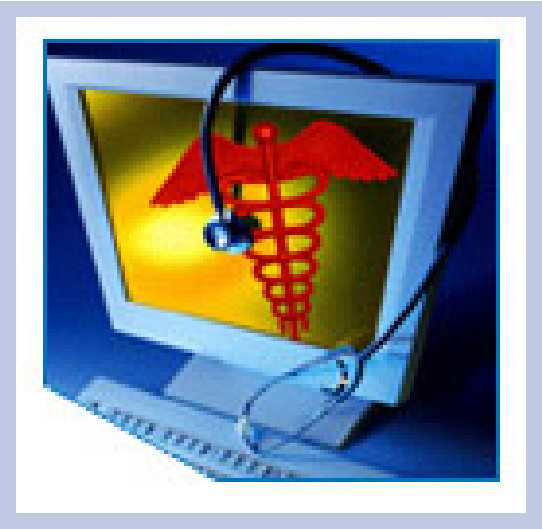
August 27, 2008
Version 3.1

HITSP Biosurveillance Interoperability Specification

HITSP/IS02



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Population Perspective Technical Committee
(Formerly Population Health Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final Draft	Biosurveillance Technical Committee	August 18, 2006
1.1	Ready for Public Comment	Biosurveillance Technical Committee	September 12, 2006
1.2	Ready for Implementation Testing	Biosurveillance Technical Committee	October 20, 2006
1.3	Review Copy	Population Heath Technical Committee	April 27, 2007
2.0	Released for Implementation	Population Heath Technical Committee	May 11, 2007
2.1	Released for Implementation	Population Heath Technical Committee	December 13, 2007
2.1.1	Review Copy	Population Heath Technical Committee	March 19, 2008
3.0	Released for Implementation	Population Health Technical Committee	March 27, 2008
3.0.1	Review Copy	Population Perspective Technical Committee	August 20, 2008
3.1	Released for Implementation	Population Perspective Technical Committee	August 27, 2008

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

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

1.1 INTEROPERABILITY SPECIFICATION OVERVIEW

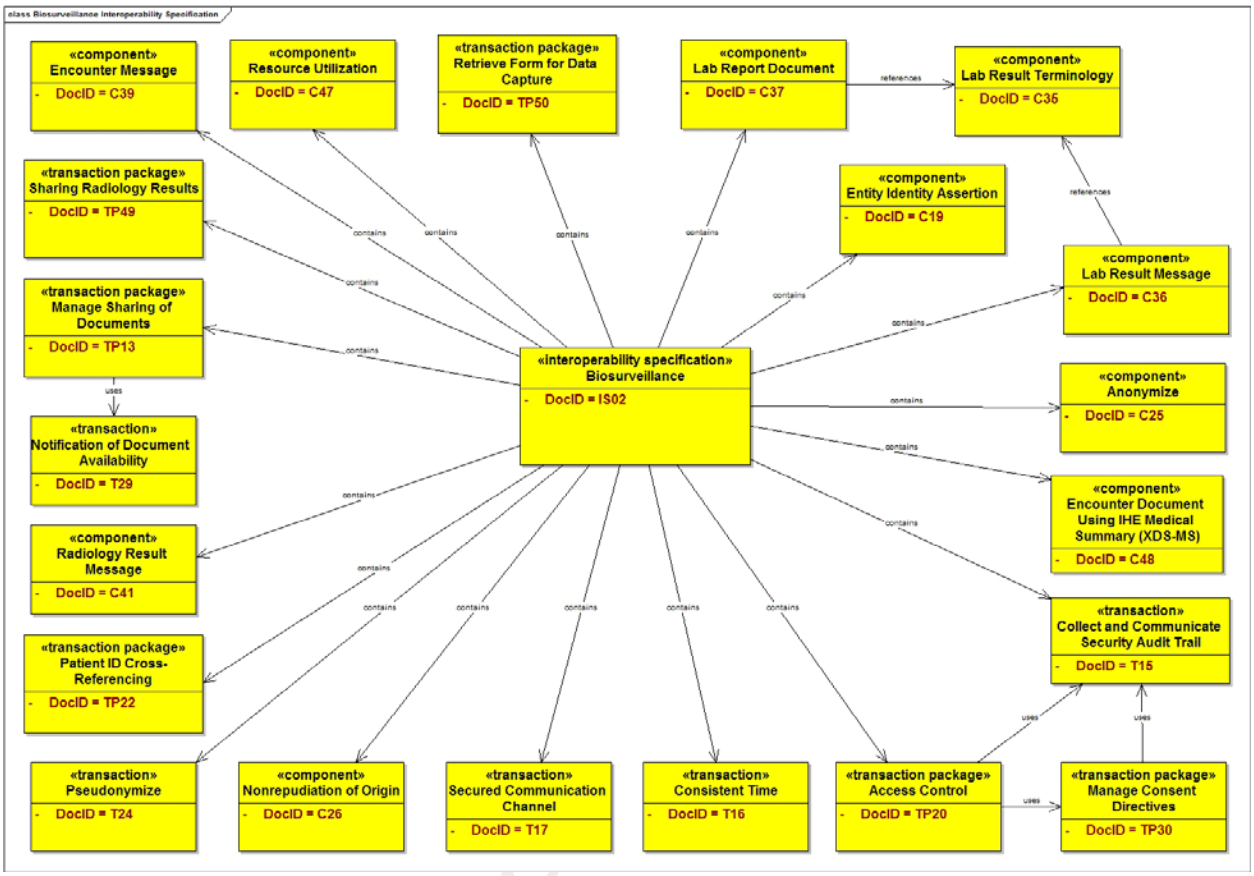
This section describes a high level definition of this Interoperability Specification and background information about the underlying Use Case that it is based upon.

Biosurveillance is an American Health Information Community (AHIC) breakthrough area defined as implementation of near real-time, nationwide public health event monitoring to support early detection, situational awareness and rapid response management across care delivery, public health, and other authorized government agencies. The Use Case describes the process or interaction that each primary stakeholder will invoke to capture, discover, anonymize and transmit relevant data.
The AHIC Biosurveillance Use Case that defines the scope of the Interoperability Specification describes the process or interaction that each primary stakeholder will invoke in the capture, discovery, anonymization and transmission of relevant data. In particular, an implementer must provide the technical infrastructure and security framework necessary to support operations in accordance with law, regulation, best practices and business agreements.

1.2 INTEROPERABILITY SPECIFICATION DOCUMENT MAP

Each HITSP Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications to satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant context(s) for the use of HITSP constructs that further identify and constrain standards where necessary. In addition to ISs, there are three other types of HITSP constructs called Transaction Packages (TP), Transactions (T) and Components (C). The document map depicted in Figure 1.2-1 identifies the HITSP constructs used to meet the IS requirements. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

Figure 1.2-1 Interoperability Specification Document Map



1.2.1 LIST OF CONSTRUCTS

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

Table 1.2.1-1 List of Constructs

Construct	Description
HITSP/C19	HITSP Entity Identity Assertion Component
HITSP/C25	HITSP Anonymize Component
HITSP/C26	HITSP Nonrepudiation of Origin Component
HITSP/C35	HITSP Lab Result Terminology Component
HITSP/C36	HITSP Lab Result Message Component
HITSP/C37	HITSP Lab Report Document Component
HITSP/C39	HITSP Encounter Message Component
HITSP/C41	HITSP Radiology Result Message Component

Construct	Description
HITSP/C47	HITSP Resource Utilization Message Component
HITSP/C48	HITSP Encounter Document Using IHE Medical Summary (XDS-MS) Component
HITSP/T15	HITSP Collect and Communicate Security Audit Trail Transaction
HITSP/T16	HITSP Consistent Time Transaction
HITSP/T17	HITSP Secured Communications Channel Transaction
HITSP/T24	HITSP Pseudonymize Transaction
HITSP/T29	HITSP Notification of Document Availability Transaction
HITSP/TP13	HITSP Manage Sharing of Documents Transaction Package
HITSP/TP20	HITSP Access Control Transaction Package
HITSP/TP22	HITSP Patient ID Cross-Referencing Transaction Package
HITSP/TP30	HITSP Manage Consent Directives Transaction Package
HITSP/TP49	HITSP Sharing Radiology Results Transaction Package
HITSP/TP50	HITSP Retrieve Form for Data Capture Transaction Package

1.3 COPYRIGHT PERMISSIONS

ASTM International materials used in this document have been extracted, with permission from E-2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. Copies of this standard are available through the ASTM Web Site at www.astm.org.

Certain materials contained in this Interoperability Specification are reproduced from Health Level Seven (HL7) Clinical Document Architecture Release 2 (CDA R2), HL7 U.S. Realm – Interoperability Specification: Lab Result Message to EHR, HL7 Role Based Access Control (RBAC) Healthcare Permissions Catalog, HL7 Version 2.5, HL7 Version 2.5.1, HL7 Version 3.0 Privacy Consent related specifications with permission of Health Level Seven, Inc. No part of the material may be copied or reproduced in any form outside of the Interoperability Specification documents, including an electronic retrieval system, or made available on the Internet without the prior written permission of Health Level Seven, Inc. Copies of standards included in this Interoperability Specification may be purchased from the Health Level Seven, Inc. Material drawn from these standards is credited where used.

IHE materials used in this document have been extracted from relevant copyrighted materials with permission of Integrating the Healthcare Enterprise (IHE) International. Copies of this standard may be retrieved from the IHE Web Site at www.ihe.net.

This material includes SNOMED Clinical Terms® (SNOMED CT®) which is used by permission of the International Health Terminology Standards Development Organisation (IHTSDO). All rights reserved. SNOMED CT® was originally created by The College of American Pathologists.
"SNOMED" and "SNOMED CT" are registered trademarks of the IHTSDO.

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

1.4 REFERENCE DOCUMENTS

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

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications

Reference Document	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
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
Harmonized Use Case for Biosurveillance (Visit, Utilization, and Lab Result Message), March 19, 2006	AHIC Use Case that is the basis of this Interoperability Specification
TN900 - Security and Privacy Technical Note	Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following: • The scope, reference policy background, and Security and Privacy principles used in the development of the constructs • A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs • A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases • A list of identified gaps and the recommended approaches to resolving those gaps • A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications • A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management • A glossary of terms used in all the Security and Privacy construct documents • A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment HITSP will periodically update this Technical Note as required by the introduction of new contexts for use

2.0 INTEROPERABILITY REQUIREMENTS

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

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

2.1 USE CASE SYNOPSIS

This section provides a synopsis of the Biosurveillance Use Case, including any applicable scenarios that are part of the Use Case.

Biosurveillance is an American Health Information Community (AHIC) breakthrough area defined as implementation of real-time, nationwide public health event monitoring to support early detection, situational awareness, and rapid response management across public health and care delivery communities and other authorized Government agencies.

This Use Case describes the process or interaction that each primary stakeholder will invoke in the capture, discovery, anonymization and transmission of relevant data.

This Use Case addressed in this document is for the transmission of essential data from in patient admissions, ambulatory care and emergency department visits, resource utilization and lab result data from healthcare delivery and public health information systems in a standardized and anonymized format, to authorized Public Health Agencies with less than one day lag time. The system and processes must also support the ability for authorized public health personnel to go back to the data source to re-link the anonymized biosurveillance data to the data source as part of an appropriate public health investigation.

The management of data to ensure proper routing, security, privacy, and timely reporting is critical to enabling biosurveillance activities. Potential architectural solutions to data flow issues include using individual facility data sources (e.g., single hospitals or ambulatory care sites) or network system such as a multi-faculty system or supporting organization that uses data in the course of providing other services and sends data to all appropriate public health agencies. Other permutations of these two models can also be considered. The role of the data or network system can be accomplished by several different stakeholders, including hospital systems, health plans, independent laboratories and other possibilities. It

is anticipated that Nationwide Health Information Network (NHIN) efforts will develop supporting approaches and infrastructure that may offer other solutions as well.

2.2 USE CASE REQUIREMENTS

This section describes the Use Case requirements and outlines all the given scenarios at a high level.

This Use Case primarily includes the actions that are required to identify specific clinical care information used in the context of care and share these data with public health organizations to support biosurveillance needs including initial event detection, situational awareness, outbreak management and response support. There are activities that occur inside of Public Health Agencies and some healthcare organizations related to biosurveillance functions and processing. These functions are not portrayed in this document since the Use Case is focused on the exchange of data from clinical sources to Public Health Agencies, rather than how the data are employed by Public Health Agencies in the execution of their missions.

Wherever possible, existing data, workflows and systems shall be leveraged to minimize the barriers to participation in data sharing. Further, while this Use Case describes delivering clinical care data to Public Health Agencies, the policies, processes and standards may be applicable to many types of public health surveillance, including communicable disease, injury and cancer surveillance. The Use Case scope **includes** the following:

1. Data routinely entered into hospital, ambulatory care, and other ancillary care data systems. These may include patient demographics; diagnostic data; chief complaints; triage data; laboratory orders and results; physician orders; healthcare facilities' capacity information; and admission, discharge and transfer data
2. Hospital systems and affiliated clinical personnel who have clinical data of public health significance or oversee response management responsibilities
3. The legally authorized local, regional, state and federal public health personnel who monitor and manage public health surveillance data

The scope of this Use Case **excludes** the following:

1. Sources other than those described in the "includes" section above, such as Emergency Medical Services (EMS) run data, school absenteeism reports, poison center calls and other sources of potentially relevant data
2. The modeling of many interactions between the perspectives in this Use Case that occur as part of conducting normal business functions related to patient care. For example, physicians who order lab tests relevant to biosurveillance activities may interact with laboratories that are captured in the Integrated Healthcare Data Suppliers perspective. However, the processes for ordering of the test (and modeling to reflect it) are not within the scope of this Use Case. The return of the results to the ordering physician is similarly out of scope. The collection and transmission of the relevant lab results to Public Health Agencies is the action of interest and is therefore included in the model

3. Policies for other use or sharing of data for non-biosurveillance purposes
4. The specific processes and algorithms used by public health to manage and respond to public health crises
5. The processes through which alerts and other information are communicated from Public Health Agencies to physicians and hospitals in the event of an outbreak or other situation of public health significance
6. The following organizations and types of individuals:
    - First responders such as police or EMS
    - The press and the general public (as a recipient of public health alerts when applicable)
7. The following Public Health Agency activities:
    - Surveillance data management
    - Surveillance analytical methods for determining trends and event correlation
    - Identifying populations at risk
    - Public health and public notification mechanisms
    - Routine health promotion and environmental health promotion programs

To accomplish the charge, two broad categories of essential data shall be provided to Public Health Agencies: data used in the process of patient care and dynamic resource utilization data.

