

HITSP Common Data Transport Technical Note

HITSP/TN907



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security and Privacy Domain Technical Committee



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
0.0.1	Review Copy	Security and Privacy Domain Technical Committee	January 31, 2010



TABLE OF CONTENTS

1.0	INTRODUCTION.....	6
1.1	Overview	6
1.2	Relationship to HITSP Work Products.....	6
1.3	Relationship to NHIN Specifications	6
1.4	Copyright Permissions	7
1.5	References	7
2.0	SCOPE	8
2.1	Interoperability	8
2.2	OSI Layers and Technology Stack	8
2.3	Types of Data	9
2.4	Interfaces and Applicable Organizations	9
2.5	Constraints	9
3.0	FUNCTIONAL REQUIREMENTS.....	11
3.1	Web Services	11
3.1.1	Selecting Web Services.....	11
3.1.2	HITSP Selection of Web Services.....	12
3.2	Supported Interactions.....	13
3.2.1	Query-Retrieve.....	13
3.2.2	Distributed Query	14
3.2.3	Publish-Subscribe	15
3.2.4	Notify-Retrieve	16
3.2.5	Unsolicited Delivery.....	17
3.2.6	HITSP and NHIN Mappings.....	18
3.2.7	Gaps and Recommendations	18
3.3	Security Attributes.....	19
3.3.1	Multiple Trust Frameworks	19
3.3.2	Confidentiality.....	20
3.3.3	Message Authentication and Integrity	20
3.3.4	Entity Authentication.....	20
3.3.5	Authorization	20
3.3.6	HITSP and NHIN Mappings.....	21
3.3.7	Gaps and Recommendations	21
3.4	Message Enclosure	22
3.4.1	Envelope Metadata	23
3.4.2	Addressing and Routing	23
3.4.3	Multiple Types of Content.....	23
3.4.4	HITSP and NHIN Mappings.....	23
3.4.5	Gaps and Recommendations	24
3.5	Discovery and Routing.....	24
3.5.1	Organizational Search and Discovery	24
3.5.2	Service Invocation Metadata.....	25
3.5.3	Message Routing	25
3.5.4	Multi-Hop Message Routing	26
3.5.5	Multiple Recipients	26
3.5.6	Discovery and Routing – Additional Scope Considerations	27
3.5.7	HITSP and NHIN Mappings.....	27
3.5.8	Gaps and Recommendations	28
3.6	Reliable Messaging.....	28



3.6.1	Multiple Delivery	28
3.6.2	Fault Notification	28
3.6.3	HITSP and NHIN Mappings.....	29
3.6.4	Gaps and Recommendations	29
4.0	NON-FUNCTIONAL REQUIREMENTS.....	30
4.1	Scalability	30
4.2	Extensibility	30
4.3	Platform Independence.....	30
4.4	Coherence	30
5.0	GAPS AND RECOMMENDATION SUMMARY	31
6.0	DOCUMENT UPDATES.....	32
6.1	January 31, 2010.....	32



FIGURES AND TABLES

Figure 2-1 Topology as Shown in HITSP/SC112 Healthcare Document Management	8
Figure 2-2 ISO Open Systems Interconnection Layers	9
Figure 3-1 Query Retrieve	14
Figure 3-2 Distributed Query.....	15
Figure 3-3 Publish Subscribe.....	16
Figure 3-4 Notify Retrieve	17
Figure 3-5 Unsolicited Delivery	18
Figure 3-6 Message Enclosure	22
Table 1-1 Reference Documents	7
Table 2-1 Constraints Identified within Common Data Transport Gap/Extensions Document.....	9
Table 3-1 SOAP/REST Web Service Functionality	12
Table 3-2 HITSP Constructs Built on Web Services	12
Table 3-3 HITSP and NHIN Mappings – Supported Interactions.....	18
Table 3-4 Gaps and Recommendations – Supported Interactions	18
Table 3-5 HITSP and NHIN Mappings – Security Attributes	21
Table 3-6 Gaps and Recommendations – Security Attributes.....	21
Table 3-7 HITSP and NHIN Mappings – Envelope Enclosure.....	24
Table 3-8 Gaps and Recommendations – Envelope Enclosure	24
Table 3-9 Discovery and Routing Standards	24
Table 3-10 Service Invocation Metadata Standards	25
Table 3-11 Message Routing Standards	25
Table 3-12 Multi-Hop Message Routing Standards	26
Table 3-13 HITSP and NHIN Mappings – Discovery and Routing.....	27
Table 3-14 Gaps and Recommendations – Discovery and Routing	28
Table 3-15 HITSP and NHIN Mappings – Reliable Messaging	29
Table 3-16 Gaps and Recommendations – Reliable Messaging.....	29
Table 5-1 Gaps and Recommendations – Summary	31



1.0 INTRODUCTION

This section provides a high level overview of the Healthcare Information Technology Standards Panel (HITSP) Common Data Transport (CDT) Technical Note, 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 Scope.

1.1 OVERVIEW

The Common Data Transport Technical Note provides guidance on how HITSP does and/or will provide support for the requirements identified in the Common Data Transport Office of the National Coordinator (ONC) Gap/Extension document. These requirements do not exist in a vacuum; therefore HITSP has gone to considerable lengths to clarify the requirements' scope (see Section 2.0) and context. HITSP has also recognized that while the scope of CDT goes well beyond applicability in the National Health Information Network (NHIN), it is highly desirable that HITSP and NHIN come to convergence in the area of CDT and that there should not be any inessential inconsistencies. HITSP also has examined the a Interim Final Rule (IFR) for the "Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology", published by the U.S. Department of Health and Human Services on December 30, 2009; the content of this Technical Note appears to be consistent in letter and in spirit with the IFR.

What does "common" mean? Our view of the term "common" in "Common Data Transport" is that given a set of specific requirements for the transport of data, there should be no unnecessary divergence from a common solution, and a common approach should be taken regardless of the content of the data transported. For example, if the communication of a specific type of clinical information has the same requirements as communication of administrative data, they should use the same common mechanisms. We specifically do not mean "singular". That is, we do not require a single mechanism be used in all contexts regardless of need. Such a "singular" approach would require that the most complex scenario for data transport dictate an approach for all types of transport.

The main body of this document is Section 3.0 where each requirement has been abstracted from the ONC Gap/Extension document. Each subsection is devoted to a separate set of requirements where the mapping to functional Capabilities in HITSP and NHIN are described. Finally, any current gaps or inconsistencies and a recommended approach for addressing them, is noted. In some circumstances, a specific requirement is fulfilled by generic information technology standards that are not unique to healthcare. Where such standards exist and do not need further constraints to enable interoperability, the standard is identified as such.

Finally, gaps and recommendations are consolidated in Section 4.0. As new constructs are developed to address these gaps and inconsistencies HITSP will update its master list of gaps. Subsequently this document will be updated to reflect those changes. Because additional constructs need to be developed this Technical Note should be viewed as an intermediate work product and not the completion of HITSP's work on Common Data Transport.

1.2 RELATIONSHIP TO HITSP WORK PRODUCTS

This is a Technical Note. It differs from HITSP constructs (Components, Transactions, Transaction Packages, Service Collaborations, and Capabilities) in that it is not a specification for interoperability; it is informative. This document references appropriate HITSP constructs that fulfill CDT functional requirements.

1.3 RELATIONSHIP TO NHIN SPECIFICATIONS

NHIN leverages HITSP constructs, but HITSP has constructs that are not used by NHIN because they are beyond its scope. Similarly, NHIN has architectural features that go beyond the scope of standards



harmonization covered by HITSP. Where HITSP and NHIN overlap in functional capabilities it is desirable that HITSP and NHIN not unnecessarily diverge.

