHE, NTDB, NASEMSO, APCO, COMCARE, HIMSS, NENA and others. The panel determined that the best way to address the issue of unique person and incident identifiers is to develop a standard and practice whereby the first actor assigns unique identifiers, or the equivalent, to both an incident and any victims, and the other actors adopt those identifiers as soon as they become aware of them. When a person's actual identity is established, then it should be associated with the unique identifiers, given above. Additionally, a person's historical health information (EHR/ECON/PHR) should be linked to the unique identifiers. Common Approaches to Delivering Incident Information Project. This effort will consider, at a minimum: OASIS EDXL Distribution Element as the routing "header" for the pre-hospital messaging. The telematics service providers (OnStar and ATX) are using or are committed to using the VEDS payload for data coming from their cars and centers. The same approach should be used for similar incident types, perhaps starting with common ones like: medical panic buttons, falls, hazmat and radiation sensors with appropriate practitioner groups and SDOs, developing detailed requirements and specifications for high profile, multiple use payloads. NEMSIS in collaboration with COMCARE, NENA, APCO, industry stakeholders, and others will develop the initial plan for this Common Approach and report back to the TC on how to extend the above approach to information about other such incident types. OASIS, HL7 or others would be considered as candidate host SDOs for messaging standards. Standardized List of Incident Types Project. There needs to be a standardized list of incident types that all emergency domains subscribe to. NEMSIS in collaboration with COMCARE, NENA, APCO, industry stakeholders, and others will develop the initial plan for developing this Managed List and report back to the TC on how to extend the above approach to information about other such incident types. Decision Support Tools Practitioner groups need to develop detailed requirements for initial decision support tools, including: matching HAVE output with patient data to make ED/hospital recommendations new versions of EMD using incident data and PHR/EHR data Core Services Core services such as agency location and access control/identity management need to be developed to enable routing and security. They need to be standardized and are currently being addressed by the Core Services Initiative led by COMCARE, Open Geospatial Consortium (OGC), National Association of State Fire Marshalls and NENA.

Event Code	Event Description	Identified HITSP Gaps	Recommended Resolution
6.1.1.2 6.1.1.3 6.2.6.2 6.3.1.2	On-Site Management and Coordination – Situational Awareness Messages and Reports to and from Actors	Various standards to exchange and accumulate information about an incident and then to compile and distribute Situational Awareness Reports keeping all involved entities informed of the situation. If ICS has been activated, the latter will be standardized ICS forms.	Situational Awareness Reporting Project The OASIS EDXL DE and OASIS Resource Messages may be used for this purpose. Other Situational Awareness Reporting messages are in early stages of development by a DHS sponsored process. Currently, the DHS-Disaster Management PWG is developing potential standards that may be used. The TC will monitor these efforts.
6.1.3.1 6.2.3.1	Emergency Contact Registry (ECON) Query	A standard for on-site care providers, typically law enforcement, to query an Emergency Contact Registry (ECON) based upon a unique identifier (e.g., VIN#) to help ascertain victim identity and to obtain victim's emergency contact information to facilitate family member reunification and expedite next-of-kin notification.	Emergency Contact Registry (ECON) Project IHE is developing a standardized query for patient-specific emergency contact information. This effort is underway. On 12/3/07 the IHE ITI Technical Committee approved the ECON Query Profile Proposal for their 2008 work cycle. In addition, the IHE PCC Technical Committee has approved the Pre-Hospital Patient Care Report (PCR) Profile Proposal for their 2008 work cycle which will develop a standard for on-site care provider electronic download and automated entry of patient-specific Emergency Contact Registry (ECON), Personal Health Record (PHR) and/or Electronic Health Record (EHR) data into an on-site Pre-Hospital Patient Care Report (PCR) system.
6.1.4.1	Assess, triage and treat patient – Transmit Heath Information from Devices	A standard or standards to transmit medical device information such as EKG, Blood Pressure, Pulse OX, etc. directly into the Episode of Care Record, or from the software of vendors to the Episode of Care Record	No Project Identified: Remote monitoring devices is within the purview of the 2008 Use Case and will be covered there. The solution needed is for data from these electronic devices to automatically update the Episode of Care Record, saving time and avoiding errors by responders. This will also allow trend lines to be easily developed. Vendors should standardize the output from their devices or provide the functional equivalent.