Data Used in the Process of Patient Care:

Within the healthcare data category, a minimum of four subcategories of essential data shall be provided in electronic format, as follows:

1. Limited Patient Demographic Data: may include but is not limited to encounter date, patient information (date of birth, age, gender, resident zip code, state of residence), date/time of last record update and randomized data linker. All data will be anonymized before transmission to Public Health Agencies. Once anonymized, a randomized data linker provides the ability to re-identify the patient, through the data provider as part of an authorized public health investigation
2. Clinical Data: may include but is not limited to patient class (outpatient, inpatient, and ER), diagnosis/injury code, diagnosis type, diagnosis date and time, and discharge disposition, chief complaint, date and time of first symptoms of illness
3. Laboratory and Radiology Test Orders: may include but is not limited to order number, order test and randomized data linker
4. Laboratory and Radiology Test Results: may include but is not limited to reporting lab ID, performing lab ID, report date/time, report status, collection date, collection method, specimen, specimen site, test ordered, test results, organism identified / result other than organism, method type, result unit, test interpretation, susceptibility test interpretation, test status and randomized data linker

Dynamic Resource Utilization Data:

Utilization data should be captured and provided to Public Health Agencies so that officials can determine the status and available capacities of participating healthcare facilities. Within the utilization data category, a minimum of three subcategories of essential data shall be provided in electronic format, as follows:

1. Institution Data: includes but is not limited to Hospital System, main facility ID/name, physical facility address and total number of beds in institution
2. Unit-level Census Data: includes but is not limited to unit name, number of patients by unit, number of beds available by unit and emergency room triage marginal capacity as a percentage and head-count
3. Facility Utilization Data: includes but is not limited to admissions, discharges, deaths and in last 24 hours at institution, date and time of report

2.2.1 MAPPING OF USE CASE REQUIREMENTS TO INTEROPERABILITY REQUIREMENTS

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

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

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
Bio-surveillance	Healthcare Delivery Organizations, (Laboratory, Radiology)	N/A	1.1.1.0 Event: Filter existing data to identify data required by Public Health Agencies	1.1.1.1.1 Action: Filter collected data records to identify biosurveillance data (Laboratory Results)	A consistent definition to screen data that should be sent to a Biosurveillance Information System (BIS) system HL7 filter, vs SQL query, standard way to represent rules (HL7 clinical decision support group) For Document Sharing, IHE XDS Registry Query, RFD, XPATH, SQL Filter data as requested by information resource Verify and track any documents requiring patient acknowledgement, consent or PH authorization Enable free-text parsers to cull coded data Need to express 'Reason for Test'	
	Integrated Healthcare Data Suppliers			1.2.1.1 Action: Filter stored data to identify biosurveillance data		
	Healthcare Delivery Organizations, (Clinician)			1.1.1.1.2 Action: Filter collected data records to identify biosurveillance data (Visit)		
	Integrated Healthcare Data Suppliers			1.2.1.1 Action: Filter stored data to identify biosurveillance data		

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
	Healthcare Delivery Organizations, (Clinician: Hospital)			1.1.1.1.3 Action: Filter collected data records to identify biosurveillance data (Utilization)	Filter data as requested by information resource Semantic Expression A data capture mechanism to support the gathering of additional information for reporting	
	Integrated Healthcare Data Suppliers			1.2.1.1 Action: Filter stored data to identify biosurveillance data		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.1.1.4 Action: Aggregate identified data	For Document Sharing, Multi-patient IHE XDS Registry Query	
	Integrated Healthcare Data Suppliers			1.2.1.2 Action: Aggregate identified data		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)		1.1.2.0 Event: Anonymize data required by Public Health Agencies	1.1.2.1 Action: Required data are checked to ensure full privacy requirement compliance	Provide the security subsystem to ensure that access to data is given only to authorized users Apply a common standard to anonymize or pseudonymize patient data to protect patient identity form undesired disclosure when communicating care data to/from external parties Ability to track the patient across multiple encounters while retaining anonymity	Data Requirement 1 Data Requirement 3 Data Requirement 4 Data Requirement 5 Data Requirement 6 Data Requirement 7 Data Requirement 8
	Integrated Healthcare Data Suppliers			1.2.2.1 Action: Required data are checked to ensure full privacy requirement compliance		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.2.2 Action: A randomized data linker is provided to allow authorized entities to re-link to patient data		

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
	Integrated Healthcare Data Suppliers			1.2.2.2 Action: A randomized data linker is provided to allow authorized entities to re-link to patient data		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)		1.1.3.0 Event: Format data required by Public Health Agencies	1.1.3.1 .1 Action: Transform data using approved standards (Laboratory Results)	Data authentication, integrity and nonrepudiation of origin Terminology Service to enable use of the data mapping across enterprises, for example knowing all the different ways blood pressure could be noted and successfully using it This Use Case includes publish and subscribe functionality, (e.g., when information has been created, others are notified of its existence) This Use Case requires standards for defining topics in such a way that notifications can be filtered effectively based on patient identity and information type Support both Persistent Documents and Messages Terminology support for: Specimen Site Presumptive Diagnosis Orders Test Battery	Data Requirement 1 Data Requirement 3 Data Requirement 6 Data Requirement 7
	Integrated Healthcare Data Suppliers			1.2.3.1 Action: Transform data using approved standards		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.3.1.2 Action: Transform data using approved standards (Visit)		Data Requirement 1 Data Requirement 3 Data Requirement 4 Data Requirement 5
	Integrated Healthcare Data Suppliers			1.2.3.1 Action: Transform data using approved standards		

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.3.1.3 Action: Transform data using approved standards (Utilization)	Data authentication, integrity and nonrepudiation of origin Access Terminology Services: Use of the data mapping across enterprises, for example knowing all the different ways blood pressure could be noted and successfully using it	Data Requirement 1 Data Requirement 2
	Integrated Healthcare Data Suppliers			1.2.3.1 Action: Transform data using approved standards		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)		1.1.4.0 Event: Identify Public Health Agencies that must be notified	1.1.4.1 Action: Determine which Public Health Agencies require notification	Interoperability with HAN: Process workflow definition	Data Requirement 1
	Integrated Healthcare Data Suppliers			1.2.4.1 Action: Determine which Public Health Agencies require notification		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)		1.1.5.0 Event: Transmit relevant data to Public Health Agencies	1.1.5.1.1 Action: Send results to public health agencies (Laboratory Results)	Assures the claimed identity of a user across enterprises, i.e., verify the user is who he says he is Provides the security subsystem to ensure that access to data is given only to authorized users Verify and track any documents	Data Requirement 1 Data Requirement 3 Data Requirement 4 Data Requirement 6 Data Requirement 7

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
	Integrated Healthcare Data Suppliers			1.2.5.1 Action: Send results to public health agencies	requiring patient acknowledgement, PH authorization, or consent Maintain Consistent Time across enterprises This Use Case includes publish and subscribe functionality (e.g., when information has been created, others are notified of its existence) This Use Case requires standard for defining topics in such a way that notifications can be filtered effectively based on patient identity and information type Ensure that communicating nodes may authenticate each other and establish a secure communication channel Register, reconcile and share credentials (machine) Support both Persistent Documents and Messages	
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.5.1.2 Action: Send results to public health agencies (Visit)		Data Requirement 1 Data Requirement 3 Data Requirement 4 Data Requirement 5
	Integrated Healthcare Data Suppliers			1.2.5.1 Action: Send results to public health agencies		
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.5.1.3 Action: Send results to public health agencies (Utilization)	Assures the claimed identity of a user across enterprises, i.e., verify the user is who he says he is Provides the security subsystem to ensure that access to data is given only to authorized users Verify and track any documents	Data Requirement 1 Data Requirement 2

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
	Integrated Healthcare Data Suppliers			1.2.5.1 Action: Send results to public health agencies	requiring patient acknowledgement, PH authorization, or consent Maintain Consistent Time across enterprises This Use Case includes publish and subscribe functionality, (e.g., when information has been created, others are notified of its existence) This Use Case requires a standard way for defining topics in such a way that notifications can be filtered effectively based on patient identity and information type Ensure that communicating nodes may authenticate each other and establish a secure communication channel Register, reconcile and share credentials (machine) Support both Persistent Documents and Messages	
	Healthcare Delivery Organizations, (Clinician, Laboratory, Radiology)			1.1.5.2 Action: Log interaction between organization systems and public health agencies	Collect and Communicate Audit Trail	
	Integrated Healthcare Data Suppliers			1.2.5.2 Action: Log interaction between organization systems and public health agencies		
	Public Health Agencies		1.3.1.0 Event: Provide listing of required biosurveillance data	1.3.1.1 Action: Notify involved organizations of data that must be transmitted to Public Health Agencies	This is a paper/human process today. Needs workflow definition Notify Document Availability across enterprises Publish information and notifications and subscribe to topics	

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
			1.3.2.0 Event: Receive biosurveillance data	1.3.2.1 Action: Receive clinical data from the all data sources	Probably PHIN MS, Certificates from PHIN MS Provide Secure Data Messaging Communicate Batch Data Assures the claimed identity of a user across enterprises, i.e., verify the user is who he says he is	Data Requirement 1 Data Requirement 2 Data Requirement 3 Data Requirement 4 Data Requirement 5 Data Requirement 6 Data Requirement 7
					Provides the security subsystem to ensure that access to data is given only to authorized users Verify and track any documents requiring patient acknowledgement, PH authorization, or consent Maintain Consistent Time across enterprises This Use Case includes publish and subscribe functionality, (e.g., when information has been created, others are notified of its existence) This Use Case requires a standard way for defining topics in such a way that notifications can be filtered effectively based on patient identity and information type Ensure that communicating nodes may authenticate each other and establish a secure communication channel Register, reconcile and share credentials (machine) Support both Persistent Documents and Messages	
				1.3.2.2 Action: Verify authenticity of transmission contents	Data authentication, integrity and nonrepudiation of origin Probably PHIN MS, Certificates from PHIN MS	

Use Case	Perspective/ Business Actor	Use Case Scenario	Event	Action	Interoperability Requirement(s) (Includes security requirements)	Data Requirement Number
				1.3.2.3 Action: Acknowledge receipt of clinical data	Built into each of the messaging standards Need consistency in the level of ACK – need an implementation guide for consistent processes The ability to assure automated or human assertion that the information was received and correct	
				1.3.2.4 Action: Log receipt and storage of lab test results	Create and communicate audit trail events for security and privacy related to the communication of patient health identified information	

2.2.2 DATA AND INFORMATION REQUIREMENTS MATRIX

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

Table 2.2.2-1 Data Element and Information Requirements

Data Requirement Number	Description
Data Requirement 1	Base Facility Data Elements: See Table 2.2.2.1-2
Data Requirement 2	Daily Facility Summary Report Elements: See Table 2.2.2.1-3
Data Requirement 3	Patient Data Elements: See Table 2.2.2.1-4
Data Requirement 4	Clinical Data Elements: See Table 2.2.2.1-5
Data Requirement 5	Laboratory and Radiology Test Orders: See Table 2.2.2.1-6
Data Requirement 6	Laboratory/Microbiology Result Data: See Table 2.2.2.1-7
Data Requirement 7	Radiology Result Data: See Table 2.2.2.1-8
Data Requirement 8	Needs a risk analysis of all data elements captured (see data requirements 1-7) to optimize anonymity.

2.2.2.1 AHIC Minimum Dataset Cross-Reference

This Biosurveillance Interoperability Specification is informed and constrained by the data element list provided by American Health Information Community (AHIC). The following tables reflect the data variables provided to HITSP by the AHIC and the Biosurveillance Data Steering Group (BDSG), along

with associated data types and selected terminologies. These tables will be updated in subsequent releases based upon the ongoing work of the AHIC and BDSG. Further specificity regarding the following selected data standards is provided in Appendix 6.3 AHIC Minimum Data Set United States Health Information Knowledgebase (USHIK) Cross-Reference.