1.4 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.

1.5 REFERENCES

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

Table 1-1 Reference Documents

Reference Document	Document Description
Common Data Transport ONC Extension/Gap, May 4, 2009	Documents the background and requirements for "Common Data Transport"
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	Provides an overview of Security and Privacy constructs
TN904 – Harmonization Framework and Exchange Architecture	Describes the current framework within which the Interoperability Specifications are built
NHIN Specifications	NHIN Specifications, including Access Consent Policies V0.4, Authorization Framework V2.2, Geocoded Interoperable Population Summary Exchange V1.0, Health Information Event Messaging (HIEM) Profile V1.5, HIEM Profile Framework V1.2, Messaging Platform Specification V1.9.8, Patient Discovery V 0.9, Query for Documents V1.6.15, Retrieve Documents V1.6.10, and Services Registry Specification V1.3
Interim Final Rule (IFR) for the Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology	Specifies the standards and technology required by HIT systems in order to be certified as Electronic Health Record (EHR) systems for the purpose of qualification under the Medicare and Medicaid EHR Incentive Programs.
ISO Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model	A description of the Open Systems Interconnection (OSI) model for computer networks



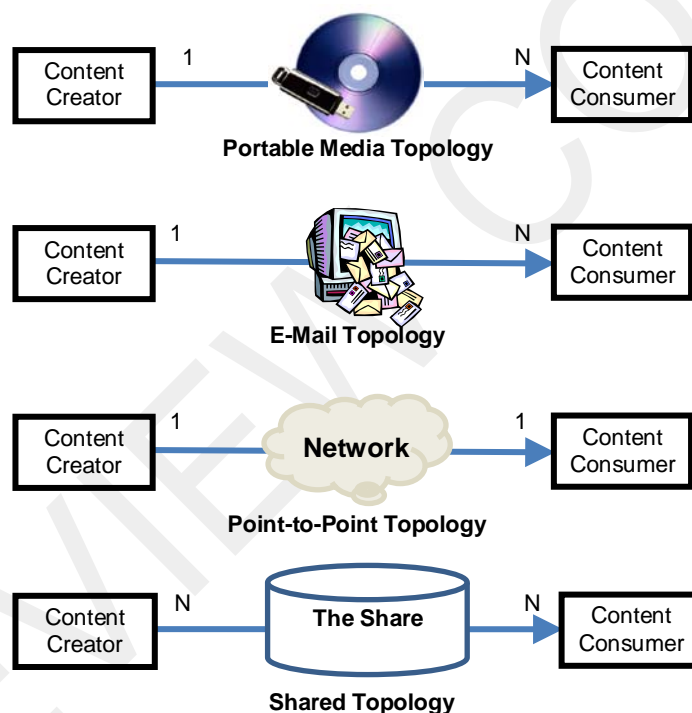
2.0 SCOPE

In the ONC Common Data Transport Gap/Extension document, a detailed description of scope is provided. This section provides HITSP's perspective on that scope. In particular, the scope is defined in terms of attributes such as the network layers within an OSI model, the types of data transports to be supported, the interfaces and their interactions.

2.1 INTEROPERABILITY

The interoperability scope is Business to Business (B2B) transport of health IT data over the Public Internet. Figure 2-1 illustrates the basic topologies supported, such as Portable Media, E-Mail, Point-to-Point and Shared Topology's within a Health Information Exchange (HIE), that is, an exchange of health information.

Figure 2-1 Topology as Shown in HITSP/SC112 Healthcare Document Management



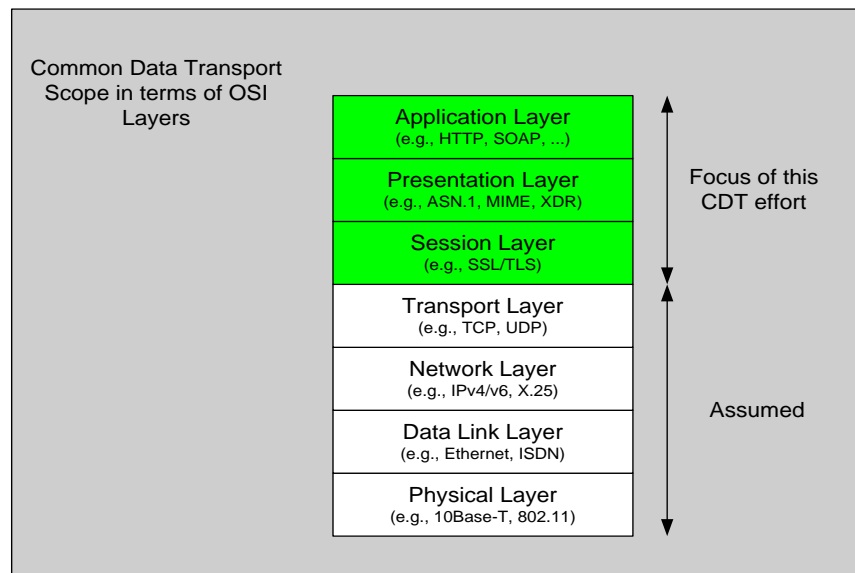
In Figure 2-1 the Point-to-Point and Shared Topologies are in scope for Common Data Transport, including single-hop point-to-point connections and multi-hop or end-to-end.

2.2 OSI LAYERS AND TECHNOLOGY STACK

The [OSI model](#) is commonly used to describe the network layers that are in scope. As shown in the diagram below, the Common Data Transport effort will be focused on the top three (Application, Presentation and Session) OSI layers. Lower layers are assumed (public Internet).



Figure 2-2 ISO Open Systems Interconnection Layers



2.3 TYPES OF DATA

The scope includes the transport of healthcare data and related information, including clinical or public health data, administrative data, emergency response data that involve complex payloads (e.g., HL7, X12, NCPDP, DICOM, EDXL/CAP), and typically require high levels of security and interoperability.

The following types of transport/interactions are assumed, hence will not be the focus of Common Data Transport:

- Electronic mail (SMTP)
- Time synchronization data (e.g., NTP)
- White page information (e.g., LDAP)
- Domain name lookups (e.g., DNS)

2.4 INTERFACES AND APPLICABLE ORGANIZATIONS

Since Common Data Transport is primarily targeted at the healthcare domain, organizations that generate, distribute or use health related information are the interfaces. This may include but is not limited to healthcare providers, labs, public health, pharmacies, emergency responders, health plans, Personal Health Record (PHR) Systems, Electronic Health Record (EHR) Systems, Health Information Organizations (HIOs) and Clearinghouses.

2.5 CONSTRAINTS

The following constraints have been identified either within the Common Data Transport Gap/Extension document or during discussions within HITSP Security, Privacy and Infrastructure Technical Committee.

Table 2-1 Constraints Identified within Common Data Transport Gap/Extensions Document

Item	Constraint	Source
1	Select a standards stack that has support for most requirements, avoids using mix and match from multiple stacks, is aligned with NHIN but supports non-NHIN Use Cases	Common Data Transport Gap/Extension Document
2	Standards selected must support end-points that have only a Client capability (using push/pull capability)	Common Data Transport Gap/Extension Document



Item	Constraint	Source
3	Standards selected must support end-to-end security (in a multi-hop scenario)	Common Data Transport Gap/Extension Document
4	Use HTTP with mutually authenticated TLS (HITSP/T17-Secured Communication Channel) as underlying transport level security	HITSP Security, Privacy and Infrastructure Technical Committee Discussions



3.0 FUNCTIONAL REQUIREMENTS

HITSP has abstracted and condensed the functional requirements from the ONC Common Data Transport Gap/Extension document. Each subsection is devoted to a separate set of requirements where the mapping to functional capabilities in HITSP and NHIN are described. Finally, any current gaps or inconsistencies and a suggested approach for addressing them, is noted. In some circumstances, a specific requirement is fulfilled by generic information technology standards that are not unique to healthcare. Where such standards exist and do not need further constraints to enable interoperability, the standard is identified as such.