Event Code	Event Description	Identified HITSP Gaps	Recommended Resolution
6.1.7.1	Start collection of data for the Electronic Emergency Care Record at ECS and then On-Site	Emergency Response Data Architecture (ERDA), which has segments: A standard data structure to accumulate patient, dispatch and care information which can be used by the various care providers and by parties such as public health. From this data structure each actor can define the data it needs to accomplish its mission (dispatch, then primary care, then triage, etc), including the production of required reports, such as an ambulance run report required by state EMS agencies. This growing body of information facilitates every step of care, from the decision of what kind of resource to dispatch to the "hand off" of the patient, such as from EMT care to the emergency department. Similarly, there are a growing number of private Personal Health Record (PHR), Emergency Contact Registry (ECON) and/or Electronic Health Record (EHR) services of various kinds. Specific data type queries for ECS and on-site care providers (EMS, Law Enforcement, Fire) to access and exchange data from such services needs to be standardized.	Data Taxonomy Harmonization Project, NEMSIS will develop a plan which describes the recommended process, stakeholders, current data standards for harmonization of taxonomies and time frames for resolving/addressing data harmonization issues between various pre-hospital, hospital and public health actors. The plan will address the collaboration and involvement of stakeholders such as; NHTSA, HL7, DHS-DM, IHE, NTDB, NASEMSO, APCO, COMCARE, HIMSS, NENA and others. NEMSIS will take the lead on developing the part of the overall plan to accomplish this, which is due within 45 days. Identify and work with appropriate SDOs to define standard data structure. Review and validate data requirements produced by Integrated Patient Tracking Initiative COMCARE led (www.patienttracking.org). This process had representatives of each stakeholder profession state their data needs from ECS to On-Site, to ED and definitive care, to EOC and public health/Red Cross. HIMSS and COMCARE are launching a national effort to validate these requirements. This information needs to be accumulated over time as not all information is known during one moment of time, and from multiple sources. Example data includes: Patient Demographics, Emergency Contact, Medical/Surgical History, Medications, Allergies, Pregnancy Status, Organ donor, outputs of decision support tools predicting injuries and suggesting care protocol, Clinical Complaint, Primary Clinical Impressions, Last Meals, Events leading up to incident, Findings (vital signs, BP Skin color, Respiratory Rate) and trends of such findings, Assessment and Plan IHE Patient Care Coordination (PCC), HL7 Emergency Department (ED) SIG and NEMSIS have related plans to address this need. An integrated mechanism to document the care, condition, treatment and location/destination of patient will be covered within the NEMSIS standardization plan.
6.2.1.1	Emergency care site management and coordination – Patient En-route Alert	A standard to notify the Emergency Department of an incoming patient and to provide ECS and On-Site care information.	Identify and assemble 'topic experts' to address resolution of identified HITSP Gap which at least includes NHTSA, HL7, DHS-DM, IHE, NTDB, NASEMSO, APCO, COMCARE, HIMSS, NENA and others. Example data includes information defined in event 6.1.7.1. The OASIS EDXL DE and OASIS CAP will be considered for this purpose as part of the GAP/Overlap Road Map effort.
6.2.6.1c	Complete disposition, Provide Information – Patient is deceased	A standard to notify organizations of a patient's death (for events such as next of kin notification, organ recovery etc.)	Identify and assemble 'topic experts' to address resolution of identified HITSP Gap which at least includes NHTSA, HL7, DHS-DM, IHE, NTDB, NASEMSO, APCO, COMCARE, HIMSS, NENA and others.

4.3 STANDARD OVERLAPS

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

Nursing Terminology Overlap

An overlap in standards has been identified by the ER-EHR Work Group in the Use Case scenario for Present Episode of Care. In particular, many of the individual data elements in Scenario 1 (On-Site), Scenario 2 (ED) and Scenario 3 (Definitive Care) may be captured by nursing and thus will be dependent upon an interoperable nursing terminology schema. Other required information in Nursing Notes, Vital Signs, Triage, Discharge Summary and others included nursing activities will be dependent on elements of an interoperable nursing terminology. A Work Group of nurses with expertise in nursing terminologies and emergency nursing was convened to address this overlap. The HITSP Nursing Terminology Work Group will prepare a work plan and report back to the ER-EHR Work Group within 45 days. It is expected that the work effort required will be completed within six months.