Table 2.2.2.1-1 Data Elements Cross Reference

DATA ELEMENTS CROSS REFERENCE	
Data Element	Definition
AHIC Data Element	Data element name/identifier as listed by American Health Information Community and the Biosurveillance Data Steering Group (BDSG)
Definition	Data element description as listed by American Health Information Community and the Biosurveillance Data Steering Group (BDSG)
Data Type	Type of data that is collected with this data element (coded, numeric, text, date/time)
Terminology	Expected data values if data element has finite values. CHI-domain recommendations were followed if available
Comments	Pertinent comments and usage

Table 2.2.2.1-2 Base Facility Data Elements

BASE FACILITY DATA ELEMENTS *[Submitted at baseline and when changes occur]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Facility Identifier	Unique facility identifier	Numeric	CMS IDs	"Organization ID" in HAVE document This is not necessarily a numeric data type
Facility Name	Name of facility	String		"Organization Name" in HAVE document
Facility Location	City and State *[May use FIPS county codes]*	String	FIPS	"Organization Location" in HAVE document City and State are Coded data type
Number of Facility Beds	All facility beds regardless of licensing status	Numeric		Not routinely messaged
Number of Licensed Beds	All facility beds considered licensed in that jurisdiction	Numeric		Not routinely messaged

Table 2.2.2.1-3 Daily Facility Summary Report Elements

DAILY FACILITY SUMMARY REPORT ELEMENTS *[Specific data capture mechanisms may be required without HL7 message structures that support these concepts]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Admissions last 24 hours	Number of admissions to facility in the last 24 hours *[Determine if daily aggregate report prepared by facility or may be calculated by data recipient]*	Numeric		Passed as observation with OASIS/HAVE XML tag: 'Admissions'

DAILY FACILITY SUMMARY REPORT ELEMENTS *[Specific data capture mechanisms may be required without HL7 message structures that support these concepts]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Discharges last 24 hours	Number of discharges from the facility in the last 24 hours *[Determine if daily aggregate report prepared by facility or may be calculated by data recipient]*	Numeric		Passed as observation with OASIS/HAVE XML tag: 'Discharges'
Deaths last 24 hours	Number of deaths recorded at facility in last 24 hours *[Determine if daily aggregate report prepared by facility or may be calculated by data recipient]*	Numeric		Passed as observation with OASIS/HAVE XML tag: 'Deaths'
Clinical Status	Facility's clinical resources are operating: Normal: Within normal limits Level-1: At Level-1 surge conditions Level-2: At Level-2 surge conditions Full: Exceeded; acceptable care cannot be provided to additional patients Diversion or community surge response is required	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag: 'ClinicalStatus' Associated comment may also be passed
Facility Status	Facility resources are operating under: Normal - No conditions exist that adversely affect the general operations of the facility Compromised - General operations of the facility have been affected due to damage, operating on emergency backup systems, or facility contamination Evacuating - Indicates that a hospital is in the process of a partial or full evacuation Closed – Closure; facility no longer capable of providing services and only emergency services/restoration personnel may remain in the facility	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag: 'HospitalFacilityStatus' Associated comment may also be passed
Facility Operations	Status of supplies necessary for facility operations Adequate - Meets the current needs Insufficient – Current needs are not being met	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag: 'FacilityOperations' Associated comment may also be passed
Staffing	Available personnel to support facility operations Adequate - Meets the current needs Insufficient – Current needs are not being me	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag:'Staffing' Associated comment may also be passed

DAILY FACILITY SUMMARY REPORT ELEMENTS *[Specific data capture mechanisms may be required without HL7 message structures that support these concepts]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Decontamination Capacity	Capacity for chemical/biological/ radiological patient decontamination Inactive - Not being used, but available if needed Open - In use and able to accept additional patients Full - In use at maximum capacity Exceeded - Needs exceed available capacity	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag: 'DeconCapacity' Associated comment may also be passed
EMS Traffic Status	Facility capable of: Normal - Accepting all EMS traffic Advisory - Experiencing specific resource limitations which may affect transport of some EMS traffic Closed - Requesting re-route of EMS traffic to other facilities Not Applicable - Not Applicable. This hospital does not have an emergency department	Coded	OASIS/HAVE Values as in definition	Passed as observation with OASIS/HAVE XML tag: 'EMSTrafficStatus' Associated comment may also be passed
EMS Capacity	The number of each triage patient type the hospital can accept triageRed (numeric) triageYellow (numeric) triageGreen (numeric) triageBlack (numeric) commentText (string)	Numeric with text/ comments	OASIS/HAVE Values:	Passed as observation with OASIS/HAVE XML tags: 'CapacityTriageRed' 'CapacityTriageYellow' 'CapacityTriageGreen' 'CapacityTriageBlack' Associated comment may also be passed
EMS Census	The number of each triage patient type the overall hospital currently has triageRed (numeric) triageYellow (numeric) triageGreen (numeric) triageBlack (numeric) commentText (string)	Numeric with text/ comments	OASIS/HAVE Values:	Passed as observation with OASIS/HAVE XML tags: 'CensusTriageRed' 'CensusTriageYellow' 'CensusTriageGreen' 'CensusTriageBlack' Associated comment may also be passed
Adult ICU	Capacity Status for adult ICU beds. *[These can support critically ill or injured patients, including ventilator support. This category includes all major subtypes of ICU beds, including neuro, cardiac, trauma, or medical, with the exception that this category does not include burn ICU beds.]*	Numeric		

DAILY FACILITY SUMMARY REPORT ELEMENTS *[Specific data capture mechanisms may be required without HL7 message structures that support these concepts]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Medical Surgical	Capacity Status for adult medical-surgical beds. *[These are also thought of as ward beds. These beds may or may not include cardiac telemetry capability.]*	Numeric		
Burn	Capacity Status for burn beds. *[These are thought of as Burn ICU beds, either approved by the American Burn Association or self-designated. These beds are NOT to be included in other ICU bed counts.]*	Numeric		
Pediatric ICU	Capacity Status for pediatric ICU beds. *[Similar to adult ICU beds, but for patients 17-years-old and younger.]*	Numeric		
Pediatrics	Capacity Status for pediatrics beds. *[These are ward medical/surgical beds for patients 17-years-old and younger.]*	Numeric		
Negative Flow Isolation	Capacity status for negative airflow isolation beds. *[These provide respiratory isolation. NOTE: This value may represent available beds included in the counts of other types.]*	Numeric		
Available Ventilators	Functional ventilators not in current use	Numeric		

Table 2.2.2.1-4 Patient Data Elements

PATIENT DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes that data are obtained by monitoring HL7 messages]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Pseudonymized Data Linker	A unique, randomly generated, encoded number that links to patient-level information (i.e., name and address) retained at the facility	Alphanumeric		Patient ID/MRN used to create the randomized linker patient ID
Encounter Date/Time	Time of the patient presentation for care. *[Encounter has meaning only for outpatient settings.]**	Date/time field		Expected on ADT^A04 Registration and ADT^A01 Admit transactions HITSP TC does not necessarily agree with the encounter comment
DOB (date of birth)	*[limited to month and year]*	Date field		Proposed definition: "Date of Birth, limited to month and year for privacy purposes" May not be passing DOB for age over 89 due to HIPAA requirements

PATIENT DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes that data are obtained by monitoring HL7 messages]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Age	*[could be calculated]*	Numeric value	Unified Code for Units of Measure (UCUM) for Age Units	Proposed definition: Patient age, which may be calculated from full date of birth before the days are removed
Gender	*[Use standard codeset (e.g., Census)]*	Coded	HL7 2.5 Administrative Sex Codes	Proposed definition: "patient sex" May want to limit to M, F, U
Zip	Home address *[minimum 5 Digit Zip]*	String		Not ZIP plus Four, but will not aggregate to the first 3 characters
State	Home address *[2 character abbreviation]*	String	FIPS State codes	Data type should be coded
Date/time last update	Expected date/time stamp for all registration (ADT) system transactions	Date		

Table 2.2.2.1-5 Clinical Data Elements

CLINICAL DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes 1) data are obtained by monitoring HL7 messages and 2) facility identifier and pseudonymized linker have been associated with the clinical data element record]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Diagnosis/Injury Code	ICD-9 code *[may vary as more information is acquired]*	String	ICD-9/10 CM Or SNOMED CT	Proposed definition: "Diagnosis or diagnoses assigned as a result of the encounter" Industry uses mostly ICD-9 diagnosis codes used for billing purposes The previously available SNOMED CT to ICD 9 CM statistical mapping has been enhanced to include a SNOMED CT to ICD-9-CM rule based reimbursement map. The mapping has been completed and is currently being evaluated by the NLM and vendor community. Further validation will be done by AHIMA

CLINICAL DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes 1) data are obtained by monitoring HL7 messages and 2) facility identifier and pseudonymized linker have been associated with the clinical data element record]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Diagnosis Type	Preliminary, Interim, Final	String	HL7 2.5 Diagnosis Type Codes	Proposed definition: "Type of diagnosis being sent (admitting, working, final)" Data type should be Coded Values are site-defined but typically are "working", "admission", and "final"
Diagnosis Date/Time	*[System time stamp of data entry likely to be only associated date and time+E94]*	Date		Proposed definition: "Date/time the diagnosis was made"
Discharge Disposition	If discharged, place to where patient was released	String	Universal Billing codes (UB-92/NUBC CURRENT UB DATA SPECIFICATIONS MANUAL)	Proposed definition: "Patient's anticipated location or status following the encounter." Data type should be Coded Expected in Discharge transactions only
Patient Class	*Need standardized list –*	String	HL7 2.5 Patient Class Codes	Proposed definition: "General type of patient, *e.g.*, Inpatient, Outpatient, Emergency." Data type should be Coded May want to constrain to Emergency, Inpatient, and Outpatient
Date and Time Illness Onset	Recorded by triage or clinician *[may not be coded value]*	Date		Proposed definition: Date and time of illness onset as recorded by triage or clinician Passed as observation tagged with LOINC code: '11368-8^Illness/Injury Onset Date/time^LN' There is a gap because illness onset date and time is not currently captured in a consistent manner at data sources. It is not always a date/time field and does not lend itself to responses such as "three days" or "two weeks ago"

CLINICAL DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes 1) data are obtained by monitoring HL7 messages and 2) facility identifier and pseudonymized linker have been associated with the clinical data element record]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Chief Complaint	Short description, recorded during triage, for seeking care. *[may have text string or coded (e.g., ICD-9) values]*	String	This HITSP Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT	May be collected as a LOINC-tagged observation: '11292-0^ED Chief Complaint – Patient Reported^LN' Expected to be available with Registration and Admission transactions
Temperature	Record temperature during triage	Numeric	Unified Code for Units of Measure (UCUM) for Temperature units	Passed as observation tagged with LOINC code '8310-5^BODY TEMPERATURE^LN', including timestamp for when it was done
Pulse Oximetry	Record pulse oximetry value during triage	Numeric		Passed as observation tagged with LOINC code: '19960-4^PULSE OXIMETRY^LN' including timestamp for when it was done
Nursing/Triage Notes	Text string written by nurse or healthcare partner *[may have implications for security and privacy]*	String	This HITSP Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT	Passed as observation tagged with LOINC code: '34120-6^INITIAL EVALUATION NOTE^LN'

CLINICAL DATA ELEMENTS *[To be transmitted for each admission, discharge and transfer at a facility. Need to determine if daily messages expected for all hospitalized patients. Presumes 1) data are obtained by monitoring HL7 messages and 2) facility identifier and pseudonymized linker have been associated with the clinical data element record]*				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Provider Identifier	Unique facility-specific provider identifier	Alpha-numeric		Proposed definition: "Unique provider (clinician) identifier. This data element is assumed to meet local biosurveillance needs." Need clarification from AHIC regarding provider role(s): (e.g., attending, primary)

Table 2.2.2.1-6 Laboratory and Radiology Test Orders

The HITSP TC has indicated through the liaison that further specificity is needed to accommodate the request for laboratory and radiology orders. Refer to Radiology/Laboratory Order Message section of Table 4.4-1 Resolution Plan.

LABORATORY AND RADIOLOGY TEST ORDER ELEMENTS [To be transmitted for a subset of all laboratory and radiology tests. Need to determine if messages include all hospitalized patients. Presumes 1) data are obtained by monitoring HL7 messages and 2) facility identifier and pseudonymized linker have been associated with the laboratory/radiology test order element record]				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Order number	Accession number as defined by reporting laboratory *[HITSP may use the term "specimen ID"]*	Alpha-numeric		<scoped out> HITSP TC Comment: This number is usually assigned by the Order Entry system. Order number is NOT the accession or specimen number. GAP: Universally agreed upon meaning of order number; Request clarification from HL7
Test/Procedure Name	Procedure name from reporting laboratory	String		<scoped out> TC Comment: This will be the name of the ordered radiology or laboratory service as the ordering system knows it
Test/Procedure Code		Alpha-numeric	LOINC/DICOM code associated with test/procedure	<scoped out> GAP: Recommend to LOINC, SNOMED-CT, and CPT to develop AND harmonize a suitable coded value set to express order test name and code values

Table 2.2.2.1-7 Laboratory/Microbiology Result Data Elements

LABORATORY/MICROBIOLOGY RESULTS DATA ELEMENTS [To be transmitted for a subset of all laboratory and radiology tests. Presumes: 1) include all hospitalized patients, 2) data are obtained by monitoring HL7 messages 3) accession number, facility identifier, and pseudonymized linker have been associated with the clinical data element record]				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Reporting Laboratory Identifier	Standard national identifier value *[e.g., CLIA or CAP laboratory number]*	Alphanumeric	CLIA Unique Laboratory ID	Proposed Definition: "Identifier for laboratory that is sending the result. This laboratory may be sending results received back from reference laboratories."
Performing Laboratory	Standard national identifier value *[e.g., CLIA or CAP laboratory number]*	Alphanumeric	CLIA Unique Laboratory ID	Proposed Definition: "Laboratory that produced the test result. This may be a reference laboratory identifier."
Report date/time		Date	HL7 Timestamp	Proposed Definition: "Date/time of report"
Report status	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Coded	HL70123 Result Status	Proposed Definition: "Status of report (preliminary, final, corrected)"
Collection date		Date	HL7 Timestamp	Proposed Definition: "Date/time of specimen collection"
Collection method	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Coded	Overlap: HL70488 – Recommend to subset SNOMED-CT for clarification and align subset with Table 488	Proposed Definition: "Method of specimen collection." Not collected that often as a data element for results
Specimen Source	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Coded	SNOMED –CT	Proposed Definition: "Body site of specimen collection." Not collected that often as a data element for results
Specimen	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Coded	HL70487 Specimen or SNOMED-CT	Proposed Definition: "Type of specimen the test was run against." Not collected that often as a separate data element, since the LOINC test code specifies the specimen type as one of the axes
Ordered test code	LOINC code associated with test/procedure	Coded	Recommend SNOMED-CT, LOINC, CPT, HCPCS and others (encouraging commercial vendor participation) get together to establish a suitable vocabulary	Proposed Definition: "The identifier code for the requested observation/test/battery." Major GAP – lack of a universal vocabulary for identifying ordered tests
Resulted test		Coded	LOINC Laboratory Test Identifiers include analytes, specimen source, methods, and sensitivity tests for drugs	Proposed Definition: "The identifier code for the specific test component resulted."