3.1 WEB SERVICES

A Web Service is traditionally defined by the W3C as "a software system designed to support interoperable machine-to-machine interaction over a network. In common usage, the term refers to clients and servers that communicate over the HyperText Transfer Protocol (HTTP) protocol. Such services tend to fall into one of two camps: SOAP Web Services and RESTful Web Services. However, this is an evolving field with emerging entrants that may be lighter-weight and better suited to certain exchange ecosystems. For this reason, requirements around transport protocols should be kept minimal as long as considerations, such as security and ability to convey data content, are supported.

SOAP Web Services use Extensible Markup Language (XML) messages that follow the Simple Object Access Protocol (SOAP) standard and have been popular with traditional enterprise. In such systems, there is often a machine-readable description of the operations offered by the service written in the Web Services Description Language (WSDL). Some industry organizations, such as the WS-I, mandate both SOAP and WSDL in their definition of a web service.

More recently, REpresentational State Transfer (RESTful) Web Services have been regaining popularity. RESTful Web Services leverage more completely the HTTP protocol including: negotiations for media types, caching, authentication, and the HTTP methods as the verbs: PUT (replace or update), GET (list or retrieve), POST (create), and DELETE (delete). Unlike SOAP-based Web Services, there is no "official" standard for RESTful Web Service. This is because REST is an architecture, unlike SOAP, which is a protocol. Even though REST is not a standard, a RESTful implementation such as the Web can use standards like HTTP, URL, XML, GIF, etc.

In specifying a Web Service, the exposed service functional capability is specified without regard to a specific interface signature, transport binding or security requirements. There are many situations where it is desirable to expose a service functional capability through both a SOAP-enabled endpoint and RESTful endpoint, exploiting the strengths of each approach to meet the needs of different service consumers.

3.1.1 SELECTING WEB SERVICES

SOAP Web Services and RESTful Web Services are both very useful tools that have advantages and disadvantages. When defining a concrete implementation of a service it is important to pick the best tool for the specific job. The Common Data Transport Technical Note outlines some of these attributes that a transport may need to have. Not all of these attributes are always needed, so it is important to use the simplest tool that can get the job done.

Where the advantages of SOAP are necessary to meet the transaction requirements, then a SOAP Web Service should be chosen. There are times when the requirements allow for a transport with specifications for both REST and SOAP. For example HITSP/T89 Sharing Imaging Results supports both REST and SOAP based transports in addition to the non-web-services transport specified in DICOM. In cases where multiple transport architectures are available, policy and implementation will need to aid with interoperability.



Table 3-1 SOAP/REST Web Service Functionality

Web Service Functionality	SOAP	REST
Web-Application deployment	Supports	Best – more easily integrated into a browser experience
Cross-Organization Interoperability	Best – more formal definition with built in support for many capabilities including end-to-end security and federated user identity	Supports
User authentication	Best support for User Assertions – Federated Identity	Leverages Browser for user authentication
Server Authentication	Secured using TLS, server or mutual authenticated	Secured using TLS, server or mutual authenticated
End-to-End security	Supports end-to-end security with WS-Security	No support
Intermediary support	Best – WS-Addressing	Minimal support for composition
Synchronous	Yes	Yes
Asynchronous	Yes	No
Interface Definition	Well-formed interface definition protocol (WSDL)	No formal method
Interface Versioning	Built in to WSDL	No formal method
Support for Reliable Messaging	Built in to WS-Reliable Messaging	No
Support for Binary attachments	Built in using MTOM	No
Support for multiple attachments	Built in using MTOM	No
Programming ease	Need to leverage available toolkits	Less need for a toolkit
Deployment ease	Automated with UDDI hosting of WSDL	Republish hosting web page
HTTP header negotiations	Not used	Most HTTP header negotiations leveraged
Commands	If the limited REST command set is not sufficient then use SOAP	Fixed Set: PUT (replace or update), GET (list or retrieve), POST (create), and DELETE

3.1.2 HITSP SELECTION OF WEB SERVICES

HITSP has selected standards that are built on Web Services in many cases. The selection used the HITSP Tier-2 criteria, a formal analysis of how well the requirements are met by potential standards. One of the criteria is fitness to the requirements. The following table shows the current HITSP constructs that are built on Web Services, both RESTful and SOAP. The table is provided to show how HITSP has used the differences between REST and SOAP during the selection. For example, in the case of HITSP/TP89 Sharing Imaging Results multiple transports are offered supporting both REST and SOAP. The other constructs have only one Web Services architectural choice at this time. The table below Reason for Selection column contains a description of a retrospective on some of the Web Services functionality that was included as part of the HITSP selection:

Table 3-2 HITSP Constructs Built on Web Services

HITSP Constructs	NHIN	Web Service	Reason for Selection
HITSP/T18 – View Laboratory Result from a Web Application		REST	Browser based user interface for viewing a lab result
HITSP/TP50 – Retrieve Form for Data Capture		REST & SOAP	Browser based form (html and x-forms) based workflows used to present a form with submission of the resulting form data
HITSP/T66 – Retrieve Value Set		REST & SOAP	Retrieval of vocabulary tables with no personal data
HITSP/T81 – Retrieval of Medical Knowledge		REST	Request for a HTML page that describes the given healthcare values, non personally identifiable
HITSP/TP89 – Sharing Imaging Results		REST & SOAP	Both are selected (as well as DICOM) to allow policy to choose the 'best'. Retrieval of an image by OID
HITSP/TP13 – Manage Sharing of Documents	Yes	SOAP	Comprehensive set of document management actions, complex queries, highly patient identifiable, multiple attachments, metadata relationships between documents, structured and coded metadata
HITSP/TP21 – Query for Existing Data		SOAP	Highly patient identifiable, XML response
HITSP/TP31 – Document Reliable Messaging	Yes	SOAP	Highly patient identifiable, multiple attachments, metadata relationships, action codes --- (Simplified use of one of the HITSP/TP13 transactions)



HITSP Constructs	NHIN	Web Service	Reason for Selection
HITSP/T63 – Emergency Message Distribution Element		SOAP	Unidirectional messaging, need for message routing to many endpoints
HITSP/T85 – Administrative Transport to Health Plan		SOAP	Highly patient identifiable, multiple attachments

3.2 SUPPORTED INTERACTIONS

The following diagrams illustrate the desired information exchange patterns. The stick figures represent the interfaces in the information exchange. An interface is a categorization of the role a system plays in an information exchange. The diagrams utilize the following interfaces:

- Information consumer: this role receives the information provided by the information supplier
- Information supplier: this role supplies the information to the information consumer role
- Query distributor: this role receives a query from an information consumer role and forwards it to multiple information suppliers so that they can respond to the query

3.2.1 QUERY-RETRIEVE

Initiated by a requestor, who specifies the desired information and provides necessary authorizations, one organization acts as a requestor of information and the other acts as a supplier. The requestor identifies the desired information and provides the necessary authorizations and credentials in the query. The supplying organization evaluates the request, confirms the requestor's credentials, adjudicates the request against known consumer preferences and associated local policies and permissions, and responds accordingly. Messaging processes should support both synchronous and asynchronous (requestor does not wait, and supplier responds subsequently) implementations of this pattern. A sequence diagram for this interaction can be seen in Figure 3-1.



Figure 3-1 Query Retrieve

information exchange pattern
requestor initiated information exchange category
query - retrieve pattern
UML sequence diagram

Legend:
The arrow head indicates the direction of information flow.
A broken line indicates a response.