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
6.1.1.16.1.1.2 6.1.1.3 6.2.1.1 6.2.6.2 6.3.1.2 6.1.7.1	ECS Gathering of Information On-Site Management and Coordination – Situational Awareness Report to and from Actors Start collection of data for the Electronic Care Record at ECS and then On-Site Emergency care site management and coordination – Patient En-route Alert	Message in HL7 V2 Message in HL7 V3 OASIS HAVE, EDXL, CAP, DE NEMSIS NIEM DEEDS GJXDM	There are many sub-domain niche de-facto standards and vocabularies, which provide partial solutions and sometimes overlap. These should be jointly worked and harmonized as part of the HITSP Gap roadmap discussed in Table 4.2.1

5.0 TECHNICAL IMPLEMENTATION

5.1 CONFORMANCE

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

5.1.1 CONFORMANCE CRITERIA

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

Claims of conformance to this specification must be made using the following language:
This product conforms to the HITSP Emergency Responder Electronic Health Record Interoperability Specification, available at www.hitsp.org.

5.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

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

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

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

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

5.1.3 TEST METHODS

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

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

6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF STANDARDS

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

Table 6.1-1 Description of Standards

Standard Name	Description
CDC Race and Ethnicity Code Sets	The U.S. Centers for Disease Control and Prevention (CDC) has prepared a code set for use in coding race and ethnicity data. This code set is based on current federal standards for classifying data on race and ethnicity, specifically the minimum race and ethnicity categories defined by the U.S. Office of Management and Budget (OMB) and a more detailed set of race and ethnicity categories maintained by the U.S. Bureau of the Census (BC). The main purpose of the code set is to facilitate use of federal standards for classifying data on race and ethnicity when these data are exchanged, stored, retrieved, or analyzed in electronic form. At the same time, the code set can be applied to paper-based record systems to the extent that these systems are used to collect, maintain, and report data on race and ethnicity in accordance with current federal standards. For more information visit www.cdc.gov
Federal Information Processing Standards (FIPS) Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas Publication # 5-2, May, 1987	A set of two-digit numeric codes and a set of two-letter alphabetic codes for representing the 50 states, the District of Columbia and the outlying areas of the United States, and associated areas. The standard covers all land areas under the sovereignty of the United States, the freely associated states of Federated States of Micronesia and Marshall Islands, and the trust territory of Palau. For more information visit www.itl.nist.gov. NOTE: ASC X12 transactions and ASC X12N Implementation Guides do not allow use of this standard; instead they require use of the U.S. Postal Service's National Zip Code and Post Office Directory -- which provides similar alphabetic code values
Federal Medication Terminologies	A set of controlled terminologies and code sets developed and maintained as part of a collaboration between the Food and Drug Administration, National Library of Medicine, Veterans Health Administration, National Cancer Institute and Agency for Healthcare Research and Quality related to medications, including medication proprietary and nonproprietary names, clinical drug code (RxNorm); ingredient names and Unique Ingredient Identifiers (UNII); routes of administration, dosage forms, and units of presentation from the NCI Thesaurus (NCIt); and certain pharmacological drug classes from the National Drug File Reference Terminology (NDF-RT) . The Federal Medication Terminology leverages medication models maintained by the Food and Drug Administration (ex. UNII, NDC Codes), National Library of Medicine (RxNorm), the Veterans Health Administration (NDF-RT), and the National Cancer Institute (NCIt). Information on the Federal Medication Terminologies may be found and downloaded from the NCI Web portal terminology resources page at www.cancer.gov/cancertopics
Health Care Provider Taxonomy	The Health Care Provider Taxonomy code set is a collection of unique alphanumeric codes, ten characters in length. The Health Care Provider Taxonomy code set includes specialty categories for individuals, groups of individuals, and non-individuals. The National Uniform Claims Committee maintains this code set. The complete code set is available from the Washington Publishing Company at www.wpc-edi.com

Standard Name	Description
Health Level Seven (HL7) Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD), April 01, 2007	The Continuity of Care Document implementation guide describes constraints on the HL7 Clinical Document Architecture, Release 2 (CDA) specification in accordance with requirements set forward in ASTM E2369-05 Standard Specification for Continuity of Care Record (CCR). The resulting specification, known as the Continuity of Care Document (CCD), is developed as a collaborative effort between ASTM and HL7. It is intended as an alternate implementation to the one specified in ASTM ADJE2369 for those institutions or organizations committed to implementation of the HL7 Clinical Document Architecture
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5/2.5.1	The HL7 Version 2.5 and 2.5.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 4, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. They are also used in HL7 order messages. For more information visit www.hl7.org
Health Level Seven (HL7) Version 3.0 Clinical Document Architecture (CDA/CDA R2)	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit www.hl7.org
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	The Data Consent RMIM captures the data and associations needed to (1) record or report a consumer's consent or dissent to authorize the access, collection, use, or disclosure of personally identifiable information; (2) convey a provider's request or intent to override a patient's recorded consent or dissent; (3) convey a type of consent directive associated with a privacy policy; or (4) to record or report a consumer's consent directive, which is to be applied to future access, collection, use or disclosure of personally identifiable information. For more information visit www.hl7.org