LABORATORY/MICROBIOLOGY RESULTS DATA ELEMENTS [To be transmitted for a subset of all laboratory and radiology tests. Presumes: 1) include all hospitalized patients, 2) data are obtained by monitoring HL7 messages 3) accession number, facility identifier, and pseudonymized linker have been associated with the clinical data element record]				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Result	Includes all test results including susceptibilities, serologies, non-organisms; coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*		Recommend SNOMED-CT	
Method type	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Alphanumeric	V3 Observation Method as a starter set. May be extended locally	Proposed Definition: "Testing method used to arrive at the specific result"
Result unit	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Alphanumeric	Unified Code for Units of Measure (UCUM) Expressions	Proposed Definition: "Unit for numeric result context"
Test interpretation	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	String	HL70078 Abnormal Flags	Proposed Definition: "Interpretation of test result, including the susceptibility test interpretation"
Test status	Coded value *[Need method to convert to a standard codeset, e.g., SNOMED]*	Alphanumeric	HL70123 Result Status	Proposed Definition: "Status of the test result"
Ordering Provider Identifier	Provider of record for the test result that is being reported.	Alphanumeric		Newly added and has not been previously considered

Table 2.2.2.1-8 Radiology Result Data Elements

Note that the AHIC minimum data set did not specify radiology report-specific data elements. These are the ones that the HITSP TC developed.

RADIOLOGY RESULT DATA ELEMENTS				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Study ID/Radiology Number	This is a unique identifier for the radiological study, so that we can link report revisions with the original report. This should be a composite of the accession numbers from the institution and the institution ID	String		Proposed Definition: "Unique identifier for the radiological study, so that report revisions can be linked with the original report"
Study date and time	Date / time the exam was performed	Date/time		Proposed Definition: "Date / time the exam was performed"
Report date/time	Report/Reading Date	Date/time		Proposed Definition: "Report/Reading Date. This date is updated with report corrections and addendums"
Report Status	A flag indicating if this is a revised report with code referencing the study ID. Status of the report (preliminary, final, corrected) is required in a result message	Coded	HL70123 Result Status	Proposed Definition: "Status of the report (preliminary, final, corrected) is required in a result message"

RADIOLOGY RESULT DATA ELEMENTS				
AHIC Data Element	Definition	Data Type	Selected Standards	Comments
Test Performed	Radiology test code/description	Coded	CPT+ Textual Description which can include modification	Proposed Definition: "Radiology test code/description"
Impressions	Radiologist's diagnosis and impressions	Alphanumeric	SNOMED CT Or ICD9-CM	Proposed Definition: "Radiologist's diagnosis and impressions." May be passed as an observation with LOINC tag: '19005-8^X-RAY IMPRESSION^LN'
Date / Time Revised	Date and time of the report revision	Date/time		Proposed Definition: "Date and time of the report revision"

2.2.3 IDENTIFICATION OF BUSINESS ACTORS, AND FUNCTIONAL FLOW SCENARIOS

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

To reflect the nuances of managing the various data types as identified in the AHIC Biosurveillance Use Case, HITSP has defined three separate functional flow scenarios. The Technical Committee has identified two functional flow scenarios for exchanging patient specific data (one message-based and the other document-based) and a third functional flow scenario has been defined for managing resource data. The functional flow scenarios are:

1. Message-based Patient-level Surveillance Data Communication (described in Section 2.2.3.1)
2. Document-based Patient-level Surveillance Data Sharing (described in Section 2.2.3.2)
3. Resource Management Data Transfer (described in Section 2.2.3.3)

Table 2.2.3-1 Business Actors

Business Actor	Description	Functional Flow Scenario
Clinician	In ambulatory and emergency department settings, the healthcare providers within Healthcare Delivery Organizations with direct patient interface in the delivery of care, including physicians, nurses, and clinical supervisors. These business actors are involved in the entry of source data into the system. In the case of reportable conditions, these business actors will also enter supplemental public health data elements into the data capture form.	All

Business Actor	Description	Functional Flow Scenario
Clinical Information Systems (Message Source :Message Sender/ Bio Data Sender, Document Source)	Information system supporting the clinical care and information management for Ambulatory, inpatient, and emergency department settings for organizations, such as hospitals, physician practices, which manage the delivery of care and submission of utilization resource information.	All
Laboratory Information Systems (Message Sender/ Bio Data Sender, Document Source)	Information system supporting the testing, analysis, and information management for laboratory organizations. Medical laboratories, in either in a hospital or ambulatory environment, which analyze specimens as ordered by clinicians to assess the health status of patients. Laboratories, depending on how they are affiliated with hospitals, can be part of either Individual Healthcare Facilities or Integrated Healthcare Data Suppliers. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	1, 2
Radiology Information Systems (Message Sender/ Bio Data Sender, Document Source)	Information system supporting the testing, analysis, and information management for radiology service organizations. Radiology services, depending on how they are affiliated with hospitals, can be part of either Individual Healthcare Facilities or Integrated Healthcare Data Suppliers. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	1, 2
Healthcare delivery organization (Message Sender/ Bio Data Sender, Document Source)	Organizations, such as hospitals, physician practices, which manage the delivery of care and submission of utilization resource information. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	All
Public Health Agencies (local/state/federal) (Message Receiver/ Bio Data Receiver, Document Consumer)	Local, state, and federal government organizations and personnel that exist to help protect and improve the health of their respective constituents. A critical effort under this charge is collecting health information to monitor for the existence of emerging health threats appearing in the population and manage these threats once manifested. Staff of these agencies interacts with the BIS to verify and validate system indications of public health threats, and to assert acknowledgements that may be required by system processes.	All
Inpatient Healthcare delivery organization (Data Source System)	Organizations, such as hospitals, Skilled Nursing Facilities, and other inpatient healthcare providers, which manage the delivery of care and submission of utilization resource information.	3
Regional Capture Center (Data Source System)	Network or collaborative of regional inpatient healthcare delivery organizations utilizing a common service to capture and forward on resource availability information to BIS Emergency Operations Centers. This may be a service facilitated by a RHIO/HIE.	3

Business Actor	Description	Functional Flow Scenario
Emergency Operations Center (Biosurveillance System)	Local, state, and federal government organizations and personnel that exist to help protect and improve the health of their respective constituents. A critical effort under this charge is collecting health information to monitor for the existence of emerging health threats appearing in the population and manage these threats once manifested.	3

2.2.3.1 Functional Flow Scenario 1: Message-Based Patient-level Surveillance Data Communication Overview

The first functional flow scenario, Message-Based Patient-level Surveillance Data Communication, is a mechanism to automate the communication of near real-time message-based data from the clinical care provider to the Biosurveillance Information System through integration with the local clinical information system. This approach leverages the traditional message-based communications, typically facilitated through an organization's interface engine, to capture messages of interest to public health surveillance and to transmit these messages to a designated recipient. If multiple recipients are to be supported, they have to be configured at each of the sources or an infrastructure duplicating these messages needs to be managed with knowledge of these destinations. The clinical information sources in this functional flow scenario send anonymized and pseudonymized clinical messages to support public health surveillance needs. This is intended to enable communication of this message data in near-real-time and within 24 hours for a use by Biosurveillance systems (BIS). The BIS provides support to, clinicians, epidemiologists and case managers to identify and manage public health threats using data received from the clinical information systems. See figure 2.2.4-1 for a high level sequence diagram of the primary actor interactions for this functional flow scenario.

Message-based Advantages

- It leverages an approach that is utilized for information sharing which is currently functional in hospitals and Emergency Departments such that data can be submitted for biosurveillance efforts using existing mechanisms of data transfer
- Existing healthcare message-based transmission standards provide a baseline for the interpretation of the data in aggregate for Syndromic surveillance and situational awareness
- The basic data submission standards, through harmonization, provide a reasonable incremental approach to provide public health with required data elements

Message-based Disadvantages

- Ambulatory systems have variable penetration of message-based data transmission capabilities. A single methodology for managing information sharing from resource-challenged ambulatory facilities is preferable and alignment with patient record-sharing initiatives is beneficial

This functional flow scenario includes the specification of multiple biosurveillance messages to capture data from healthcare providers and laboratory systems, which contain data that can be used by the

epidemiologist to assess the health of the population. Operationally, they are typically collected at any point in time, including admission, clinical order, transfer or discharge. These exchanges are conducted over secured communications between trusted nodes; however the HITSP Biosurveillance Interoperability Specification does not specify the transport mechanisms. Audit logs are updated to capture the disclosure and receipt of the data. Consistent time services are implemented to enable meaningful audit tracking across the systems involved in the exchanges. Consent directives are leveraged to indicate that the disclosures were authorized under policies indicating the public health authorization. Entity identity assertions are leveraged as needed to comply with jurisdictional or Regional Health Information Organization (RHIO)/Health Information Exchange (HIE) policy.

While it is anticipated that information sources and content will expand for biosurveillance purposes, in support of the current Use Case, the following types of clinical messages are defined:

- Laboratory Orders
- Laboratory Results including preliminary, interim, and final results
- Encounter Messages from Electronic Medical Records Systems
- Radiology Orders
- Radiology Results

Pre-existing information contained in clinical orders may be used as early warning indicators for events of public health significance. Because clinical orders contain information describing patients and the types of clinical tests requested, the Biosurveillance Use Case for laboratory and radiology orders seeks to “re-use” this pre-existing information, and consequently represents a “secondary” use of such data.
The Biosurveillance Use Case is dependent on the primary Use Case developed for Laboratory and Radiology ordering. The selection of messages to be used for Laboratory and Radiology orders should be driven by the primary Use Case for orders, not a more limited secondary Biosurveillance Use Case. Consequently, we advocate that Biosurveillance should not dictate the order message(s) used to convey Laboratory and Radiology orders. Rather, the Biosurveillance work group should ensure that the information necessary for public health surveillance is included in order messages. HITSP propose that any preliminary document developed for the Biosurveillance Use Case would maximally identify candidate messages that could contain the information of interest, and the location of the desired information in each transaction.

Also of crucial importance is that the most common order message used for both Laboratory and Radiology orders today (the ORM^O01) has been temporarily retained for backward compatibility, but not recommended for use in HL7 2.5. Subsequently, the HL7 2.5 order messages that may be selected by HITSP may *not* be the most universally implemented message for orders. For Biosurveillance to take advantage of the information found in orders, focus should be on where surveillance information can be found in a variety of order message types, not just a single order message type that is dictated for a Biosurveillance Use Case.

To be broadly applicable, the Biosurveillance Use Case should leverage clinical order transactions commonly exchanged among clinical healthcare stakeholders, as well as public health entities. It should

be noted that the laboratory order message selected by PHIN is intended for a narrow Use Case for messaging orders between public health laboratories, which has limited application to the Biosurveillance and Electronic Health Record Use Cases.

2.2.3.1.1 Message-based option 1: Laboratory order message

This functional flow scenario option involves generation of laboratory order messages from clinical healthcare provider systems.

The pre-conditions assume the existence of the secure transport mechanisms and that an order for laboratory testing has been entered into the clinical information system that is within the category of interest for biosurveillance reporting as required by federal, state or local health departments. It is also assumed that the healthcare provider information system is able to generate standard terminology. This option defines the content of the message to be delivered over that transport to communicate laboratory orders defined to be of interest to the public health authorities for biosurveillance purposes. An assumption is made that the healthcare provider has a computer information system with capability to capture the information required to generate the message.

The specific data elements managed by the provider clinical information system are expected to be the source for the information used in creating the biosurveillance laboratory order message. A variety of clinical information system implementations and usage by clinicians may result in some variability in the content of the biosurveillance laboratory order message.

There is no HITSP specification provided for the laboratory order message option.

2.2.3.1.2 Message-based option 2: Laboratory results message including preliminary, interim, and final results

This functional flow scenario option involves generation of laboratory result messages from Laboratory Information Management systems (LIMS).

The pre-conditions assume a laboratory has processed a sample and the test result is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. It is also assumes that the healthcare provider information system is able to generate standard terminology. This option defines the content of the message to be delivered over that transport to communicate laboratory results defined to be of interest to the public health authorities for biosurveillance purposes. An assumption is made that the laboratory has a LIMS system with capability to capture the information required to generate the message.

The specific data elements managed by the laboratory's LIM are expected to be the source for the information used in creating the biosurveillance message. A variety of LIMS implementations and usage by clinicians may result in some variability in the content of the biosurveillance message.

The detailed content of the biosurveillance report to support this Use Case will be detailed as part of the HITSP Component specification (See *HITSP/C36 Lab Result Message*).

2.2.3.1.3 Message-based option 3: Encounter messages from Electronic Medical Records (EMR) Systems

This Use Case involves a generation of encounter summary messages from clinical healthcare provider systems.

The pre-conditions assume a patient has presented to a healthcare provider. After examination and evaluation of the patient condition, the provider (or provider EMR) determines that the case is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. An assumption is made that the provider has an EMR system with capability to capture the information required to generate the message.

The specific data elements managed by the provider EMR are expected to be the source for the information used in creating the biosurveillance message. A variety of EMR implementations and usage by clinicians may result in some variability in the content of the biosurveillance message.
The detailed content of the biosurveillance encounter message to support this Use Case will be detailed as part of the HITSP Component specification (See *HITSP/C39 Encounter Message Component*).

