January 25, 2010
Version 1.0

HITSP Communicate Quality Measure Data Capability

HITSP/CAP130

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 Team	November 9, 2009
0.0.2	Review Copy	Selected Perspective, Domain and/or Tiger Team reviewers	January 18, 2010
1.0	Released for Implementation	Selected Perspective, Domain and/or Tiger Team reviewers	January 25, 2010

TABLE OF CONTENTS

FIGURES AND TABLES

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 for an EHR-compatible, standards-based quality measure. In the measure specification, needed patient encounter data elements are identified so they can

be extracted from local systems and from longitudinal data available through other sources such as a Health Information Exchange (HIE). The measure specification also includes various sets of exclusion/inclusion criteria to identify which patients to include in calculation of the measure. This Capability may use Value Set Sharing.

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

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
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
TN900 – Security and Privacy	TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs
TN903 – Data Architecture	TN903 is a reference document that provides the overall context for use of the HITSP Data Architecture constructs
TN904 – Harmonization Framework and Exchange Architecture	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 4-7 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
eMeasure Source	The system which sends or responds to requests for the eMeasure
eMeasure Consumer	The system which receives or initiates requests for eMeasure
Health Information Exchange	System providing infrastructure services supporting sharing of health information

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.

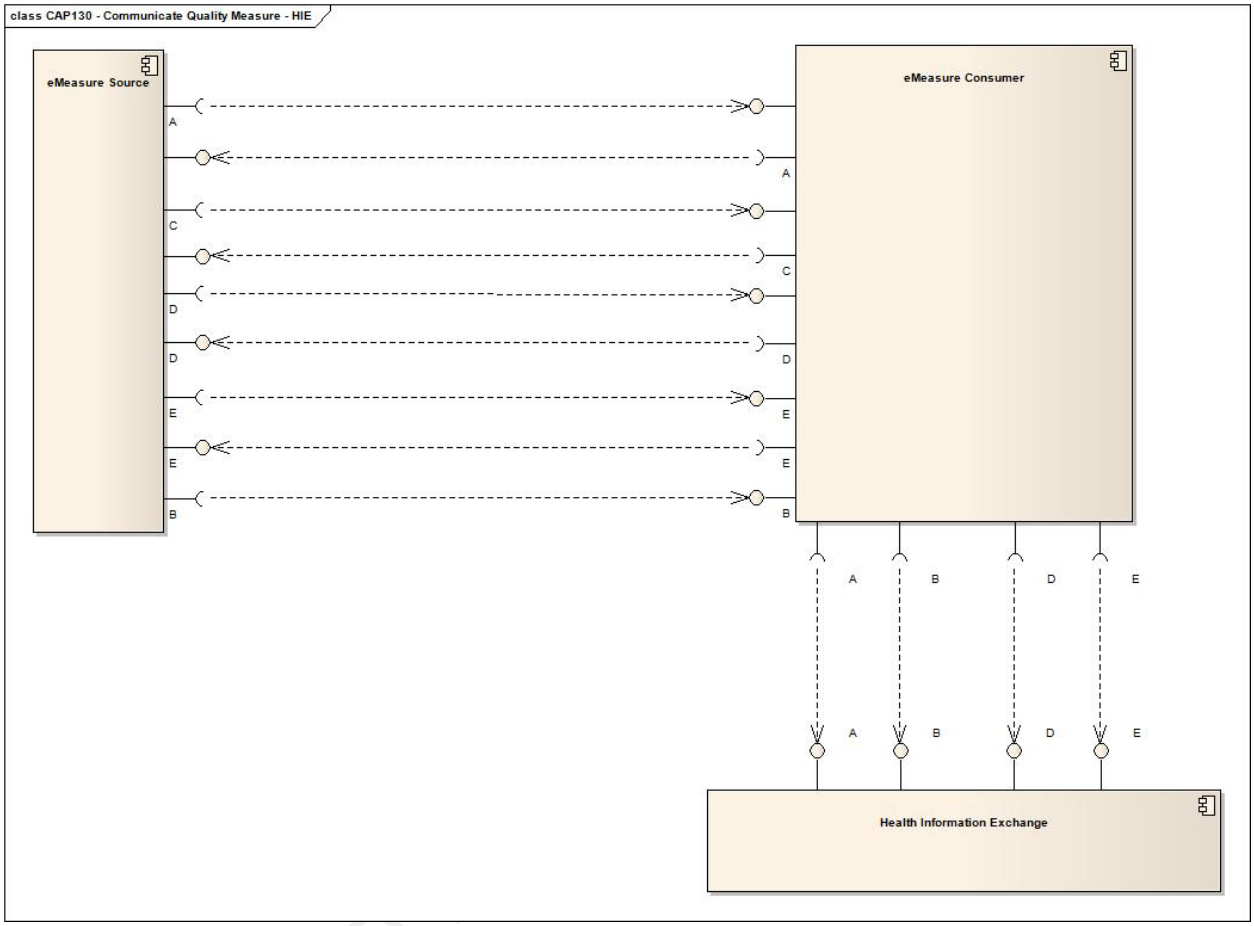
Table 2-3 Supported Information Exchanges