Standard Name	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Consistent Time (CT) Integration Profile	The Consistent Time Integration Profile (CT) provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE CT Integration Profile, and other transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the user identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the entities, and others that may have chosen to use a third party to perform the authentication. The latest version of the IHE framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Demographics Query (PDQ) Integration Profile	Provides ways for multiple distributed applications to query a central patient information server for a list of patients, based on user-defined search criteria, and retrieve a patient's demographic (and, optionally, visit or visit-related) information directly into the application. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net

Standard Name	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	The Basic Patient Privacy Consents (BPPC) profile provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use. This profile complements XDS by describing a mechanism whereby an XDS Affinity Domain can develop and implement multiple privacy policies, and describes how that mechanism can be integrated with the access control mechanisms supported by the XDS Actors (e.g. systems). There are two key parts of the profile: 1) It provides a document content specification for capturing a patient acknowledgement of a privacy consent policy or policies. 2) It describes the method by which XD* Actors can enforce the privacy policies determined by the document confidentialityCode related to the patient privacy consents. The latest version of specification is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	The Patient Identifier Cross-referencing Integration Profile (PIX) is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1)The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification. By specifying the above transactions among specific actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise.. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev.3.0 for Final Text, specifies the IHE transactions defined and implemented as of December 9, 2006. The latest version of the IHE Technical Framework is available at www.ihe.net

Standard Name	Description
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC) - Emergency Department Encounter Summary (EDES), Technical Framework Supplement, Volume I, Revision 3.0, 2007-2008.	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Emergency Department Encounter Summary (EDES) enables the sharing of emergency department summary information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	The International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS), describes the classification of inpatient procedures for statistical purposes and for the indexing of healthcare records by procedures. ICD-10-PCS is a procedural coding system managed by the Centers for Medicare and Medicaid Services (CMS). For more information visit www.cms.hhs.gov. Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Classification of Diseases, 10th Revision, Related Health Problems (ICD-10-CM)	The International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM), describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases. The National Center for Health Statistics (NCHS), the Federal agency responsible for use of the International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) in the United States, developed a clinical modification of the classification for morbidity purposes. For more information visit www.cdc.gov/nchs. Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Classification of Diseases, 9th Revision, Clinical Modifications (ICD-9-CM)	The International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), Volumes I, II (diagnoses) and III (procedures) describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases and procedures. For more information visit www.cdc.gov/nchs
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	SNOMED CT consists of a technical design, core content architecture, and Core content. SNOMED CT Core content includes the technical specification of SNOMED CT and fully integrated multi-specialty clinical content. The Core content also includes a concepts table, description table, relationships table, history table, ICD-9-CM mapping, and Technical Reference Guide. Additionally, SNOMED CT provides a framework to manage language dialects, clinically relevant subsets, qualifiers and extensions, as well as concepts and terms unique to particular organizations or localities. For more information visit www.ihtsdo.com
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. For more information visit www.ietf.org