2.2.3.1.4 Message-based option 4: Radiology order messages

This functional flow scenario option involves generation of radiology order messages from clinical healthcare provider systems.

The pre-conditions assume the existence of the secure transport mechanisms, and that an order for radiology testing has been entered into the clinical information system that is within the category of interest for biosurveillance reporting as required by federal, state or local health departments. It is also assumed that the healthcare provider information system is able to generate standard terminology. This option defines the content of the message to be delivered over that transport to communicate radiology orders defined to be of interest to the public health authorities for biosurveillance purposes. An assumption is made that the healthcare provider has a computer information system with capability to capture the information required to generate the message.

The specific data elements managed by the provider clinical information system are expected to be the source for the information used in creating the biosurveillance laboratory order message. A variety of clinical information system implementations and usage by clinicians may result in some variability in the content of the biosurveillance radiology order message.

There is no HITSP specification provided for the radiology order message option.

2.2.3.1.5 Message-based option 5: Radiology result messages

This functional flow scenario option involves generation of Radiology Result messages.

The pre-conditions assume a radiology clinic has processed a sample, and the interpretation is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. It is also assumed that the healthcare provider information system is able to generate standard terminology. This option defines the content of the message to be delivered over the transport to communicate radiology results defined and are of interest to the public health authorities for biosurveillance purposes. An assumption is made that the radiology system will have the capability to capture the information required to generate the message.

The specific data elements managed by the radiology system are expected to be the source for the information used in creating the biosurveillance message. A variety of radiology system implementations and usage by clinicians may result in some variability in the content of the biosurveillance message.

The detailed content of the biosurveillance report to support this Use Case will be detailed as part of the HITSP Component specification (See *HITSP/C41Radiology Result Message).*

2.2.3.2 Functional Flow Scenario 2: Document-based Patient-level Surveillance Data Sharing (Biosurveillance Documents) Overview

The second functional flow scenario, Document-based Patient-level Surveillance Data Sharing (Biosurveillance Documents), is the shared document resource data submission model. This approach leverages a shared registry and repository resource to which the clinical information sources can send anonymized and pseudonymized biosurveillance documents to support public health surveillance needs. This is intended to enable sharing of these documents in near-real-time and within 24 hours for use by Biosurveillance systems, clinicians, epidemiologists and case managers to identify and manage public health threats. See Figure 2.2.4-2 for a high level sequence diagram of the primary actor interactions for this functional flow scenario.

Document-based information sharing is included in this Interoperability Specification to align and maintain consistency with other HITSP efforts in Electronic Health Record and Consumer Empowerment. The document-based information sharing approach has not previously been considered for secondary use of data as required by Biosurveillance or other secondary use systems (e.g., clinical trials, aggregate performance measurements, disease management and population health). The Technical Committee identified several areas for further evaluation prior to endorsing full document-based data sharing for Biosurveillance activities. These areas identified for evaluation include:

- Methodology and criteria for publish and subscribe capability such that subscription filtering can be modified in real time as the situation requires
- Document Sharing Service requirements to meet the needs of public health and potentially other forms of secondary data use

- Extent of usable information within documents; i.e., structured vs human readable text and the extent of natural language processing required to enable document sharing as a viable Biosurveillance solution
- Extent to which document-based sharing encapsulates message-based standards that correlate with the message-based functional flow as detailed elsewhere in this document

Implementation sites are encouraged to explore and research these areas of concern to provide additional evidence for more robust usage of document-based information sharing for secondary usage of data.

This functional flow scenario offers several advantages and disadvantages.

Document-based Advantages

- It leverages an emerging approach of sharing patient care clinical document and as such, could facilitate the capture of information from source systems, especially in the ambulatory setting
- A shared document resource could provide access to regional information allowing authorized neighboring public health authorities access to patient care clinical documents when there is a need to extend investigative and monitoring actions across public health jurisdictions
- Since many local public health departments have limited computing resources, this offers a means by which these stakeholders can leverage patient care clinical documents to support a largely manual approach to biosurveillance with minimal additional investment
- By providing a resource that maintains persistent, human readable documents, support for case investigation can be offered

Document-based Disadvantages

- HL7 Clinical Document Architecture (CDA R2) is required for more fully structured content within the document; it has not yet been implemented
- The intent of the document-based information is to facilitate the sharing of human readable transfer of care information between providers
- These documents are not tailored for Biosurveillance; the Use Cases for which document-based data sharing have been developed are based on sharing of data about individual patients from one provider to another
- End of encounter submission of documents for hospital admissions, and to some extent Emergency Departments, would be compiled too late to meet the Biosurveillance Use Case requirement for Syndromic surveillance and situational awareness
- A document share must enable publish and subscribe capability to allow public health useful access to required information
- Hospitals and Emergency Departments have existing message-based data transmission capabilities that can be leveraged in the near term
- Document-based transmission is not in general use by healthcare organizations and requires significant additional resource expense with limited additional benefit to the facility

Pre-conditions include configuration of communication and identification of communication exchanges partners. This functional flow scenario includes the specification of multiple Biosurveillance documents, which form a class of clinical documents that contain information and data that can provide the epidemiologist with sufficient data on the health of the population. Operationally, they can be created at any point in time, including admission, clinical order, transfer or discharge. These exchanges are conducted over secured communications between trusted nodes. Audit logs are updated to capture the disclosure and receipt of the data. Consistent time services are implemented to enable meaningful audit tracking across the systems involved in the exchanges. Consent directives are leveraged to indicate that the disclosures were authorized under policies indicating the public health authorization. Entity identity assertions, document integrity, access control and nonrepudiation are leveraged as needed to comply with jurisdictional or RHIO/HIE policy.

While it is anticipated that information sources and content will expand for biosurveillance purposes, in support of the current Use Case, the following types of clinical Biosurveillance Documents should be collected:

- Laboratory Results Documents, including preliminary, interim, and final result documents
- Encounter summaries from Electronic Medical Records Systems (including orders for laboratory and radiology testing)
- Radiology Results Documents, particularly interpretation reports

Because content, business rules and electronic capture of data from LIMS and EMRs differ significantly, these are defined as separate functional flow scenario options. Users or implementers of this functional flow scenario are offered several options.

2.2.3.2.1 Document-based option 1: Submission of Laboratory Biosurveillance Document

This functional flow scenario option involves a submission of laboratory biosurveillance documents from a laboratory to a Biosurveillance Information System. This functional flow scenario option is a central component of routine public health reporting processes, which typically requires an established trusted communication channel prior to the actual transfer of biosurveillance documents being initiated.

The pre-conditions assume a laboratory has processed a sample, and the test result is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. The laboratory is also assumed to have a LIM system that can capture the information required to generate the document.

The specific data elements managed by the laboratory LIM system are expected to be the source for the information used in creating the biosurveillance document. A variety of LIM implementations and usage by clinicians may result in some variability in the content of the biosurveillance document.

Detailed contents of the biosurveillance report to support this Use Case are included in the HITSP/C37 Lab Report Document Component Specification.

2.2.3.2.2 Document-based option 2: Submission of EMR-Generated Biosurveillance Document

This Use Case involves a submission of healthcare provider generated biosurveillance documents from a Hospital/ED/Ambulatory clinic to a Biosurveillance Information System (BIS).

The pre-conditions assume a patient having presented to a healthcare provider. After examination and evaluation of the patient condition, the provider (or provider EMR) determines that the case is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. An assumption is made that the provider has an EMR system with capability to capture the information required to generate the report.

The specific data elements managed by the provider EMR are expected to be the source for the information used in creating the biosurveillance report related to this reportable condition. A variety of EMR implementations and usage by clinicians may result in some variability in the content of the biosurveillance report.

The detailed content of the biosurveillance report are in accordance with HITSP/C48 Encounter Document Using IHE Cross-Enterprise Document Sharing Medical Summary (XDS-MS) Component subject to the constraints listed in Section 3.1.2 of this document.

2.2.3.2.3 Document-based option 3: Submission of Radiology Result Biosurveillance Document

The AHIC Use Case includes capture of Radiology Results. This functional flow scenario option involves a submission of radiology result biosurveillance documents from radiology systems to a Biosurveillance Information System. While this functional flow scenario option is not a central component of routine public health reporting processes existing work will be leveraged to accommodate this document type.
The pre-conditions assume a radiologist has captured the data of interest and provided an interpretation of that data into the radiology information system and the test result is within the range and category of interest for biosurveillance reporting as required by federal, state or local health departments. An assumption is made that the radiologist has a system with capability to capture the information required to generate the document.

The specific data elements managed by the radiology system are expected to be the source for the information used in creating the biosurveillance document. A variety of radiology information system implementations and usage by clinicians may result in some variability in the content of the biosurveillance document.

Until further specification requirements are defined to enable additional constraints, the Radiology Result Biosurveillance Document references IHE Cross-Enterprise Document Sharing for Imaging (XDS-I) Integration Profile without further constraint as described by the HITSP/TP49 Sharing Radiology Results Transaction Package.

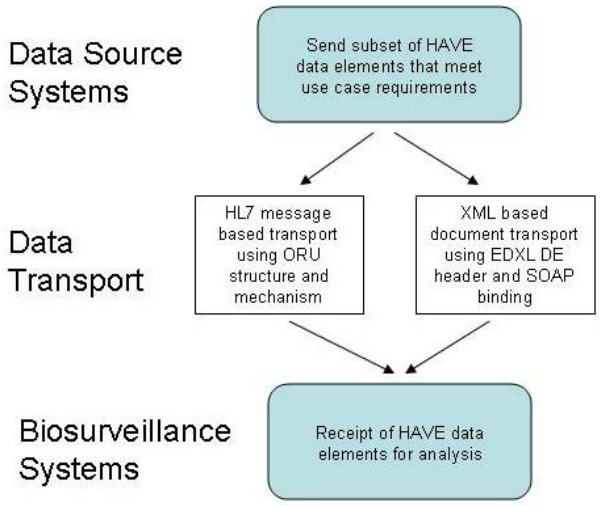
2.2.3.3 Functional Flow Scenario 3: Resource Management Data Transfer (Document-based and Message-based) Overview

The third functional flow scenario provides a mechanism to automate the communication of resource availability from a resource provider to a resource management information service. In this Use Case, utilization data only goes to Public Health Authorities. See Figure 2.2.4-3 for a high level sequence diagram of the primary actor interactions for this functional flow scenario.

HITSP has identified a need for both data element definition and a messaging schema to support the exchange of information for reporting the utilization and availability of hospitals and health resources. HITSP is informed by the harmonized Biosurveillance Use Case provided by AHIC. HITSP is further informed with regard to the desirable set of data elements relevant to this purpose by the Biosurveillance Data Steering Group which in turn reports to the Biosurveillance Work Group of the AHIC.

With regard to the messaging approach to support the exchange of hospital and health resource availability information HITSP recommends that either of two acceptable specifications be utilized as illustrated in Figure 2.2.3.3-1.

Figure 2.2.3.3-1 Information Flows for Bed Availability



The two specifications are the Emergency Data Exchange Language Distribution Element (EDXL-DE) version 1.0 for information exchange in an XML/SOAP/Web Services environment or the HL7 version 2.5 Observation Result Unsolicited (HL7 ORU) message constrained to transmit the Hospital Availability Exchange (HAVE) format dataset. These exchanges are conducted over secured communications between trusted nodes. Audit logs are updated to capture the disclosure and receipt of the data. Consistent time services are implemented to enable meaningful audit tracking across the systems involved in the exchanges. Entity identity assertions, document integrity, access control and nonrepudiation are leveraged as needed to comply with jurisdictional or HIE policy.

2.2.3.3.1 Resource management option 1: Generation of bed availability document

This functional flow scenario option involves generation of a bed resource availability document from the healthcare provider environment. This document is defined specifically to represent the characteristics and breadth of specificity desired for optimal use by Emergency Operations Centers. This information may be generated through manual input, or from existing systems or from a combined integrated system with supplemental data entry.

The pre-conditions assume the existence of the secure transport mechanisms, and that the bed availability data are available to the system and/or individual generating the resource availability data. This option defines the content of the document to be delivered over the transport to communicate bed availability documents that are defined.

An assumption is made that the healthcare provider has a computer information system with capability to capture the information required to generate the document. No assumption is made as to the source of the bed availability information. A variety of administrative classifications for bed type, provider specialty and usage by provider organizations may result in some variability in the content and detail of the bed availability document.

The detailed content of the associated bed availability document to support this Use Case is detailed as part of the HITSP/C47 Resource Utilization Message Component.

2.2.3.3.2 Resource management option 2: Generation of bed availability message

This functional flow scenario option involves generation of bed availability messages from inpatient healthcare provider administrative systems.

The pre-conditions assume the existence of the secure transport mechanisms and that the bed availability data are available to the system generating the resource availability data. This option defines the content of the message to be delivered over that transport to communicate bed availability documents defined. An assumption is made that the healthcare provider has a computer information system with capability to capture the information required to generate the message.

It is assumed that the bed availability message will be captured from the organization admitting/discharge system. A variety of administrative classifications for bed type, provider specialty and usage by provider organizations may result in some variability in the content and detail of the bed availability document. The detailed content of the associated bed availability document to support this Use Case will be detailed as part of the HITSP/C47 Resource Utilization Message Component.