3.2.2 DISTRIBUTED QUERY

Initiated by a requestor, who specifies the desired information and provides necessary authorizations, one organization acts as a requestor of information and the other acts as a supplier. One organization acts as the requestor of information, initiating the request to multiple supplier organizations. The request may identify specific data supplier organizations, or alternatively, may include attributes of potential supplier organizations which would be interpreted and applied by the various networks which process the distributed query. The supplying organization(s) evaluates the request, confirms the requestor's credentials, adjudicates the request against available consumer preferences, and responds accordingly. Messaging processes should support both synchronous (requestor waits until supplier responds) and asynchronous (requestor does not wait, and supplier responds subsequently) implementations of this pattern. A sequence diagram for this interaction can be seen in Figure 3-2.



Figure 3-2 Distributed Query

information exchange pattern
requestor initiated information exchange category
distributed query pattern
UML sequence diagram

Legend:
The arrow head indicates the direction of information flow.
A broken line indicates a response.

3.2.3 PUBLISH-SUBSCRIBE

The data supplier initiates the delivery to one or more recipients. This may be initiated using electronic transactions between the data supplier and recipient (publish-subscribe), or may be based on agreed-upon business processes, policies, or regulatory requirements. The requestor subscribes for information from a supplier for some period of time. The information requested is articulated as a set of criteria, or topics, that are of interest to the subscriber. It is the supplier's responsibility to determine on an ongoing basis whether they have new or updated information that conforms to the subscription criteria, and if so, to send the information to the subscriber(s). The requestor's subscription request includes the necessary credentials for access to the requested information, which are evaluated by the data supplier at each occurrence of data delivery. A sequence diagram for this interaction can be seen in Figure 3-3.



Figure 3-3 Publish Subscribe

information exchange pattern
supplier initiated information exchange category
publish - subscribe pattern
UML sequence diagram

Legend:

The arrow head indicates the direction of information flow.
A broken line indicates a response.

3.2.4 NOTIFY-RETRIEVE

The data supplier initiates the delivery to one or more recipients. This may be initiated using electronic transactions between the data supplier and recipient (publish-subscribe), or may be based on agreed-upon business processes, policies, or regulatory requirements. The supplier notifies the recipient of the availability of information, without disclosing the content, or attributes of the information. The recipient then retrieves the available information using the query/retrieve pattern which may incorporate data location pointers provided in the notification. The retrieval portion of this pattern may be initiated by the individual person who receives the notification, or by automated retrieval processes operated by the recipient's systems. This process allows the supplier to confirm the current credentials of the recipient before delivering the information. A sequence diagram for this interaction can be seen in Figure 3-4.



Figure 3-4 Notify Retrieve

information exchange pattern
supplier initiated information exchange category
notify - retrieve pattern
UML sequence diagram

Legend:
The arrow head indicates the direction of information flow.
A broken line indicates a response.

3.2.5 UNSOLICITED DELIVERY

The data supplier initiates the delivery to one or more recipients. This may be initiated using electronic transactions between the data supplier and recipient (publish-subscribe), or may be based on agreed-upon business processes, policies, or regulatory requirements. Information is sent from a supplier to a recipient without having received a direct prior request for the information from the recipient. (e.g., delivery of public health case reports). Due to the unique challenges of ensuring that the recipient is authorized to receive the information and confirming the recipient's electronic address, this pattern may be applicable in specialized situations where the recipient's authorization is defined by business agreements, policy or regulatory requirements. There may be situations where the intent of this pattern can be accomplished using the publish-subscribe pattern or notify-retrieve pattern to implement a persistent information delivery relationship between the supplier and recipient. A sequence diagram for this interaction can be seen in Figure 3-5.



Figure 3-5 Unsolicited Delivery

information exchange pattern
 supplier initiated information exchange category
 unsolicited delivery pattern
 UML sequence diagram

Legend:
 The arrow head indicates the direction of information flow.
 A broken line indicates a response.

3.2.6 HITSP AND NHIN MAPPINGS

Table 3-3 summarizes the mapping between each of the individual supported interaction requirements and the relevant HITSP constructs and NHIN specifications, as discussed in the previous sections.

Table 3-3 HITSP and NHIN Mappings – Supported Interactions

Requirement	HITSP Constructs	NHIN Specifications
Query-Retrieve	HITSP/TP13 – Managing Sharing of Documents	Addressed by Query for Documents and Retrieve Document specifications, including dynamic/deferred documents
Distributed Query	HITSP/TP13 can be depending on the Harmonization Request	No specification to support distributed query, but any application or gateway can perform distributed query. This makes use of the Query for Documents specification
Publish-Subscribe	HITSP/TP13 has recently incorporated Integrating the Healthcare Enterprise (IHE) Document Metadata subscription (DSUB) for a specific use	Addressed by Health Information Event Messaging (HIEM) specification
Notify-Retrieve	HITSP/TP13 has recently incorporated IHE DSUB for a specific use	Addressed by Health Information Event Messaging (HIEM) specification
Unsolicited Delivery	HITSP/T31 – Document Reliable Exchange, or HITSP/TP13 with HITSP/T29 – Notification of Document Availability, or HITSP/T33 – Transfer of Documents on Media with email transport	In pilot stage (Document Submission Specification)—based on IHE XDR profile

3.2.7 GAPS AND RECOMMENDATIONS

Table 3-4 summarizes the gap analysis and HITSP recommendations for resolving those gaps.

Table 3-4 Gaps and Recommendations – Supported Interactions

Requirement	Gap	Recommendations
Query-Retrieve	Support for dynamic/deferred documents in	IHE has an open work item to resolve this issue. HITSP



	NHIN does not exist in HITSP/TP13	will evaluate this work product once this work has been completed in IHE
Distributed Query	No standard supports the generic requirement of distributed query. Any standard which supports query capability can be used to create a distributed query application for a well-bounded Harmonization Request	No Action Necessary
Publish-Subscribe	None	WS-Notification provides a generic publish/subscribe framework, which will not be restated in HITSP unless specific profiling is required
Notify-Retrieve	None	No Action Necessary
Unsolicited Delivery	None	No Action Necessary

3.3 SECURITY ATTRIBUTES

Security attributes includes capabilities needed to establish trust between systems, provide confidentiality while in-transit, ensure authenticity of the data, and ensure that only authorized individuals have access to the data.

The functional capabilities or requirements below are derived from the ONC Security Attribute descriptions. The following terms are used:

- Access Decision Information (ADI) – a generic name for information used in determining an access control decision. It includes any requestor-asserted identity and other credentials as well as any other information associated with the request context that the access policy requires to reach an access decision
- Trust -- a “trusted” ADI source is one that a security domain authority will rely upon to provide certain information used to make access decisions. In order for ADI to be trusted for access decisions, the source of the ADI must be verified and the integrity of any assertion confirmed

3.3.1 MULTIPLE TRUST FRAMEWORKS

To enable secure, trusted communications between systems during message transmission. Common data transport should support multiple forms of trust authentication (such as, but not limited to, digital certificates, mechanisms for granting security tokens to participants, username and password verification, and hardware-based tokens such as smart cards) using a single common security framework. These capabilities need to be implementable across multiple security domains as well as within a single domain.

The previous paragraph requires a Single Common Security Framework that supports:

- Cross-domain ADI transfer with trust resolution
- Multiple ADI forms (implies token exchange capability)
- Verification of ADI source identity (enables trust resolution)
- Verification of ADI integrity (enables trust resolution)
- ADI token extensibility

HITSP/TP20 Access Control policies provide a means for establishing the ADI sources and asserted attributes that are trusted in determining an access decision. Both HITSP/C19 Entity Identity Assertion and HITSP/TP20 specify the use of the WS-Security and WS-Trust framework specifications for transferring ADI in security tokens carried in SOAP messages. Both Security Assertion Markup Language (SAML) assertions and WS-Trust security tokens can be extended to meet healthcare specific requirements if necessary.