Information Exchange Identifier	Exchange Action	Exchange Content
A	Request & Respond	Measurement Criteria plus Knowledge and Vocabulary
B	Send	Measurement Criteria
C	Request & Respond	Nonrepudiation
D	Request & Respond	Access Control
E	Request & Respond	Knowledge and Vocabulary

Figure 2-1 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 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 – Request and Respond Measurement Criteria/Knowledge and Vocabulary	Action	HITSP/SC111 - Knowledge and Vocabulary	The HITSP Knowledge and Vocabulary Service Collaboration provides the ability to retrieve medical knowledge and terminology
	Content	HITSP/C106 - Measurement Criteria Document	This Component supports communication of a quality measure (aka an "eMeasure"). Clinical concepts (e.g. "atrial fibrillation", "coronary artery disease") and parameters (e.g. "numerator", "denominator") in an eMeasure are formally defined to support consistent and unambiguous interpretation. The eMeasure is standardized as a structured document, where one can capture the complete narrative of the measure and a formalized computable representation of statements
B - Send Measurement Criteria	Action	HITSP/SC111 - Knowledge and Vocabulary	The HITSP Knowledge and Vocabulary Service Collaboration provides the ability to retrieve medical knowledge and terminology

Information Exchange Identifier	Exchange Type	Construct Identifier	Description
	Content	HITSP/C106 - Measurement Criteria Document	This Component supports communication of a quality measure (aka an "eMeasure"). Clinical concepts (e.g. "atrial fibrillation", "coronary artery disease") and parameters (e.g. "numerator", "denominator") in an eMeasure are formally defined to support consistent and unambiguous interpretation. The eMeasure is standardized as a structured document, where one can capture the complete narrative of the measure and a formalized computable representation of statements
C – Request and Respond Nonrepudiation of Origin	Action	HITSP/SC111 - Knowledge and Vocabulary	The HITSP Knowledge and Vocabulary Service Collaboration provides the ability to retrieve medical knowledge and terminology
	Content	HITSP/C26 - Nonrepudiation of Origin	The Nonrepudiation of Origin Component provides the mechanisms to support Nonrepudiation of Origin, which refers to both the proof of the integrity and origin of documents in a high-assurance manner, which can be verified by any party. This Component does not provide Nonrepudiation of Receipt Nonrepudiation allows the recipient to be sure it is the right measure, and the measure is unchanged
D – Request and Respond Access Control	Action and Content	HITSP/SC108 - Access Control	The HITSP Access Control Service Collaboration provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives Some measures may require licensing, and may require access control
E – Request and Respond Knowledge and Vocabulary	Action	HITSP/SC111 - Knowledge and Vocabulary	The HITSP Knowledge and Vocabulary Service Collaboration provides the ability to retrieve medical knowledge and terminology

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
New measure or updated measure is ready to be communicated – to publish, record, send, or review	Trigger
Quality measures are provided with sufficient specification that they are well-defined and unambiguous.	Assumptions

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 first system role as defined in Table 2-2.

Table 4-4 eMeasure Source System Role Mapped to HITSP Construct Interfaces

Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Request Access Control Decision	Initiating	Access Control (HITSP/SC108)	C130[101]
Respond to Medical Knowledge	Responding	Knowledge and Vocabulary (HITSP/SC111)	R
		Measurement Criteria (HITSP/C106)	R
		Nonrepudiation of Origin (HITSP/C26)	C130[201]

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

Table 4-5 specifies interfaces for responding system roles as defined in Table 2-2.

Table 4-5 eMeasure Consumer System Role Mapped to HITSP Construct Interfaces

Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Request Medical Knowledge	Initiating	Knowledge and Vocabulary (HITSP/SC111)	C[102]

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

Table 4-6 specifies interfaces for initiating gateway system roles as defined in Table 2-2.

Table 4-6 Health Information Exchange System Role Mapped to HITSP Construct Interfaces

Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Request Access Control Decision	Responding	Access Control (HITSP/SC108)	C[101]
Request Medical Knowledge	Responding	Knowledge and Vocabulary (HITSP/SC111)	C[102]
		Measurement Criteria (HITSP/C106)	R
		Nonrepudiation of Origin (HITSP/C26)	C[201]

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

Table 4-7 specifies optionality conditions referenced in Table 4-4 through Table 4-6 above.