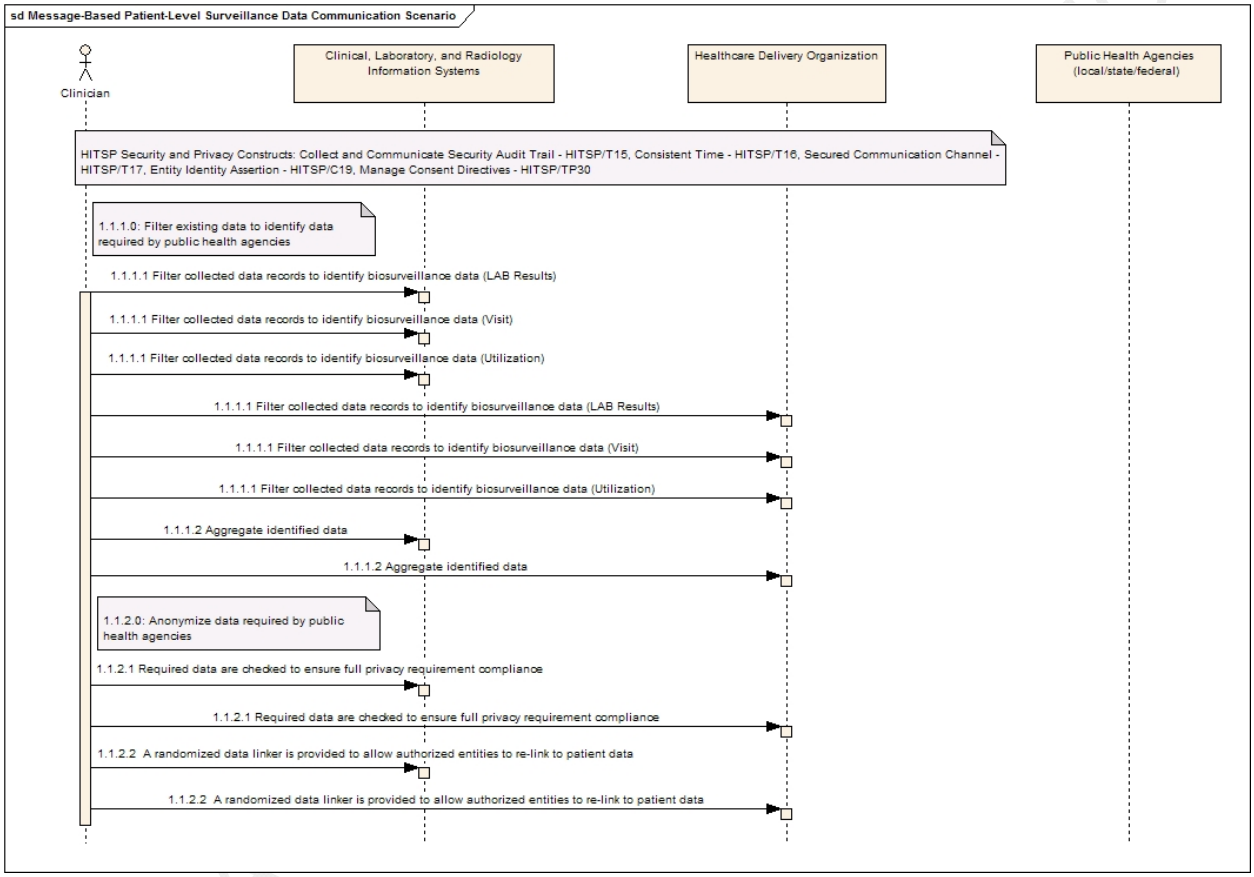
2.2.4 HIGH-LEVEL UML BUSINESS SEQUENCE DIAGRAM

This section contains an explanation of the relationship between the business actors and data interactions between the primary actors and alternative actors for the Use Case. The diagrams that follow

illustrate the Use Case with a representation of a normal sequence of exchange between the primary actors.

Figure 2.2.4-1 shows the Use Case events for the message-based patient level biosurveillance data communication functional flow scenario. This functional flow scenario is described in detail in Section 2.2.3.1.

Figure 2.2.4-1 Biosurveillance Business Sequence Diagram for Message-based Patient-level Surveillance Data Communication



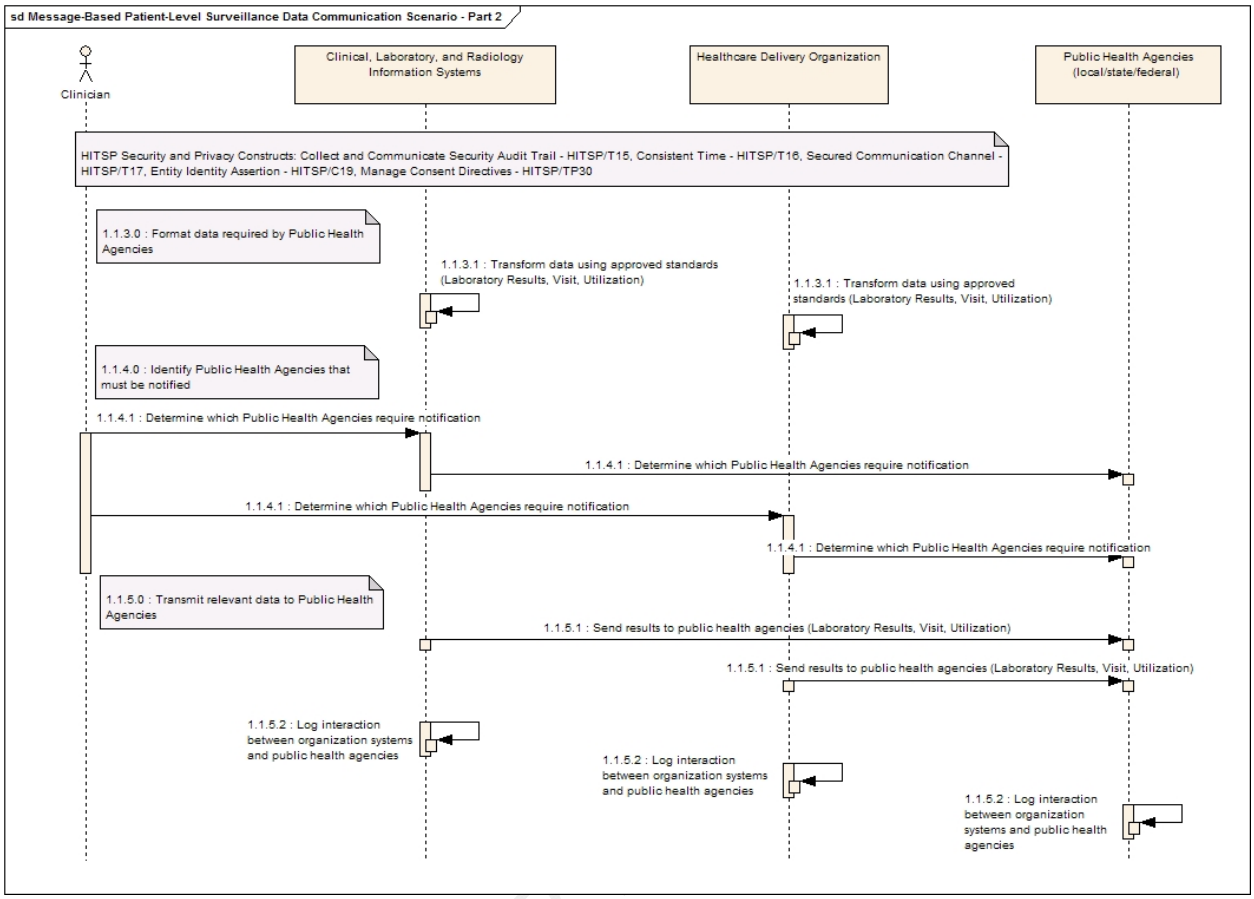
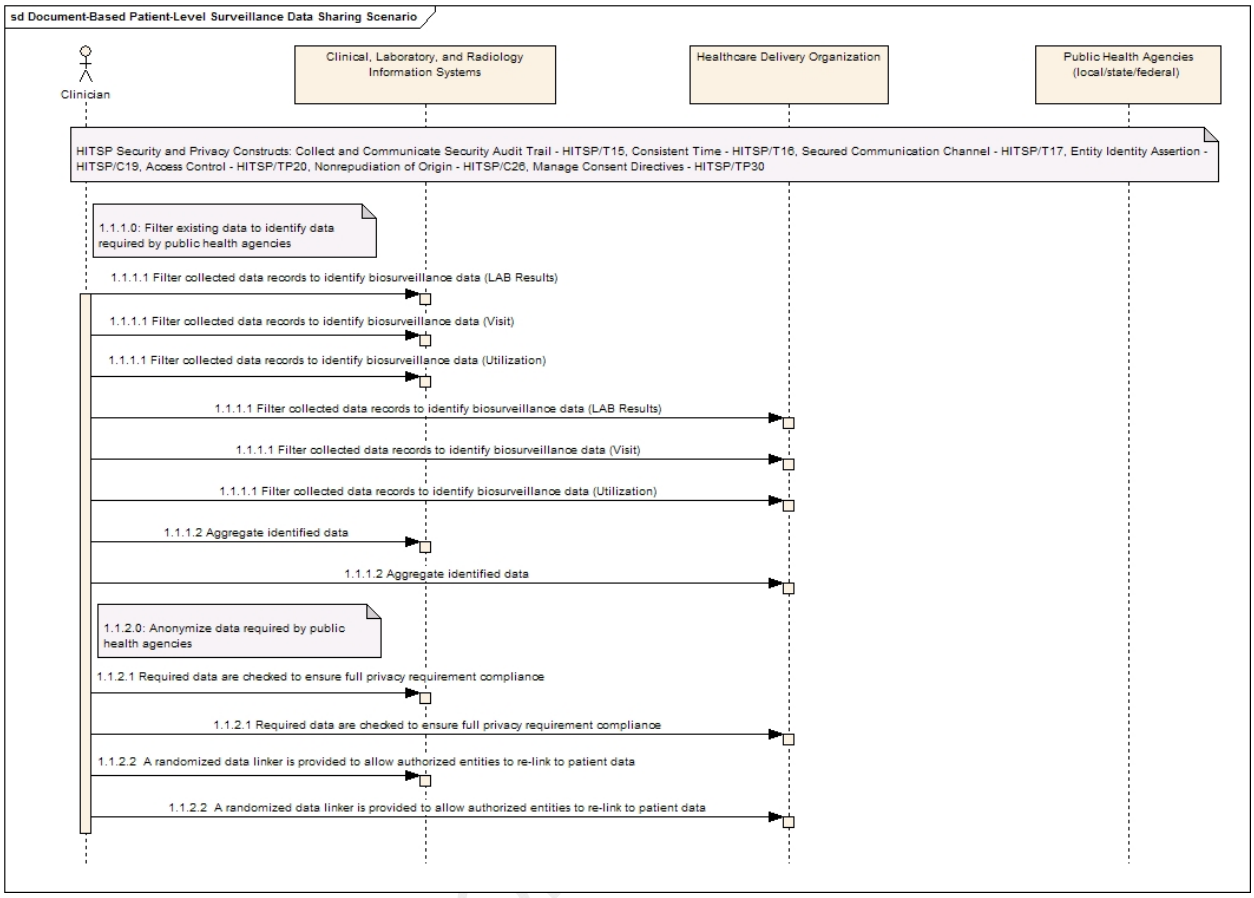


Figure 2.2.4-2 shows the Use Case events for the document-based patient-level biosurveillance data communication functional flow scenario. This functional flow scenario is described in detail in Section 2.2.3.2.

Figure 2.2.4-2 Biosurveillance Business Sequence Diagram for Document-based Patient-level Surveillance Data Sharing



