

# HITSP Communicate Emergency Alert Capability

---

HITSP/CAP136



Healthcare Information Technology Standards Panel

*Submitted to:*

**Healthcare Information Technology Standards Panel**

*Submitted by:*

**Capabilities Team**



## DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
0.0.1	Review Copy	Capabilities TT	January 31, 2010



## TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION.....</b>	<b>5</b>
1.1	Capability Overview .....	5
1.2	Scope .....	6
1.3	Copyright Permissions .....	6
1.4	Reference Documents .....	6
1.5	Guidance for Use of a Capability .....	6
<b>2.0</b>	<b>REQUIREMENTS ANALYSIS.....</b>	<b>8</b>
2.1	Introduction.....	8
2.2	Requirements .....	8
2.2.1	Information Exchanges.....	8
<b>3.0</b>	<b>EXTERNAL CAPABILITY OPTIONS .....</b>	<b>10</b>
3.1	Security and Privacy .....	10
<b>4.0</b>	<b>DESIGN SPECIFICATION .....</b>	<b>11</b>
4.1	Requirements Mapped to Constructs .....	11
4.1.1	Constructs.....	11
4.2	Constraints and Assumptions.....	11
4.3	Specified Interfaces by System Role .....	12
<b>5.0</b>	<b>STANDARDS .....</b>	<b>13</b>
5.1	Standards Used.....	13
5.1.1	Regulatory Guidance.....	13
5.1.2	Selected Standards.....	13
5.1.3	Informative Reference Standards .....	13
5.2	Standards Gaps and Overlaps .....	14
<b>6.0</b>	<b>APPENDIX .....</b>	<b>15</b>
<b>7.0</b>	<b>DOCUMENT UPDATES.....</b>	<b>16</b>
7.1	January 31, 2010.....	16



## FIGURES AND TABLES

Figure 2-1 Information Exchanges Between System Roles .....	9
Table 1-1 Reader's Guide for Capability .....	5
Table 1-2 Reference Documents .....	6
Table 2-1 Reader's Guide for Section 2.0.....	8
Table 2-2 Capability System Roles .....	8
Table 2-3 Supported Information Exchanges .....	8
Table 3-1 Reader's Guide for Section 3.0.....	10
Table 4-1 Reader's Guide for Section 4.0.....	11
Table 4-2 Information Exchanges Mapped to Constructs .....	11
Table 4-3 Context .....	12
Table 4-4 Alert Message Transmitter System Role Mapped to HITSP Construct Interfaces .....	12
Table 4-5 Alert Message Receiver System Role Mapped to HITSP Construct Interfaces .....	12
Table 4-6 Implementation Conditions.....	12
Table 5-1 Reader's Guide for Section 5.0.....	13
Table 5-2 Regulatory Guidance .....	13
Table 5-3 Selected Standards.....	13
Table 5-4 Informative Reference Standards.....	13
Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps.....	14
Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps .....	14



## 1.0 INTRODUCTION

This Healthcare Information Technology Standards Panel (HITSP) document is divided into Requirements Analysis, External Capability Options, Design Specifications and Standards sections which may be used by analysts, architects and implementers. Analysts refer to this document to determine if the Capability satisfies their requirements. Architects and system implementers refer to this document as the architectural specifications for a system design, while software developers will use a Capability as the source of the design for interoperable information exchange. The Appendix lists requirements satisfied by this Capability.

All sections may be useful to analysts and architects. However as shown in Table 1-1, different readers may find specific sections of greater interest and utility. This table is provided as an aid to readers to assist them in identifying sections to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

**Table 1-1 Reader's Guide for Capability**

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional security and privacy functions supported by the Capability
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	Lists regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	5.2 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues

### 1.1 CAPABILITY OVERVIEW

This Capability addresses interoperability requirements to support multicast of non-patient specific notification messages about emergencies events, alerts concerning incidence of communicable diseases,



alerts concerning population needs for vaccines and other generic alerts sent to an identified channel. The intended recipients are populations such as “all emergency departments in XXX county”, “within a geographic area”, etc. In the event that patient specific emergency alerting is required, other Capabilities such as HITSP/CAP120 Communicate Unstructured Document or HITSP/CAP122 Retrieval of Medical Knowledge may be used (See HITSP/IS10 Section 3.2.2).