NHIN supports the requirement for a single common security framework through its Messaging Platform and Authorization Framework specifications. The Messaging Platform specifies the use of WS-I Basic and Basic Security Profiles that provide support for cross-domain transfer of security tokens.



3.3.2 CONFIDENTIALITY

For securing message content during message transmission to prevent interception and observation. Digital encryption is an example of a technology that can be used to implement this Capability. Common data transport should define approaches for point-to-point confidentiality of messages between systems at the edges of health organizations, as well as for end-to-end confidentiality of messages between originator and recipient at the message content level.

HITSP/T17 provides for point-to-point and, using WS-I Basic Security Profile, end-to-end confidentiality of messages between systems. The NHIN Messaging Platform specifies the use of WS-I Basic and Basic Security profiles that provide support for both point-to-point and end-to-end message confidentiality compatible with HITSP/T17.

3.3.3 MESSAGE AUTHENTICATION AND INTEGRITY

To provide message integrity and nonrepudiation capabilities. An example of a technology that can be used to implement this Capability is digital signature.

HITSP/T17 provides message integrity during transport between network nodes and, using WS-I Basic Security Profile, support for end-to-end message integrity. The NHIN Messaging Platform specifies the use of WS-I Basic and Basic Security profiles that provide support for end-to-end message integrity.

HITSP/T17 can provide nonrepudiation at the network node level and, using WS-I Basic Security Profile, at the message level. The NHIN specifies the use of WS-I Basic and Basic Security Profiles that can provide support for message-level nonrepudiation.

3.3.4 ENTITY AUTHENTICATION

To enable message senders to provide entity authentication credentials to message recipients through a variety of trust mechanisms described above, including descriptions of the level of trust, and methods used for entity authentication.

The Single Common Security Framework described above also provides the framework required to transport security tokens used for entity authentication.

In order to meet healthcare domain trust requirements, the information model of ADI assertions must be extensible. Both HITSP/C19 Entity Assertion and HITSP/TP20 Patient ID Cross-Referencing specify the use of the WS-Security and WS-Trust framework specifications for transferring ADI in security tokens carried in SOAP messages. Both SAML assertions and WS-Trust security tokens can be extended to meet healthcare specific requirements if necessary. The NHIN Messaging Platform specifies the use of WS-I Basic and Basic Security Profiles that provide support for extensible SAML and WS-Trust security tokens.

SAML and WS-Trust security tokens also enable the cross-domain exchange of identity and other credentials.

3.3.5 AUTHORIZATION

To enable recipients of electronic health information to assert their justification for receiving electronic health information from the sender. This may require a framework for describing authorizations for the release of information, including roles and rationales, pursuant to statutory requirements such as HIPAA and other applicable law and policy.

The authorization framework must be able to determine whether, for a particular set of requested health information and the overall request context, policy criteria permit the transfer of that health information to the requestor. HITSP/TP20 provides such an access control framework for describing authorizations (via access policies). It provides for processing policy against access control information in or to reach an



access decision. A HITSP/TP20 Access Control service can also request additional assertions beyond those submitted with the resource request if needed to reach an access decision.

3.3.6 HITSP AND NHIN MAPPINGS

Table 3-5 summarizes the mapping between each of the individual security attribute requirements and the relevant HITSP constructs and NHIN specifications, as discussed in the previous sections.

Table 3-5 HITSP and NHIN Mappings – Security Attributes

Requirement	HITSP Constructs	NHIN Specifications
Single common security framework with trust resolution	HITSP/C19, HITSP/TP20 through reference to SAML, WS-Security, WS-Trust	Authorization Framework and Messaging Platform through reference to WS-I Basic and Basic Security profiles
Point-to-point message confidentiality	HITSP/T17	Authorization Framework and Messaging Platform with reference to WS-I Basic Security profile providing HITSP/T17 compatibility
End-to-end message confidentiality	HITSP/T17 using WS-I reference	Authorization Framework and Messaging Platform through reference to WS-I Basic and Basic Security profiles
Message integrity	HITSP/T17 using WS-I reference	Authorization Framework and Messaging Platform provide full support through reference to WS-I Basic and Basic Security profiles using digital signatures
Nonrepudiation of message	HITSP/T17 using WS-I reference	Authorization Framework and Messaging Platform
Transport framework for ADI/security tokens	HITSP/C19, HITSP/TP20	Authorization Framework and Messaging Platform through reference to WS-I Basic and Basic Security profiles
Extend ADI assertion information models for healthcare needs	HITSP/C19, HITSP/TP20 through WS-Security and WS-Trust references	Messaging Platform through the WS-I Basic and Basic Security profiles support for extensible SAML and Ws-Trust security tokens
Requestor assertion of identity and other credentials	HITSP/C19, HITSP/TP20	Messaging Platform through the WS-I Basic and Basic Security profiles support for cross-domain transfer of SAML and Ws-Trust security tokens
Authorization framework	HITSP/TP20	Limited HITSP/TP20 support through Access Consent Policy. HITSP/TP20 support can be provided via policy adapters

3.3.7 GAPS AND RECOMMENDATIONS

In the case of each of the above requirements, either HITSP constructs, NHIN specifications or their combination provide the functional capabilities necessary to meet the requirement. A resolution that removes any gaps and also serves to better align the HITSP constructs and NHIN specifications is as follows:

- Adopt standard information models for common ADI assertions that carry attributes impacting trust and interoperability in the healthcare environment

Table 3-6 summarizes the gap analysis and HITSP recommendations for resolving those gaps.

Table 3-6 Gaps and Recommendations – Security Attributes

Requirement	Gap	Recommendations
Single common security framework with trust resolution	None	No Action Necessary
Point-to-point message confidentiality	None	No Action Necessary
End-to-end message confidentiality	None	No Action Necessary
Message integrity	None	No Action Necessary
Nonrepudiation of message	None	No Action Necessary
Transport framework for ADI/security tokens	None	No Action Necessary



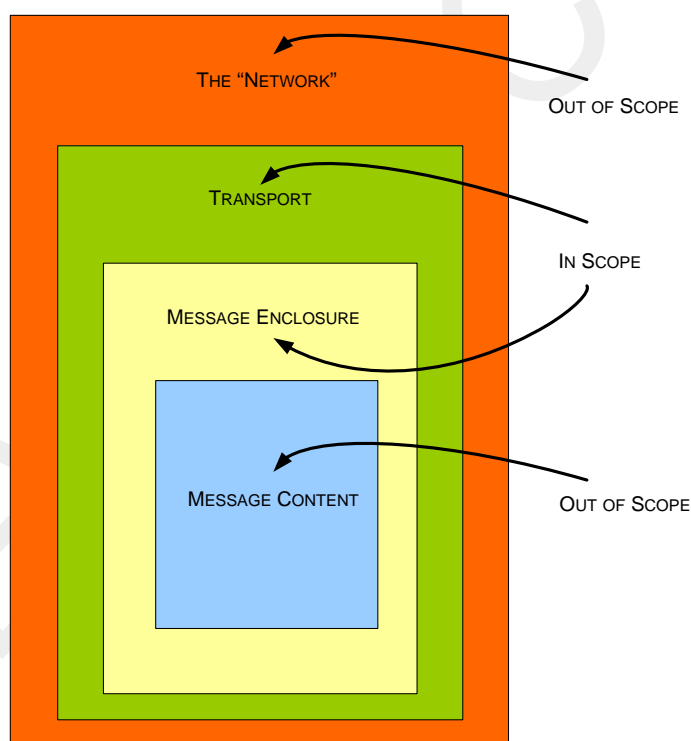
Requirement	Gap	Recommendations
Extend ADI assertion information models for healthcare needs	Missing or incomplete information models or schema for exchanging information required for access control decisions	Adopt standard information models for common ADI assertions that carry attributes impacting trust and interoperability in the healthcare environment
Requestor assertion of identity and other credentials	None	No Action Necessary
Authorization framework	None	No Action Necessary

3.4 MESSAGE ENCLOSURE

Message Encapsulation enables system implementers to create program code to process data exchange. This enforces the separation between the message envelope and the message boundaries and establishes the boundaries between them. This separation allows implementers to use metadata in the Message Enclosure without access to the Message Content.