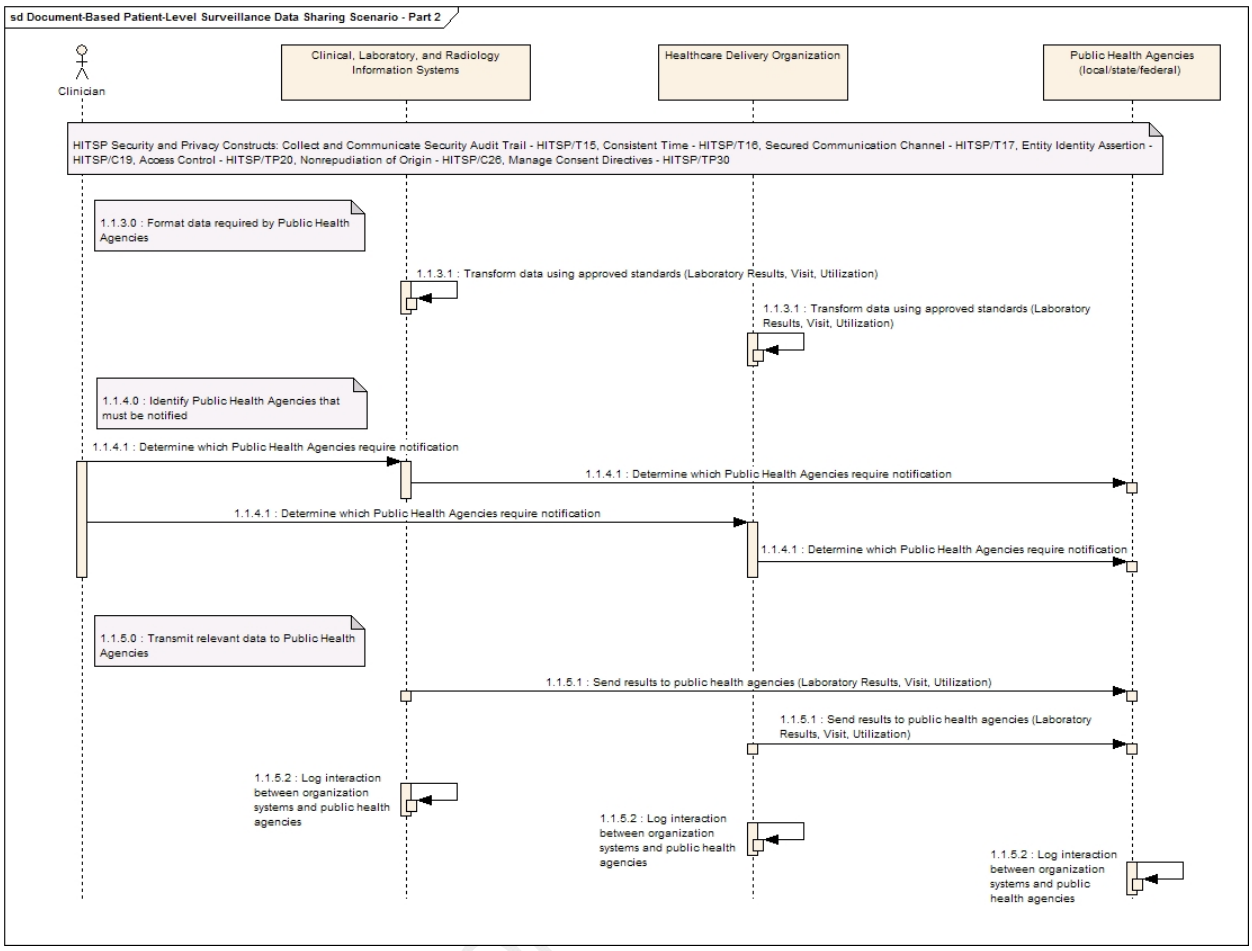
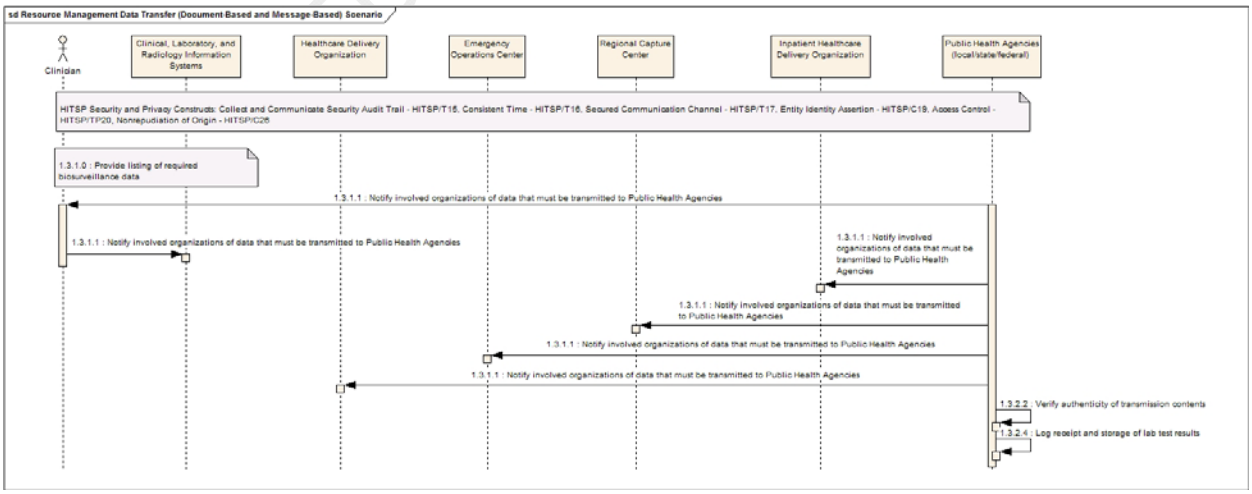
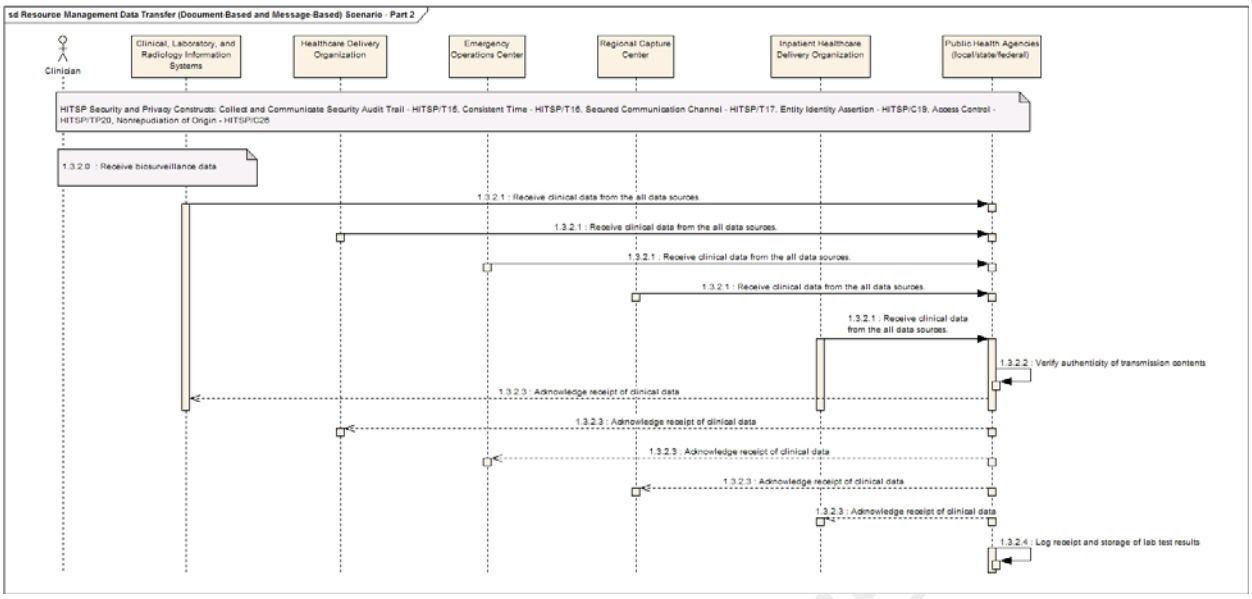


Figure 2.2.4-3 shows the Use Case events for the resource management data transfer functional flow scenario. This functional flow scenario is described in detail in Section 2.2.3.3.

Figure 2.2.4-3 Biosurveillance Business Sequence Diagram for Resource Management Data Transfer





3.0 DESIGN

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

3.1 SCOPE OF DESIGN

This section describes the scope of the design as it relates to the requirements for this Use Case that were identified in Section 2.2 above. The scope identifies the assumptions that provide the boundaries for the specification and the constraints that limit the use of the specification. In addition, any pre-conditions, post-conditions and triggers that underlie the interactions between the various actors, data and transactions are provided.

The AHIC Biosurveillance Use Case that defines the scope of this Interoperability Specification describes the process or interaction that each primary stakeholder will invoke in the capture, discovery, anonymization and transmission of relevant data.

The scope addressed in this document is the transmission of essential data from inpatient and ambulatory care and emergency department visits, resource utilization, and laboratory result data from electronically enabled healthcare delivery and public health systems in a standardized and anonymized format, to authorized Public Health Agencies with less than one day lag time. While the system and processes ultimately must also support the ability for authorized public health personnel to go back to the data source to seek to re-link the anonymized biosurveillance data to the data source as part of an appropriate public health investigation, such re-linking has been deferred for future effort and is not addressed in this IS. The anonymization and pseudonymization processes may require product engineering and external calls not specified in this document. This document will not specify where these calls are to be made in order to remain architecturally neutral.

The management of data to ensure proper routing, security, privacy, and timely reporting is critical to enabling biosurveillance activities. Potential architectural solutions to data flow issues include using individual facility data sources (e.g., single hospitals or ambulatory care sites) or networked system such as a multi-facility system or supporting organization that uses data in the course of providing other services and sends data to all appropriate public health agencies. Other permutations of these two models can also be considered. The role of the data or network system can be accomplished by several different stakeholders, including hospital systems, health plans, independent laboratories and other possibilities. However, this IS was defined to be independent of architecture choice and is intended to support any variant of the architectural choices identified above.

CLINICAL EXAMPLES

To maintain context and perspective, HITSP approached the creation of an Interoperability Specification using clinical example scenarios as shown in Table 3.1-1 below.

Table 3.1-1 Clinical Example Scenarios

National Planning Scenarios	
1	Nuclear detonation – 10–Kiloton Improvised Nuclear Device
2	Biological Attack – Aerosol Anthrax
3	Biological Disease Outbreak – Pandemic Influenza
4	Biological Attack – Plague
5	Chemical Attack – Blister Agent
6	Chemical Attack – Toxic Industrial Chemicals
7	Chemical Attack – Nerve Agent
8	Chemical Attack – Chlorine Tank Explosion
9	Natural Disaster – Major Earthquake
10	Natural Disaster – Major Hurricane
11	Radiological Attack – Radiological Dispersal Devices
12	Explosives Attack – Bombing Using Improvised Explosive Devices
13	Biological Attack – Food Contamination
14	Biological Attack – Foreign Animal Disease (Foot and Mouth Disease)
15	Cyber Attack

These examples were consistent with the 15 National Planning Scenarios created by the U.S. Department of Homeland Security. Specific attention was given to biological attack with aerosol anthrax (#2 above) and biological disease outbreak with pandemic influenza (#3 above). To establish utility of interoperability for routine public health syndromic surveillance and situational awareness efforts, sexually transmitted disease (Chlamydia) and food-borne illness (Salmonella) were considered among clinical examples.

HITSP has developed this Interoperability Specification in conformance with the AHIC Biosurveillance Use Case to the extent that there are current standards and options with which to accomplish the requirements set forth in that Use Case. HITSP has further worked in parallel with the AHIC Biosurveillance Data Steering Committee to adopt the initial work from the newly formed group to inform the work of this Interoperability Specification.

Section 3.1.2 describes security constraints that are specified to fulfill the security requirements of the Use Case and to enable conformance to possible additional policy restrictions.

.

Although the Use Case specifies a requirement for anonymization, some Biosurveillance systems may be exempt from such requirements due to Public Health Law, contracts, or legal agreements. This specification utilizes the Pseudonymization Service to implement the Randomized Data Linker functionality. In some cases today, pseudonymization has been done as a cross-reference table at the data source. This, however, can pose a burden on the data source system. As such, HITSP recommends establishing regional and/or national services for patient pseudonymization for biosurveillance. This would allow:

- Tracking of patients across institutions for better Biosurveillance reporting or analysis
- A reduction in duplicate counts
- A reduction in the work effort on any individual sending system

While this is not yet pervasively available, we recommend this as a roadmap to accomplish this goal.

There are a number of challenges related to automated capture of biosurveillance data that have been considered in the development of this specification. Because the biosurveillance capture relies on routine processes, the ability to require conformance with the specified formats is limited to the organization's ability to comply with those formats. As such, the requirements are somewhat less prescriptive than those that are associated with clinical systems integration.

The HITSP recognizes that current systems used by stakeholders with an interest in resource availability data may differ from systems used for individual patient information. Therefore, Interoperability Specifications that support resource utilization also differ from those primarily concerned with patient specific data.

3.1.1 ASSUMPTIONS

This section provides an overview of the assumptions, including the circumstances, actors, policies and/or technologies that need to be in place for the design to be completed as specified. Assumptions are different from constraints which are specifically used to narrow the definition or indicate limitations of the specified interactions.

Table 3.1.1-1 Assumptions

Assumption	Use Case Scenario
Security/communications policies between institutions are established using established standards for trust management, risk assessment and cross-jurisdiction information exchange.	N/A
Standards will differ by data source (Lab, Visit, Resource Utilization (Utilization))	N/A
Machine-generated Radiology Results are included in data requirements for Lab Results	N/A
Re-identification as needed is authorized for public health authorities	N/A
Visit data are likely to be supplied through the admitting/registration system	N/A
Transformation includes formatting data into a message and content mapping	N/A
Standards will differ by data source (Lab, Visit, Utilization)	N/A

Assumption	Use Case Scenario
Machine-generated Radiology Results are included in data requirements for Lab Results	N/A
A separate response is sent from the BIS to the originating source indicating that a person or automated process has reviewed the data. This is more than an application acknowledgment that the data was received	N/A
Architecture of BIS system will in part dictate the security and access	N/A
Security standard selection must be done in accordance with HIPAA and based upon the risk assessment for the selected architecture	N/A

3.1.2 CONSTRAINTS

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

Table 3.1.2-1 Constraints

Constraint	Functional Flow Scenario
AHIC Data Steering Committee Data set: See AHIC Minimum Data Set Cross-reference table in Data Requirements Section	All
AHIC Biosurveillance Use Case	All
Message constraints: HITSP/C36 - Lab Result Message HITSP/C39 - Encounter Message HITSP/C41 - Radiology Results message	1
Document constraints: HITSP/C37 - Lab Report Document Component HITSP/C48 - Encounter Document HITSP/TP49 - Sharing Radiology Results	2
Vocabulary Constraints: Laboratory Terminology See AHIC Minimum Data Set Cross-reference table in Data Requirements Section Bed Availability Data Elements constrained to HAVE	All
The policy of the implementation environment MAY require the HITSP/C19 Entity Identity Assertion. This enables those policies that would require audit logs identifying the end user. It also enables authorization decisions where the privilege to conduct the associated transaction is determined based upon the entity identity	All
The policy of the implementation environment MAY require HITSP/C26 Nonrepudiation. This enables those policies that would require nonrepudiation for domain transactions	All
The policy of the implementation environment MAY require the HITSP/TP20 Access Control. This enables those policies that would require the bio-message receiver or the document consumer to be subject to implementation-defined access control rules	All

Constraint	Functional Flow Scenario
The policy of the implementation environment MAY require HITSP/TP30 Manage Consent Directives where the policy under which the document is published references the appropriate legal citation. This enables those policies that would require tracking of authorized disclosures of biosurveillance information	All

Additional constraint considerations are provided in the following sections. These are specific to the functional flow scenarios, and the applicable implementation option.