## 1.2 SCOPE

A Capability enables business and policy requirements for a business need to be implemented through information exchanges specified in HITSP constructs. The objective of a Capability is to provide the bridge between the business, policy and implementation disciplines by defining a set of information exchanges at a level relevant to policy and business decisions and specifying the use of HITSP constructs sufficiently for implementation. A Capability supports stakeholder requirements and business processes and includes information content, infrastructure, security and privacy. The design of Capabilities leverages existing HITSP constructs and communication methodologies. As new constructs become available, the scope of this Capability may be extended.

## 1.3 COPYRIGHT PERMISSIONS

### COPYRIGHT NOTICE

© 2010 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

## 1.4 REFERENCE DOCUMENTS

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from [HITSP Web Site](#).

**Table 1-2 Reference Documents**

Reference Documents	Document Description
<a href="#">HITSP Acronyms List</a>	Lists and defines the acronyms used in this document
<a href="#">HITSP Glossary</a>	Provides definitions for relevant terms used by HITSP documents
<a href="#">TN900 – Security and Privacy</a>	TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs
<a href="#">TN903 – Data Architecture</a>	TN903 is a reference document that provides the overall context for use of the HITSP Data Architecture constructs
<a href="#">TN904 – Harmonization Framework and Exchange Architecture</a>	TN904 is a reference document that provides the overall context for use of the HITSP Harmonization Framework and Exchange Architecture constructs

## 1.5 GUIDANCE FOR USE OF A CAPABILITY

NOTE: For questions related to details on HITSP Capabilities and HITSP System Roles, please refer to HITSP/TN904 Harmonization Framework and Exchange Architecture Technical Note.

To use a HITSP Capability, a HITSP Interoperability Specification or an implementation conformance statement must assign specific systems to one or more HITSP Capability System Roles and identify how the HITSP Capability Options are to be addressed. In order to assign systems to HITSP System Roles, the reader uses Table 2-3 Supported Information Exchanges to determine what systems can support the specific information exchanges required. For an example of how HITSP System Roles and systems are mapped, readers can consult a HITSP Interoperability Specification Table 3-3 Orchestration of Capabilities by System. In the case of an Implementation Guide, systems can be assigned to HITSP System Roles using a similar methodology.

The use of a HITSP Capability implies that these specific rules will be followed:



- For each HITSP Capability System Role listed in Table 2-2 Capability System Roles, the defined responsibilities of that HITSP Capability System Role are supported. Responsibilities for the HITSP Capability System Role are defined as support for the HITSP Construct interfaces listed in Section 4.3 Specified Interfaces by System Role. Support implies that the system assigned to the HITSP Capability System Role makes the associated HITSP construct interfaces available for use by other systems. For those HITSP construct interfaces in Section 4.3 that have associated content optionality, the HITSP Capability System Role must comply with the optionality condition listed in Table 4-6 Implementation Conditions.
- Responsibilities also include the constraints and assumptions associated with use of a Capability, as outlined in Table 4-3 Context. For those Capabilities with Section 3.2 options, the following additional rules apply:
  1. Each topology option listed in Table 3-2 Topology Related Options should be supported by the implementation
  2. Each content import option listed in Table 3-3 Content Import Options should be supported by the implementation
  3. Each document content option listed in Table 3-4 Document Content Options should be supported by the implementation



## 2.0 REQUIREMENTS ANALYSIS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

**Table 2-1 Reader's Guide for Section 2.0**

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record

### 2.1 INTRODUCTION

Table 2-2 summarizes the system roles of the Capability. Section 2.2 identifies how these system roles participate in the set of information exchanges.

**Table 2-2 Capability System Roles**

System Role	System Role Definition
Alert Message Transmitter	The system which sends out the emergency message
Alert Message Receiver	The system which receives the emergency message

### 2.2 REQUIREMENTS

#### 2.2.1 INFORMATION EXCHANGES

Table 2-3 defines each of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA) or Exchange Content (EC) used.