As shown in Figure 3-6 below, the Message Envelope is outside the Message Content (payload), and inside the Transport and “Network”. The Message Enclosure is encapsulated by the Transport. It typically includes metadata (data about the message content), as well as addressing, routing, and security information. It is separate from the Message Content being transported, which is opaque to the data transport.

Figure 3-6 Message Enclosure



Characteristics of encapsulation include for example in an open distributed processing environment, that the user or program code cannot (1) look into the message content and are (2) accessed by a set of services supported by the message content, as (3) the users may know what the purpose of the message content is, but not how it fulfills that purpose. Message encapsulation allows the appropriate application of security to the Message Envelope and/or Message Content, since Message Envelope and Message Content may have different security requirements.



Should be consistent with secure design principles and facilitate normative and open source processes and interoperable Key Management Protocols and Encryption.

Message Encapsulation as a process should:

- Define a Harmonization Request
- Operationally define the boundaries between metadata and message content
- Define the format, schema and semantics of the metadata
- Agree upon a method or mode of communication

3.4.1 ENVELOPE METADATA

Provide a clear distinction between metadata describing the message (envelope) and the content of the message (body). The sender needs the ability to indicate which elements of the message envelope must be understood and processed by the receiver, and which are optional.

For SOAP message, the process should include:

- Encryption of message enclosure
- Encryption before encapsulation, and
- Encryption of the message content

The ability to support separate encryption on message enclosure and message content enables end-to-end security with multi-hop routing (see Section 3.5.4).

3.4.2 ADDRESSING AND ROUTING

Metadata associated with the message should include addressing information about the sender and receivers of a message. Addressing capabilities within the message enclosure should support message routing for all interactions.

The process described in Section 3.4.1 results in minimum routing headers being visible. Message IDs should be different from original "message ID". The Manifest header will/should contain a single reference element focused on the original message or to the header in which the original message is contained, as in the case of encryption.

New headers shall have a new manifest with focus of single entry as to content or payload with a Service and Action element, to facilitate additional applications or program code inclusive of time-stamp and/or signature.

3.4.3 MULTIPLE TYPES OF CONTENT

Messages need be able to transport information that is encoded in many forms. The message content may be directly encoded within the message (for example, as Extensible Markup Language - XML), but in other cases, the information may be one or more documents in a variety of formats (such as text or binary) enclosed or attached to the message. Content should be encrypted at strength levels as related to value or risk to the content.

3.4.4 HITSP AND NHIN MAPPINGS

Content and headers should be in compliance with standard methods of model driven architecture or development of Business Process Models or Common Taxonomy to enhance interoperability of solutions.

Table 3-7 summarizes the mapping between each of the individual envelope enclosure requirements and the relevant HITSP constructs and NHIN specifications, as discussed in the previous sections.



Table 3-7 HITSP and NHIN Mappings – Envelope Enclosure

Requirement	HITSP Constructs	NHIN Specifications
Envelope Metadata	SOAP 1.2; where SOAP is used, SOAP 1.2 applies and no additional HITSP construct is required	SOAP 1.2 specified in Messaging Platform
Addressing and Routing	WS addressing; where SOAP is used, WS addressing applies and no additional HITSP construct is required	WS-Addressing specified in Messaging Platform
Multiple Types of Content	MTOM is supported; where SOAP is used, MTOM applies and no additional HITSP construct is required	MTOM specified in Messaging Platform

3.4.5 GAPS AND RECOMMENDATIONS

Table 3-8 summarizes the gap analysis and HITSP recommendations for resolving those gaps.

Table 3-8 Gaps and Recommendations – Envelope Enclosure

Requirement	Gap	Recommendations
Envelope Metadata	None	No Action Necessary
Addressing and Routing	None	No Action Necessary
Multiple Types of Content	None	No Action Necessary

3.5 DISCOVERY AND ROUTING

Discovery and routing allows organizations to search and discover other organizations as well as available capabilities, manage secure connections, and exchange necessary data. The sub-sections below have a discussion on the key requirements for discovery and routing, the current standards that support the requirements, additional scope considerations, potential gaps in HITSP and NHIN work products, and recommendations to resolve those gaps.

3.5.1 ORGANIZATIONAL SEARCH AND DISCOVERY

Organizations must be able to search and discover the existence and the services of each other in order to establish secure connections with each other. This would include basic information for each organization such as its name, location(s), unique network identifier, public key (if the network utilizes public key infrastructure), the set of network services supported by that organization, and the universal resource identifiers (URI) necessary to invoke each of the supported services.

Pre-conditions:

- Unique identifiers must be associated with entities (organizations), such that a deterministic lookup can be used to find the right information
- Entities will publish information to repositories where they can be discovered
- Only vetted information is published in repositories (requires governance)
- The address of a repository or service where search can be conducted (e.g., a directory, or a service that queries a set of directories) is known or can be discovered

Existing Standards that support this requirement:

Table 3-9 Discovery and Routing Standards

Acronym	Standard	Description
UDDI	Universal Description Discovery and Integration UDDI Version 3.0.2 (http://www.uddi.org/pubs/uddi_v3.htm)	Directory, query and retrieval standard for organization and service invocation data



Acronym	Standard	Description
ebRS	ebXML Registry Service http://www.oasis-open.org/committees/regrep/documents/2.5/specs/ebrs-2.5.pdf	Directory, query and retrieval standard for organization and service invocation data
LDAP	Lightweight Directory Access Protocol http://tools.ietf.org/html/rfc4510	Directory, query and retrieval standard for organizational user information and public key certificates
DNS	Domain Name Service http://www.ietf.org/rfc/rfc1034.txt	Directory, query and retrieval standard to map

3.5.2 SERVICE INVOCATION METADATA

To invoke a service offered by another organization, that service must be fully described by its supplier. This information should include the interface description and network endpoint for that service, any applicable policy and metadata information (e.g. interface versioning) that constrains the invocation of that interface, and a binding mechanism to link the service interface to its implementation by the supplier.

Pre-conditions:

- Underlying transport/envelope standard must support a normative service description language. **Note:** SOAP based services can be described using WSDL, and ebXML based services can be described using CPP, CPA and BPSS. REST has no service description language standard at this time¹

Existing Standards that Support this Requirement:

Table 3-10 Service Invocation Metadata Standards

Acronym	Standard	Description
WSDL	Universal Description Discovery and Integration UDDI Version 3.0.2 (http://www.uddi.org/pubs/uddi_v3.htm)	Service Invocation metadata
ebXML CPP, CPA and BPSS	ebXML Collaboration Protocol Profile, Collaboration Protocol Agreement and Business Process Specification Schema	Service Invocation metadata

3.5.3 MESSAGE ROUTING

In many cases, messages must contain sufficient metadata such that they can be routed not just to an organization (URI) but to specific entity in an organization. These entities could include, for example, providers and clinical EHR systems, patient PHR records, hospital departments, pharmacies, or other potential information recipients. Utilizing internet-based protocols, health information messages need to be capable of being routed through any number of intermediary routers and firewalls before reaching their final destination. Message metadata needs to support a “return address” for asynchronous messaging support.