Standard Name	Description
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), The mailto URL (Uniform Resource Locators) scheme (RFC 2368) Proposed Standard	This document defines the format of Uniform Resource Locators (URL) for designating electronic mail addresses. It is one of a suite of documents which replace RFC 1738, 'Uniform Resource Locators', and RFC 1808, 'Relative Uniform Resource Locators'. The syntax of 'mailto' URLs from RFC 1738 is extended to allow creation of more RFC 822 messages by allowing the URL to express additional header and body fields. For more information visit www.ietf.org
Internet Engineering Task Force (IETF), The tel URI (Uniform Resource Identifier) for Telephone Numbers (RFC 3966) Proposed Standard	This document specifies the URI (Uniform Resource Identifier) scheme "tel". The "tel" URI describes resources identified by telephone numbers. This document obsoletes RFC 2806. For more information visit www.ietf.org
Logical Observation Identifiers Names and Codes (LOINC®)	A database of universal identifiers for laboratory and other clinical observations. The laboratory portion of the LOINC database contains the usual categories of chemistry, hematology, serology, microbiology (including parasitology and virology), and toxicology; as well as categories for drugs and the cell counts typically reported on a complete blood count or a cerebrospinal fluid cell count. Antibiotic susceptibilities are a separate category. The clinical portion of the LOINC database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments, and other clinical observations. For more information visit www.loinc.org
National Library of Medicine (NLM) Unified Medical Language System (UMLS) RxNorm	Provides standard names for (1) clinical drugs and (2) drug dose forms as administered to a patient. Also provides links from clinical drugs, both branded and generic, to their active ingredients, drug components (active ingredient + strength), and related brand names. Food and Drug Administration (FDA) National Drug Codes (NDCs) for specific drug products and many of the drug vocabularies commonly used in pharmacy management and drug interaction software are additionally linked to RxNorm. RxNorm is a part of the Federal Medication Terminologies. For more information visit www.nlm.nih.gov
National Uniform Billing Committee (NUBC) Uniform Bill Version 1992 (UB-92) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	A code set identifying status of patient discharge on an institutional claim (e.g., inpatient, outpatient, hospice, home care). For more information visit www.nubc.org
National Uniform Billing Committee (NUBC) Uniform Bill Version 2007 (UB-04) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	A code set identifying status of patient discharge on an institutional claim (e.g., inpatient, outpatient, hospice, home care). For more information visit www.nubc.org
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	SA SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims. For more information visit www.oasis-open.org

Standard Name	Description
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Toke Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XCML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit www.oasis-open.org
Unified Code for Units of Measure (UCUM)	A code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. For more information visit aurora.regenstrief.org

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

Table 6.1-2 Description of Candidate Standards

Standard Name	Description
OASIS Common Alerting Protocol (CAP) Version 1.1	The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience. CAP functions both as a standalone protocol and as a payload for EDXL messages. Visit http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf for more information
OASIS Emergency Data Exchange Language (EDXL) Distribution Element (DE) Version 1.0	This Distribution Element specification describes a standard message distribution framework for data sharing among emergency information systems using the XML-based Emergency Data Exchange Language (EDXL). This format may be used over any data transmission system, including but not limited to the SOAP HTTP binding. Visit http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf for more information.
OASIS Emergency Data Exchange Language (EDXL) Resource Messaging (RM) Version 1.0	This Distribution Element specification describes a standard message distribution framework for data sharing among emergency information systems using the XML-based Emergency Data Exchange Language (EDXL). This format may be used over any data transmission system, including but not limited to the SOAP HTTP binding. Visit http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf for more information.

Standard Name	Description
OASIS Emergency Data Exchange Language (EDXL) Hospital Availability Exchange (HAVE) Version 1.0	This Hospital Availability Exchange (HAVE) describes a standard message for data sharing among emergency information systems using the XML-based Emergency Data Exchange Language (EDXL). This format may be used over any data transmission system, including but not limited to the SOAP HTTP binding. The specification is approved as a Committee Draft and is open for public review through December 18, 2007. Visit http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency for more information
Vehicular Emergency Data Set (VEDS)	The Vehicular Emergency Data Set (VEDS) is an XML based data standard that determines useful and critical elements needed to prove an efficient emergency response to vehicular emergency incidents. The Protocol identifies crash and medical data elements. VEDS is the de facto standard currently being used in the field by OnStar. Visit www.comcare.org/veds.html for more information.
National Highway Traffic Safety Administration NEMSIS Data Set	The NHTSA EMS Uniform PreHospital Dataset, Version 2.2.1 is composed of three separate components. A Demographic Dataset provides a standardized set of definitions describing an EMS System. An EMS Dataset provides a standardized set of definitions describing an EMS event. The third component of the Version 2.2.1 standard is an XML format and definition created to promote the movement of the Version 2.2.1 data elements between data systems. Any implementation of the NHTSA Version 2.2.1 dataset must include the use of the Demographic dataset, EMS dataset, and XML standard. This document provides over 400 definitions which can be implemented by an EMS system. The National EMS Information System Initiative (NEMSIS) serves to provide technical assistance for the implementation of the dataset. National data elements are defined which should be collected by a National EMS Database but additional data elements should be considered for use at the state and local levels depending on each state or local EMS systems need. The goal of NEMSIS is to establish an EMS data system at the local, state, and national levels. Please see www.nemsis.org for more information.