**Table 2-3 Supported Information Exchanges**

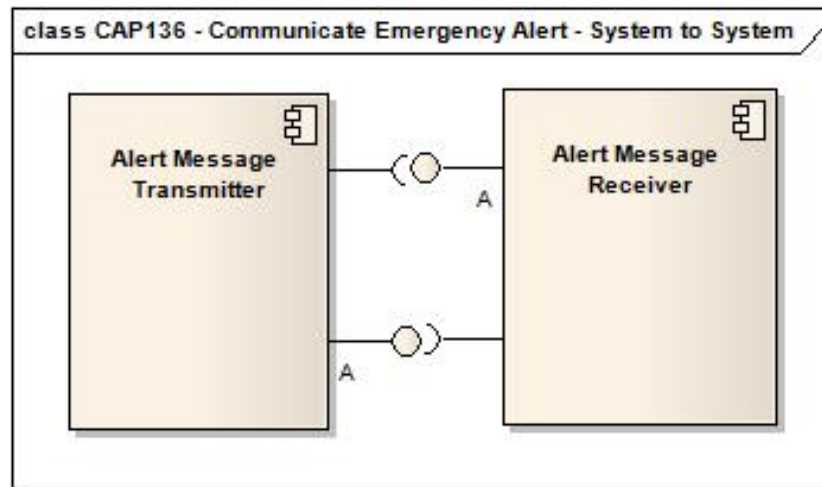
Information Exchange Identifier	Exchange Action	Exchange Content
A	Send	Emergency Alert

**Error! Reference source not found.** identifies how this Capability supports various system roles within multiple system architectures. For example, either an Electronic Health Record (EHR) system or a Health Information Exchange (HIE) might fill a document repository system role in an information exchange). In an implementation architecture, system roles may be combined locally (e.g., Hospital EHR System) and in others, the system roles may be provided by multiple-distributed trusted third parties (e.g., pharmacies within an HIE).





Figure 2-1 Information Exchanges Between System Roles



## 3.0 EXTERNAL CAPABILITY OPTIONS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

**Table 3-1 Reader's Guide for Section 3.0**

Document Section	Section Number	Intended Audience	Information Contained
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional Security and Privacy functions supported by the Capability

This section is primarily for architects, engineers and analysts. It allows those who consider using this Capability to evaluate and/or constrain the options that are externally made available for the Capability implementers.

Interoperability among system roles defined by this Capability often requires the selection of consistent options.

### 3.1 SECURITY AND PRIVACY

The application of Security and Privacy is highly influenced by the security and privacy policies. The HITSP Security and Privacy Technical Note (HITSP/TN900) provides a detailed discussion of the Security and Privacy constructs, including consideration and appropriate context for needed security and privacy related policy decisions. Security and Privacy constructs are integrated comprehensively into the Service Collaborations. The actual constructs used and the way in which the constructs are used is dependent on the policies and physical setting. Conformance claims are against the Security and Privacy constructs that are chosen to enforce the policies.



## 4.0 DESIGN SPECIFICATION

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

**Table 4-1 Reader's Guide for Section 4.0**

Document Section	Section Number	Intended Audience	Information Contained
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use

### 4.1 REQUIREMENTS MAPPED TO CONSTRUCTS

#### 4.1.1 CONSTRUCTS

Table 4-2 defines the mapping of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA), Exchange Content (EC) and any Constraints applied to the Information Exchange with specific initiating and/or responding system interfaces. This provides the traceability of constructs to the information exchanges identified in Section 2.0 above. Content modules and terminology Components are not listed here because they are referenced by other constructs, but do not provide an interface. HITSP/TN903 discusses how content modules and terminology Components are referenced by other constructs.

**Table 4-2 Information Exchanges Mapped to Constructs**

Information Exchange Identifier	Exchange Type	Construct Identifier	Description
A – Send Emergency Alert	Action	HITSP/SC116 – Emergency Message Distribution	The HITSP Emergency Message Distribution Service Collaboration performs a multicast notification to specifically identified populations, such as emergency departments
A – Send Emergency Alert	Content	HITSP/C82 – Emergency Common Alerting Protocol	The HITSP Emergency Common Alerting Protocol Component selects the OASIS Common Alerting Protocol (CAP) v1.1 standard, and is used as a multicast notification message sent to an identified channel. The intended recipients are populations such as "all emergency departments in XXX county", "within a geographic area", etc.

### 4.2 CONSTRAINTS AND ASSUMPTIONS

Table 4-3 specifies the context that must be provided in order to use the Capability, identifying any assumptions, pre-conditions, post-conditions, and triggers relevant for use of the Capability.