Existing Standards that Support this Requirement:

Table 3-11 Message Routing Standards

Acronym	Standard	Description
WS-Addressing	Web-Services Addressing (http://www.w3.org/Submission/ws-addressing/)	Metadata for routing messages

¹REST community has drafted a service description language called “Web Application Description Language” or WADL, but it is not yet a standard (not been ratified by any SDO).



3.5.4 MULTI-HOP MESSAGE ROUTING

In the case of routing via intermediaries such as health information exchanges, the messages go through multiple point-to-point connections, also known as “multi-hop”. Considerations for multi-hop message routing are provided below:

Pre-conditions for Multi-hop Message Routing:

- For multi-hop messaging to be interoperable, the underlying envelope standard must support addressing that is independent of the single hop address. WS-Addressing has this feature, which SOAP based transport can use (at this time, support for multi-hop addressing does not seem to be a part of REST framework)
- For there to be routing of business related and potential sensitive information between entities, a business and trust relationship must already exist between them
- To achieve multi-hop messaging via intermediaries such as HIE gateways, there needs to be a unique identification scheme at two or more levels. Each HIE gateway needs to have a unique identity, and each organization inside the HIE needs to have a unique identity within the HIE; e.g., <ProviderA@HIE1> sending a message to <LabB@HIE2>. Intermediaries will need to be trusted to resolve the address and deliver the message to the right end points based on these unique identifiers
- For inter-domain message routing with end-to-end encryption, the originator (e.g., ProviderA@HIE1) must be able to obtain the encryption key of the recipient (e.g., LabB@HIE2). If ProviderA uses HIE1 as the gateway to the NHIN, it needs to be able to perform a query for the encryption key via HIE1, which in turn may query HIE2’s PKI repository (e.g., LDAP) for this information and supply this to ProviderA@HIE1

Existing Standards that Support this Requirement:

Table 3-12 Multi-Hop Message Routing Standards

Acronym	Standard	Description
WS-Addressing	Web-Services Addressing (http://www.w3.org/Submission/ws-addressing/)	Metadata for routing messages

3.5.5 MULTIPLE RECIPIENTS

In certain circumstances messages will need to be transmitted to multiple recipients. This can include situations where the requestor asks the supplier to send the information to the requestor and additional recipients. This can also include broadcast or multicast capabilities, where a message is addressed to many organizations within a common community of interest (for example, public health alerting).

Pre-conditions:

- For broadcast, a service that can be a proxy and perform broadcast messaging to a list based on an alias. The identifiers used for such aliases must be unique and well known, and these identifiers need to be published and discovered
- For multicast of business related and potential sensitive information between entities, a business and trust relationship must already exist between the initiator and each recipient

Standards Gap:

- At this time, there is a standards gap in establishing end-to-end confidentiality (assuming asymmetric encryption) while performing broadcast messaging. In theory it is possible to distribute a symmetric “broadcast key” to all participants in a broadcast using asymmetric keys to secure the distribution of such a broadcast key. However in practice, such a secure broadcast key establishment protocol has not been established in the Internet space



3.5.6 DISCOVERY AND ROUTING – ADDITIONAL SCOPE CONSIDERATIONS

Since the scope of discovery and routing needs to be established, the following scope considerations need to be made regarding discovery and routing.

- Install-time (static) vs. Run-time (dynamic) Discovery
 - If the scope of discovery is limited to finding information at install-time (static), then one or more manual steps (e.g., signing of DURSA, exchange of security information) can be assumed to occur before routing takes place. Although this reduces complexity, the value of discovery in this case is limited, as additional manual steps are involved to get to routing
 - In contrast, run-time (dynamic) discovery assumes that there are no manual steps between discovery and routing. However, such a dynamic establishment of routing requires that (a) all information needed for routing be made available dynamically, which makes it more complex (and possibly less secure), and (b) assumes that the entities involved have a pre-existing business and trust relationship even prior to discovery and routing, which may not be realistic in most situations
- Intra- vs. Inter-Domain
 - Intra-domain discovery can be accomplished using a shared directory. However, for inter-domain discovery a shared directory cannot be assumed. Within the current NHIN architecture, gateways may mediate the communications between entities that belong to different domains (HIEs), hence both discovery and routing related communication may need to be routed through these gateways. NHIN specifications have been created for subject discovery across HIEs, but currently there seems to be a gap in specifications for mediated discovery of organizations/services and their connectivity and security metadata using the HIE gateways as intermediaries

In summary, the complexity and utility of discovery and routing are shown below in ascending order:

- Intra-domain, static
- Intra-domain, dynamic
- Inter-domain, static
- Inter-domain, dynamic

3.5.7 HITSP AND NHIN MAPPINGS

Table 3-13 summarizes the mapping between each of the individual discovery and routing requirements and the relevant HITSP constructs and NHIN specifications, as discussed in the previous sections.

Table 3-13 HITSP and NHIN Mappings – Discovery and Routing

Requirement	HITSP Constructs	NHIN Specifications
Organizational Search and Discovery	No HITSP constructs. De-facto standards are assumed (e.g., UDDI, LDAP, DNS)	NHIN Services Registry specification uses UDDI 3.0 standards for publication and discovery of entity information
Service Invocation Metadata	WSDL; where SOAP is used, SOAP 1.2 applies. REST does not have a standards based way to specify service invocation metadata	SOAP and WSDL is specified in Messaging Platform specification
Message Routing	WS addressing; where SOAP is used, WS addressing applies. REST does not have a transport independent way to perform routing	WS-Addressing is specified in Messaging Platform specification
Multi-hop Message Routing	WS addressing; where SOAP is used, WS addressing applies; HITSP/T17 specifically covers this using WS-I. REST does not have a transport independent way to perform multi-hop addressing/routing. Gaps exist in end-to-end discovery and multi-hop routing via HIE gateways	WS-Addressing is specified in Messaging Platform specification. Gaps exist in end-to-end discovery and multi-hop routing via HIE gateways



Requirement	HITSP Constructs	NHIN Specifications
Multiple Recipients	HITSP/SC116 (Emergency Message Distribution Element) supports multiple recipients	No specification exists at this time

3.5.8 GAPS AND RECOMMENDATIONS

Table 3-14 summarizes the gap analysis and HITSP recommendations for resolving those gaps.

Table 3-14 Gaps and Recommendations – Discovery and Routing

Requirement	Gap	Recommendations
Organizational Search and Discovery	No HITSP constructs exist for discovery at this time Unique identifiers for entities and repositories	HITSP will evaluate whether a new construct is needed or appropriate. UDDI 3.0 would be one candidate. HITSP will evaluate whether an identifier structure needs to be specified in a construct. Possible candidates are DNS names, URIs, and ISO OIDs
Service Invocation Metadata	No gaps if SOAP+WSDL is used REST has no service invocation metadata language	If REST based transport must support Harmonization Requests where a service invocation metadata is required, then HITSP will need to work with SDOs to identify the metadata language
Message Routing	No gaps if SOAP+WS-Addressing is used REST does not have a transport independent addressing capability equivalent to WS-Addressing	If REST based transport must support Harmonization Requests where addressing and message routing in a transport independent manner is required, then HITSP will need to work with SDOs to identify such an addressing language
Multi-hop Message Routing	End-to-end discovery of organizations, services and security metadata and routing with HIEs acting as gateways	Assuming there are Harmonization Requests that need this, work with SDOs to identify standards that meet these requirements, and create new HITSP work-products
Multiple Recipients	SC116 (Emergency Message Distribution Element) is not sufficiently secure to communicate PHI and only goes to distribution nodes and is therefore not end-to-end End-to-end confidentiality requires key negotiation protocols	Assuming there are Harmonization Requests that need this, work with SDOs to identify standards that meet these requirements, and create new HITSP work-products

3.6 RELIABLE MESSAGING

Reliable messaging requirements cover the ability of a transport to either deliver a message or ensure that both parties to a data interchange are aware that a message may not have been delivered. In general, it is impossible to absolutely ensure the reliable delivery of messages. It is only possible to ensure that reliability is acceptable for a particular application and that both parties, knowing the delivery semantics, can recover from errors. In the general case, this is a provably unsolvable problem.