Table 4-7 Implementation Conditions

Condition ID	Condition Description
C[101]	Where access control required by policy
C[102]	This may be optionally used to deliver HITSP/C106 content. Other ways of transmitting HITSP/C106 are permissible (e.g. eMail) as this is not patient-specific content
C[201]	Shall be applied where nonrepudiation required by policy

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
Health Level Seven (HL7) eMeasure: Representation of quality measures in the Health Quality Measures Format (HQMF), Release 1 (Draft Standard for Trial Use)	The HL7 HQMF Standard is a formalism for encoding quality measures (aka creating eMeasures). The HL7 HQMF Standard is part of the HL7 Version 3.0 family of standards, based on a Reference Information Model (RIM). Visit www.hl7.org for more information
American Society for Testing and Materials (ASTM International) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	Defines a document structure for use by electronic signature mechanisms, describes the characteristics of an electronic signature process. Defines minimum requirements for different electronic signature mechanisms, defines signature attributes for use with electronic signature mechanisms, describes acceptable electronic signature mechanisms and technologies, defines minimum requirements for user identification, access control, and other security requirements for electronic signatures, and outlines technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism. For more information visit www.astm.org
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	Extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of nonrepudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European Directive. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with this document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. For more information visit www.etsi.org

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 6.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile, Section 9.1 Authentication	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Health Level Seven (HL7) Common Terminology Services (CTS) Release 1	The HL7 Common Terminology Services (HL7 CTS) defines an Application Programming Interface (API) that can be used when accessing terminological content. The CTS specification was developed as an alternative to a common data structure. Instead of specifying what an external terminology must look like, HL7 has chosen to identify the common functional characteristics that an external terminology must be able to provide. As an example, an HL7 compliant terminology service will need to be able to determine whether a given concept code is valid within the particular resource. Instead of describing a table keyed by the resource identifier and concept code, the CTS specification describes an Application Programming Interface (API) call that takes a resource identifier and concept code as input and returns a true/false value. Each terminology developer is free to implement this API call in whatever way is most appropriate or them. It describes a set of API calls that represent the core functionality that will be needed by basic HL7 Version 3 applications. For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2008-2009 Sharing Value Sets (SVS) Integration Profile	The Sharing Value Sets (SVS) Integration Profile provides a means through which healthcare systems producing clinical or administrative data, such as diagnostic imaging equipment, laboratory reporting systems, primary care physician office EMR systems, or national healthcare record systems, can receive a common, uniform nomenclature managed centrally. Shared nomenclatures are essential to achieving semantic interoperability. For more information visit www.ihe.net
Health Level Seven (HL7) Version 3.0 Context-Aware Information Retrieval Specification: URL Implementation Guide	Informative Implementation Guide for URL-based implementations of the context-aware information retrieval (“Infobutton”) The goal of this infobutton Implementation Guide is to recommend a URL-based implementation of the context-aware information retrieval ('infobutton') domain. The intent is to provide a simple way to implement infobuttons that is compatible with the current state of the market in this area. Most infobutton implementations to date, especially on the side of on-line information resources, rely on URL-based APIs. For more information visit www.hl7.org
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
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	Description
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security 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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 6.0, 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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 6.0 - 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 6.0 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
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	Description
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

The HL7 HQMF, Release 1 DSTU is included in this Component as Intended for Use, and it is anticipated that the standard, while ballot approved, will not be available as a published Draft Standard For Trial Use (DSTU) before the end of the First quarter of 2010. Once the standard is released, this Component will be updated to align with the final DSTU version and the status of the standard is expected to be changed from 'Intended for Use' to 'Selected' within HITSP.

Rather than include a snapshot of the evolving HL7 HQMF, Release 1 DSTU, this Component references the latest draft at: [http://wiki.hl7.org/index.php?title=HQMF%20 (userid: "wiki", password: "wikiwiki")]. Note that draft documentation is subject to change as part of the HL7 Comment Resolution process, and may be updated or replaced by a revised draft at any time.

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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 6.0	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
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

Standard	Description
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

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
6.1.8, 7.1.8	Transmit patient level quality information	Discipline-recognized point-of-care user interface terminologies	Discipline-recognized point-of-care user interface terminologies may be used for end systems. Harmonization of these terminologies is needed and should be accelerated SNOMED CT to be used for interoperability transactions
6.1.8, 7.1.8	Transmit patient level quality information	Role term is used in various standards differently.	Refer to SDOs for harmonization
6.1.1, 7.1.1	Receive listing of defined measures & abstraction guidelines	Arden Syntax, GLIF, GELLO, OWL, ISO Common Logic	Refer for evaluation and harmonization
6.1.5, 7.1.5	6.1.5 Augment EHR data with manual extraction of patient data (may also occur prior to discharge) 7.1.5 Merge administrative data with EHR data and manual extraction of patient data	UN Standard product and services code – Coalition for healthcare e-standards; overlaps with LOINC possible	Pending further review

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.

Legacy Interoperability Specifications were used to derive this Capability.

- HITSP/IS06 Quality

7.0 DOCUMENT UPDATES

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

7.1 NOVEMBER 9, 2009

This is the first published version of the document

7.2 JANUARY 18, 2010

Changes reflect the new HITSP Capability Template 2.3 and the disposition of Public Comments by the Population Perspective Technical Committee.

7.3 JANUARY 25, 2010

Upon approval by the HITSP Panel on January 25, 2010, this document is now Released for Implementation.