**Table 4-3 Context**

Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
Behavior and Policy of Public Safety Officer (PSO) is defined by jurisdiction	Assumption
Authorizations for capture of supplemental data are defined by jurisdiction	Assumption
The entity that needs to receive/file the report is determined by jurisdiction or domain policy agreements	Assumption
Trans-border communication expectations/specifications and mutual reporting are specified by policy	Assumption
Case count is not the priority/purpose here – goal is to manage/contain event not to produce a case count	Assumption
Assume that the perspective addresses both National and Local jurisdiction; Local PH jurisdiction perspective may differ from CDC perspective	Assumption
Policy considerations apply to exposure notifications and IRB/research authorization	Assumption
Jurisdiction or HIE Policy may impose information exchange restrictions for some of these communications if electronic	Assumption
Authentication service to authenticate requestors and/or data submissions from various locations	Pre-condition

### 4.3 SPECIFIED INTERFACES BY SYSTEM ROLE

This section specifies the HITSP Capability interfaces in terms of the System Roles identified in Table 2-2 Capability's System Roles.

Table 4-4 below specifies interfaces for the alert message transmitter system role as defined in Table 2-2.

**Table 4-4 Alert Message Transmitter System Role Mapped to HITSP Construct Interfaces**

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
N/A	Initiating	Send Message (HITSP/C82)	R
Send Emergency Message Distribution Element	Initiating	Emergency Message Distribution Element (HITSP/SC116)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-5 below specifies interfaces for the alert message receiver system role as defined in Table 2-2.

**Table 4-5 Alert Message Receiver System Role Mapped to HITSP Construct Interfaces**

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
N/A	Responding	Receive Message (HITSP/C82)	R
Receive Emergency Message Distribution Element	Responding	Emergency Message Distribution Element (HITSP/SC116)	R

Table 4-6 specifies optionality conditions referenced in Table 4-4 through Table 4-5 above.

**Table 4-6 Implementation Conditions**

Condition ID	Condition Description
None	



## 5.0 STANDARDS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

**Table 5-1 Reader's Guide for Section 5.0**

Document Section	Section Number	Intended Audience	Information Contained
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	List regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	5.2 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues

### 5.1 STANDARDS USED

#### 5.1.1 REGULATORY GUIDANCE

Table 5-2 lists any regulatory guidance that determines or constrains use of standards.

**Table 5-2 Regulatory Guidance**

Regulation	Description
No applicable regulatory guidance	

#### 5.1.2 SELECTED STANDARDS

Table 5-3 lists the standards selected as relevant to this Capability.

**Table 5-3 Selected Standards**

Standard	Description
American Medical Association (AMA) Current Procedural Terminology (CPT®) Fourth Edition (CPT-4); CPT Evaluation and Management Codes	This 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. For more information visit <a href="http://www.oasis-open.org">www.oasis-open.org</a>

#### 5.1.3 INFORMATIVE REFERENCE STANDARDS

Table 5-4 includes reference standards that inform the overall semantic interoperability.

**Table 5-4 Informative Reference Standards**

Standard	Description
No applicable informative reference standards	



## 5.2 STANDARDS GAPS AND OVERLAPS

Table 5-5 identifies the information exchange requirements and known standards gaps, along with the recommended resolutions to the gaps.

**Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps**

IER Gap Description	Responsible HITSP TC	Design Approach	Required Standards Now Unavailable for Constructs	SDO Working on Unavailable Standards	Expected Availability
None					

Table 5-6 lists any standards overlaps and describes plans to resolve each of the overlaps.

**Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps**

IER Number	Summary Description	Standard Overlap	Recommended Resolution
None			



## 6.0 APPENDIX

This section may include additional materials referenced throughout this document, such as requirements analysis tables and figures. If the Capability is yet to be implemented, it may contain the candidate standards for Tier 2 evaluations.

The following legacy Interoperability Specifications were used to derive this Capability:

- HITSP/IS04 – Emergency Responder Electronic Health Record
- HITSP/IS10 – Immunizations and Response Management
- HITSP/IS11 – Public Health Case Reporting



## 7.0 DOCUMENT UPDATES

The following sections provide the details of updates made to this document.

### 7.1 JANUARY 31, 2010

No changes. This is the first published version of the document.