Ultimately, arbitrary reliable messaging semantics require application level and/or Harmonization Request specific semantics. Two examples are the use of “Application Acknowledgements” in HL7 and the CAQH/CORE operating rules for acknowledgements which are incorporated into HITSP/T40 Patient Generic Health Plan Eligibility Verification.

3.6.1 MULTIPLE DELIVERY

Messaging processes should support multiple delivery semantics, including delivery at least once, at most once, or exactly once. Additionally, capabilities should be available to provide assurances with respect to the order in which messages are delivered, if required.

3.6.2 FAULT NOTIFICATION

Capabilities are needed to provide a standards-based framework for receivers of messages to transmit fault information to senders when messages cannot be understood or processed.



3.6.3 HITSP AND NHIN MAPPINGS

Table 3-15 summarizes the mapping between each of the individual reliable messaging requirements and the relevant HITSP constructs and NHIN specifications, as discussed in the previous sections.

Table 3-15 HITSP and NHIN Mappings – Reliable Messaging

Requirement	HITSP Constructs	NHIN Specifications
Multiple Delivery Semantics	No standards have been selected by HITSP and no general solution is desired within the context of HITSP harmonization, although specific constructs may include Harmonization Request specific delivery semantics	Addressed through WS-ReliableMessaging in the Messaging Platform specification. This does not apply to every message and is constrained to specific profiles
Fault Notification	No standards have been selected by HITSP and no general solution is desired within the context of HITSP harmonization, although specific constructs may include Harmonization Request specific delivery semantics	Addressed through SOAP fault support in Messaging Platform. Custom SOAP faults defined at the profile level

3.6.4 GAPS AND RECOMMENDATIONS

Table 3-16 summarizes the gap analysis and HITSP recommendations for resolving those gaps.

Table 3-16 Gaps and Recommendations – Reliable Messaging

Requirement	Gap	Recommendations
Multiple Delivery Semantics	None	No Action Necessary
Fault Notification	None	No Action Necessary



4.0 NON-FUNCTIONAL REQUIREMENTS

Most of the requirements covered by the ONC Gap/Extension document are functional requirements—requirements tied to specific behaviors. All other types of requirements are known as non-functional requirements and are generally transitive across an entire system, regardless of specific behaviors in a system. The ONC Gap/Extension document identifies several non-functional requirements.

4.1 SCALABILITY

Requirement: Harmonized standards could support the ability to scale the messaging transmission (clinical data exchange) services to any size organization regardless of the technologies it implements.

4.2 EXTENSIBILITY

Requirement: Harmonized standards could support the ability of an organization to expand the range of services it chooses to provide through re-use of implementable technologies. It could support new ways and methods for exchanging health information via any type of data message or format. It could support new values for codes, additional data and routing information in the message headers, while supporting a bridge to existing data transport methodologies leading to a clear migration path.

NHIN: The NHIN is essentially a service interface specification. Thus, the extensibility requirement is partially met by virtual allowing for new (unforeseen) services to be specified and implemented in future versions. However, the current (at time of writing this document) NHIN specifications do constrain extensibility to the extent that NHIN services should provide for certain minimal data elements related to purpose of use, user identity, system identity, policy statements, etc.

4.3 PLATFORM INDEPENDENCE

Requirement: Harmonized standards could support an organization's unique technical capabilities while promoting health information exchange regardless of a particular organization's hardware, software, services, and/or programming language.

NHIN: Addressed by selection of XML, Web Services (WS-*), WS-I and SOAP in the NHIN Messaging Platform specification. These standards were specifically intended to be platform independent and were explicitly selected by the NHIN to provide for platform independence.

4.4 COHERENCE

Requirement: It is important that the harmonized standards be logically related to each other within a common and coherent framework for communication and security.

NHIN: Addressed by selection of WS-* in Messaging Platform, which provides services at the transport, discovery and exchange level of communications. WS stack is coherent—they build on each other and are consistent with each other. However, it should be noted that coherence can sometimes be opposed to the goal of extensibility since one may need to extend the system to handle incoherent protocols, and data.



5.0 GAPS AND RECOMMENDATION SUMMARY

The identification of gaps and recommendations are consolidated and documented in the table below. HITSP recognizes that the level of privacy and security required is a policy decision informed by risk analysis, whereas the ONC Gap/Extension document sets a baseline for the set of security and privacy requirements that need to be met. Therefore HITSP is guided by the requirements identified in the requirements document and is cognizant of the rapidly evolving market requirements. HITSP expects a prioritized roadmap will be developed in response to specific Harmonization Requests.

Table 5-1 Gaps and Recommendations – Summary

Requirement	Gap	Recommendation
Web Services	SOAP is required by the IHE XDR profile, which was selected for HITSP/TP31	Possible variant of HITSP/TP31 based on REST could be developed by an SDO
Query-Retrieve	Support for dynamic/deferred documents in NHIN does not exist in HITSP/TP13	IHE has an open work item to resolve this issue. HITSP will evaluate this work product once this work has been completed in IHE
End-to-end message confidentiality	None	No Action Necessary
Message integrity	None	No Action Necessary
Nonrepudiation of message	None	No Action Necessary
Extend ADI assertion information models for healthcare needs	Missing or incomplete information models or schema for exchanging information required for access control decisions	Adopt standard information models for common ADI assertions that carry attributes impacting trust and interoperability in the healthcare environment
Organizational Search and Discovery	<ul style="list-style-type: none"> No HITSP constructs exist for discovery at this time Unique identifiers for entities and repositories 	<ul style="list-style-type: none"> HITSP will evaluate whether a new construct is needed or appropriate. UDDI 3.0 would be one candidate HITSP will evaluate whether an identifier structure needs to be specified in a construct. Possible candidates are DNS names, URIs, and ISO OIDs
Service Invocation Metadata	<ul style="list-style-type: none"> No gaps if SOAP+WSDL is used REST has no service invocation metadata language 	If REST based transport must support Harmonization Requests where a service invocation metadata is required, then HITSP will need to work with SDOs to identify the metadata language
Message Routing	<ul style="list-style-type: none"> No gaps if SOAP+WS-Addressing is used REST does not have a transport independent addressing capability equivalent to WS-Addressing 	If REST based transport must support Harmonization Requests where addressing and message routing in a transport independent manner is required, then HITSP will need to work with SDOs to identify such an addressing language
Multi-hop Message Routing	End-to-end discovery of organizations, services and security metadata and routing with HIEs acting as gateways	Assuming there are Harmonization Requests that need this, work with SDOs to identify standards that meet these requirements, and create new HITSP work-products
Multiple Recipients	<ul style="list-style-type: none"> HITSP/SC116 (Emergency Message Distribution Element) is not sufficiently secure to communicate PHI and only goes to distribution nodes and is therefore not end-to-end End-to-end confidentiality requires key negotiation protocols 	Assuming there are Harmonization Requests that need this, work with SDOs to identify standards that meet these requirements, and create new HITSP work-products



6.0 DOCUMENT UPDATES

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

6.1 JANUARY 31, 2010

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