6.2 ER-EHR ACRONYMS

(ACS)	Auxiliary Care Sites
(ADL)	Activities of Daily Living
(APCO)	Association of Public-Safety Communications Officials
(BAS)	Battalion Aid Stations
(CAD)	Computer Aided Dispatch
(CIMS)	Consequence Incident Management System
(CCD)	Continuity of Care Document
(DEEDS)	Data Elements for Emergency Department Systems
(DHS-DM)	Department of Homeland Security – Disaster Management
(DMATs)	Disaster Medical Assistance Teams
(DMORTs)	Disaster Mortuary Operational Response Teams
(EHR)	Electronic Health Record
(ECC)	Emergency Communications Center
(ECS)	Emergency Communications System
(ECON)	Emergency Contact Registry
(ED)	Emergency Department
(EMD)	Emergency Medical Dispatch
(EMS)	Emergency Medical Services
(EMTs)	Emergency Medical Technicians
(EOC)	Emergency Operations Centers
(ER-EHR)	Emergency Responder-Electronic Health Record
(ECR)	Episode of Care Record
(FEMA)	Federal Emergency Management Agency
(FMS)	Federal Medical Stations
(Global JXDM)(GJXDM)	Global Justice XML Data Model
(HIMSS)	Healthcare Information and Management Systems Society
(HRSA)	Health Resources and Services Administration's
(HIS)	Healthcare Information System
(ICS)	Incident Command System
(ME)	Medical Examiner
(MTF)	Medical Treatment Facility
(NASEMSO)	National Association of State EMS Officials
(NASFE)	National Association of State Fire Marshals
(NEMSIS)	National Emergency Medical Services Information Systems
(NENA)	National Emergency Number Association
(NHTSA)	National Highway Traffic Safety Administration
(NHTSA)	National Highway Traffic Safety Administration
(NIMS)	National Incident Management System
(NIEM)	National Information Exchange Model

(NTDB)	National Trauma Data Bank
(OASIS CAP)	OASIS Common Alerting Protocol
(OASIS DE)	OASIS Distribution Element
(OASIS EDXL)	OASIS Emergency Data Exchange Language
(OASIS HAVE)	OASIS Hospital Availability Exchange
(OGC)	Open Geospatial Consortium
(PCR)	Patient Care Report
(PHR)	Personal Health Record
(PHS)	Public Health Service
(PSAPs)	Public Safety Answering Points
(RFID)	Radio Frequency Identification
(SARs)	Situational Awareness Reports
(TSP)	Telematics Service Providers
(VIN)	Vehicle Identification Number
(VEDS)	Vehicular Emergency Data Set

7.0 CHANGE HISTORY

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

7.1 DECEMBER 5, 2007

The changes in this cycle address the following comments:

528, 531, 532, 537, 538, 549, 574, 629, 632, 669, 763, 764, 770, 786, 795, 799, 800, 802, 803, 804, 808, 809, 811, 812, 813, 820, 828, 830, 831, 884, 1171, 1178, 1179, 1182, 1186, 1190, 1191, 1192

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

- Incorporated all of the 287 Public Comment TC dispositions into the document
- Added detail to the description of the pre-hospital scenario to provide clarity regarding Interoperability requirements and differentiation among and between the Use Case elements.
    - Introduced the global concept of an Emergency Communications System for Emergency Communications Center to connect the current approach with the more advanced capabilities that are envisioned by the Use Case and underway in the EMS industry
    - Updated the UML diagrams for completeness, accuracy and improved understanding
- Reflected the additional analysis and Section 3 Design necessary to identify the appropriate HITSP constructs to support the Use Case
    - Figure 3.2.2-1 and 3.2.2-2 – Detailed Design
    - Table 3.2.3-1 – Detailed Design
    - Made a number of standards selections to support the constructs
- Identified and documented Section 4 Gaps and Overlaps in required standards and created supporting technical actors for the Gaps.
    - Created and documented a Road Map to address the Gaps and Overlaps identified including a planning effort, the identification of a number of interrelated projects and potential resources that will be involved in the resolution
    - Identified a number of Candidate Standards that will require review and analysis as part of the Road Map effort
- Reformatted the document content to adhere to the new HITSP document templates
    - Added diagrams and tables based on the new HITSP document templates

7.2 DECEMBER 13, 2007

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

7.3 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References. Please refer to the underlying constructs for specific changes to standards.

7.4 AUGUST 27, 2008

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