3.1.2.1 Functional Flow Scenario 1: Message-Based Patient-level Surveillance Data Communication Constraints

The Message-Based Patient-level Surveillance Data Communication functional flow scenario leverages the common messaging approach used in intra-organizational communications. A number of constraints are added as part of this Interoperability Specification so as to assert common content and assure authenticity of transmission contents. These constraints address privacy protection, authenticity and message content.

In support of this functional flow scenario, this Interoperability Specification provides constraints to the Use Case for those topics that merit significant additional biosurveillance workflow and semantic interoperability consideration. These key constraints are with respect to terminology and support for content specification for the varying reportable conditions forms required by state public health departments to collect supplemental data relevant to support detection and monitoring of public health threats for the local environment. Some of these areas need additional consideration and in some cases harmonization efforts before HITSP can fully specify a robust implementation. While this specification defines the fit for these constructs, detailed specification in some cases will be deferred to enable sufficient consideration for the complexity of the subject matter. It is also assumed that the healthcare provider information systems are able to translate local codes into standard terminology.

3.1.2.1.1 Transmission Option: Retrieve Form for Data Capture (HITSP/TP50: Retrieve Form for Data Capture Transaction Package)

In support of public health authority reportable conditions monitoring and management, the clinical or laboratory information source may optionally implement the Retrieve Form for Data Capture Transaction Package. This option allows for capture of supplemental data variables not typically maintained in an electronic health record or laboratory information system through a more seamless integration with the local information system. This option allows for the local system to retrieve a form specific to the identified potential public health threat. This is one option currently available for reportable conditions which may need additional local configuration and architectural constraints or considerations for implementation architectures.

3.1.2.2 Functional Flow Scenario 2: Document-Based Patient-level Surveillance Data Communication Constraints

The Document-Based Patient-level Surveillance Data Communication functional flow scenario leverages the shared document resource approach common to each of the current HITSP Use Cases. The use of this type of shared resource for biosurveillance differs from the use of the resource to support sharing of clinical care records primarily in that the information is anonymized and in that the resource is used to support secondary use. To support secondary use functions, query support must be included that supports retrieval of multiple records at one time and to support retrieval of subsets of interest to public health. A number of constraints are added which are specific to biosurveillance use of such a resource, and will be included as a part of this Interoperability Specification. These constraints address privacy protection, authenticity, query and polling considerations associated with event detection uses and with secondary use of clinical data for analytical purposes.

Notification of Document Availability and associated actors are optional in this functional flow scenario.

Transmission Options

Note that the Use Cases above use the same set of transactions and differ only by the content of the Biosurveillance Report. This functional flow scenario describes the use of a common document repository to enable communication of biosurveillance data with one or many public health authorities. Four key communication options are available to the Biosurveillance Information System (BIS) using this shared document resource option:

3.1.2.2.1 Notification/Retrieve (HITSP/T29 - Notification of Document Availability Component)

The first transmission option is to enable interested parties (e.g. local, state, federal public health authorities) to subscribe to notification events for published data. Neighboring states, for instance, may be interested in notification for conditions that are registered of a particular type or source. Filtering options for this cycle will be limited, but this is an area for expansion opportunities to incorporate more semantically sophisticated notifications. While the IHE Notification of Document Availability (NAV) Integration Profile is referenced to accomplish this goal, it is still insufficient and this is an area where additional work is needed. What is actually needed is the ability to subscribe to data of interest in fulfillment of the Use Case requirement to filter existing data such that the Biosurveillance Information System can subscribe to data of interest. HITSP recommends that IHE review and identify a mechanism to enhance this profile to include publish and subscribe options in support to public health

3.1.2.2.2 Query Option (HITSP/TP13 - Manage Sharing of Documents Component)

The query option is included in this case to enable communication with Biosurveillance Information Systems (BIS) through an option to poll or query the content of the shared document resource. In some cases, this may be routine polling. For instance, the state and local public health department may wish to poll the resource on an incremental basis so as to retrieve all new records (possibly with a defined time overlap) since the last query. This approach is suited to enable routine access to multiple parties. The query option may also be used to enable access to Biosurveillance documents in order to Query

Neighboring Jurisdiction for Event Detection, Monitor a Suspected Event or for Case Management purposes.

In many cases, the Biosurveillance Information System may need to assess information from the patient care history, and patients may have Biosurveillance case documents in the IHE-XDS repository from prior visits to other providers. For example, if a patient is diagnosed with a new strain of flu, the epidemiologist may want to collect the medical history associated with the case to identify trends in symptoms for early detection.

A query option will be defined as part of this functional flow scenario in order to complete the Biosurveillance Use Case requirement to populate the BIS. A shared information resource environment with query options enables an organization BIS to access and populate its own resource from one or many shared document resources. This serves to accomplish the goals of the Use Case, while better enabling more robust support for the BIS to gather data of interest for multiple regions and information types.

In support of this functional flow scenario, this Interoperability Specification provides constraints to the Use Case for those topics that merit significant additional biosurveillance workflow consideration. These key constraints are with respect to terminology, notifications and support for content specification for the varying reportable conditions forms required by state public health departments to collect supplemental data relevant to support detection and monitoring of public health threats for the local environment. Some of these areas need additional consideration and in some cases harmonization efforts before HITSP can fully specify a robust implementation. While this specification defines the fit for these constructs, detailed specification in some cases will be deferred to enable sufficient consideration for the complexity of the subject matter. It is also assumed that the healthcare provider information systems are able to translate local codes into standard terminology.

3.1.2.2.3 Data Monitor Option Constraints

A data monitor option will be available to enable retrieval from the document repository or additional feed from the document source. This will enable a service to be defined with optional rules for selecting and sending data of interest to the BIS.

3.1.2.2.4 Retrieve Form for Data Capture Option (See HITSP/TP50 - Retrieve Form for Data Capture Transaction Package)

In support of public health authority reportable conditions monitoring and management, the clinical or laboratory information source may optionally implement HITSP/TP50 Retrieve Form for Data Capture Transaction Package. This option allows for capture of supplemental data variables not typically maintained in an electronic health record or laboratory information system through a more seamless integration with the local electronic management system. This option allows for the local system to retrieve a form specific to the identified potential public health threat. This is one option currently available

for reportable conditions which may need additional local configuration and architectural constraints or considerations for implementation architectures.

3.1.2.3 Functional Flow Scenario 3: Resource Management Data Transfer Constraints

The Resource Management Data Transfer functional flow scenario assumes a point-to-point communication from the source to the recipient. No constraints are included at this time with respect to information or processes otherwise needed to support the Emergency Operations Center system. However, as the resource content and sources will likely be expanded in future iterations, it is anticipated that additional constraints will be added at that time to support infrastructure and emergency response needs.

Constraints are included primarily to assert interoperable data communications. In particular, this Interoperability Specification has constrained HL7 messages so as to be able to communicate the resource management information so as to better support integration with existing system capabilities at inpatient locations. As the OASIS HAVE standard was specifically designed to support the Emergency Operations Center system, few additional constraints are added to accommodate this standard.

These standards have been identified in Section 4.3 as an overlap. As a result of the HITSP Biosurveillance Overlap Analysis deliverable, harmonization between these two standards is more formally underway between the two standards bodies. Subsequent versions of the Biosurveillance Interoperability Specification may be modified so as to accommodate any updates and resolutions resulting from the harmonization effort.

3.1.3 PRE-CONDITIONS

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

Table 3.1.3-1 Pre-conditions

Pre-condition	Functional Flow Scenario
For this IS version, the acknowledgements are limited to those provided by underlying transport or HL7	1, 3
Configuration of communication and identification of communication exchanges partners	All
Radiology and laboratory clinical orders are available electronically, may be used, and contain information describing patients and the types of clinical tests requested	1, 2
Secure communications are in place, and all policy, compliance, and authorization issues are addressed through automated or manual means	All
Communication of biosurveillance messages occurs in an environment where public health authorities, clinical offices, laboratories, resource suppliers and hospitals have secured point-to-point network connections. This may be through either VPN or S/MIME approaches	1, 3

Pre-condition	Functional Flow Scenario
Data sent from the Bio Message Sender to the Bio Message Receiver must be Anonymized unless otherwise permitted through legal and out-of-band arrangements. This is required to protect the confidentiality of the patients whose personal health information is sent to the BIS such that the patients can be re-identified as needed to manage public health threats	1
A Regional Capture Center (Data Source System) exists	1,2
Support the technical measures to ensure security and privacy of consumer/patient health information	All
Authentication service to authenticate requestors and/or data submissions from various locations	All
Security and privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient security and privacy	All
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	All
Support the following HITSP Security and Privacy constructs: HITSP/T16 - Consistent Time – Maintain time HITSP/T17 - Secure Communication Channel – Authenticate node HITSP/T15 - Collect and Communicate Security Audit Trail – Record audit event in repository HITSP/TP30 - Manage Consent Directives – Capture/Request consent directive HITSP/TP20 - Access Control – Access control request	All

3.1.4 POST-CONDITIONS

This section provides an overview of the conditions or results that must occur at the end of each scenario in order for the scenario to be deemed successfully completed. This includes any required outputs from the scenario or specific actor states.

Table 3.1.4-1 Post-conditions

Post-condition	Functional Flow Scenario
The Biosurveillance Information System has received the submitted data	1, 3
The Shared Document Resource is available to all authorized Public Health Agencies	2, 3

3.1.5 PROCESS TRIGGERS

This section describes the triggers, including actors and/or processes, which are necessary to start any scenarios, actions or events. It can be an automatic or manual process or result that in turn starts off another scenario, action or event. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

Table 3.1.5-1 Process Triggers

Process Trigger	Functional Flow Scenario
No applicable process triggers	

3.2 DETAILED DESIGN

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

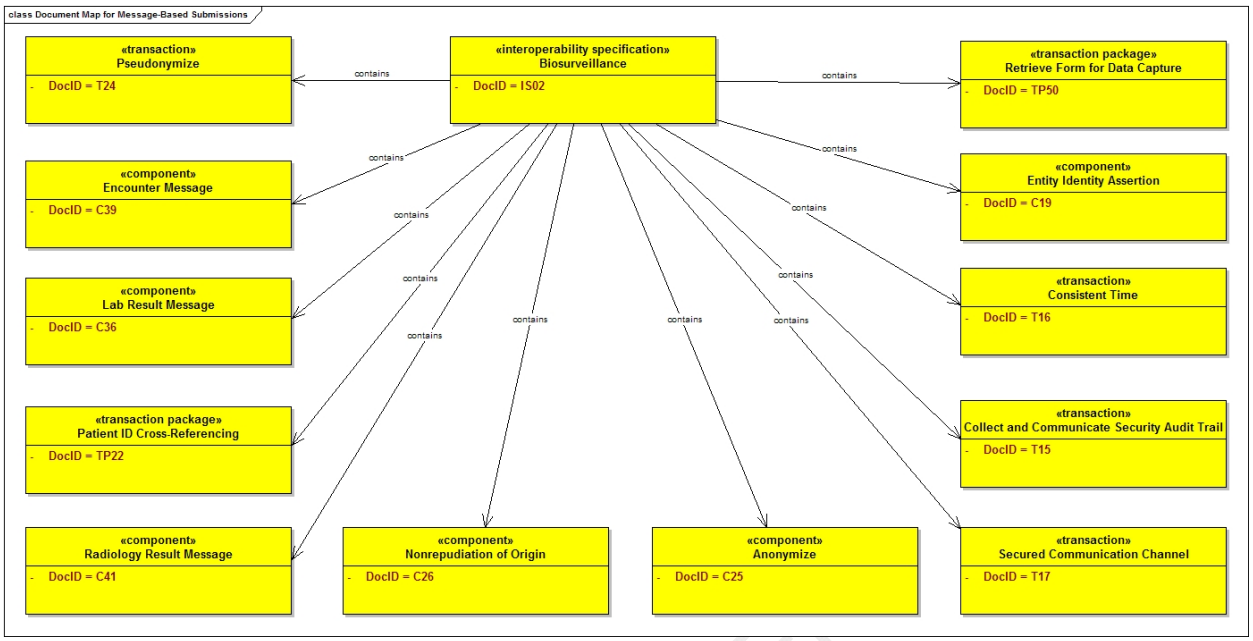
Local implementation policy as determined by risk assessment, including assessment of jurisdictional and regulatory requirements, will determine which assurance level of nonrepudiation of origin is needed. For instance, in document-based transmissions, a low level is offered by the basic use of HITSP/TP13 - Manage Sharing of Documents construct. A medium level of assurance is offered by the use of the HITSP/TP13 construct option called “Document Integrity.” A high level of assurance is offered by the use of the HITSP/C26 - Nonrepudiation of Origin construct which requires the existence of a Public Key Infrastructure (See TN900 for a discussion on the challenges with PKIs).

Message-Based Patient-Level Surveillance Data Communication

As discussed in Section 2.2.3, the message-based communication of patient-level surveillance data functional flow scenario is a mechanism to automate the communication of near real-time message-based data from the clinical care provider to the Biosurveillance Information System through integration with the local clinical information system. This is intended to communicate this data in near-real-time and within 24 hours to Biosurveillance systems to identify and manage public health threats.

It is expected that the communication of biosurveillance messages in this functional flow scenario will occur in an environment where the public health authorities, physician offices, laboratories, resource suppliers and hospitals establish secured point-to-point network connections. This may be achieved through either VPN or S/MIME approaches. There is no sharing in this functional flow scenario. Figure 3.1.1-1 depicts the documents referenced for this implementation.

Figure 3.1-1 Document Map for Message-based Submissions



This functional flow scenario leverages message-based communications. The content of these messages are defined in the associated components.

Several HITSP Security and Privacy Construct are leveraged for supporting services as well. These include:

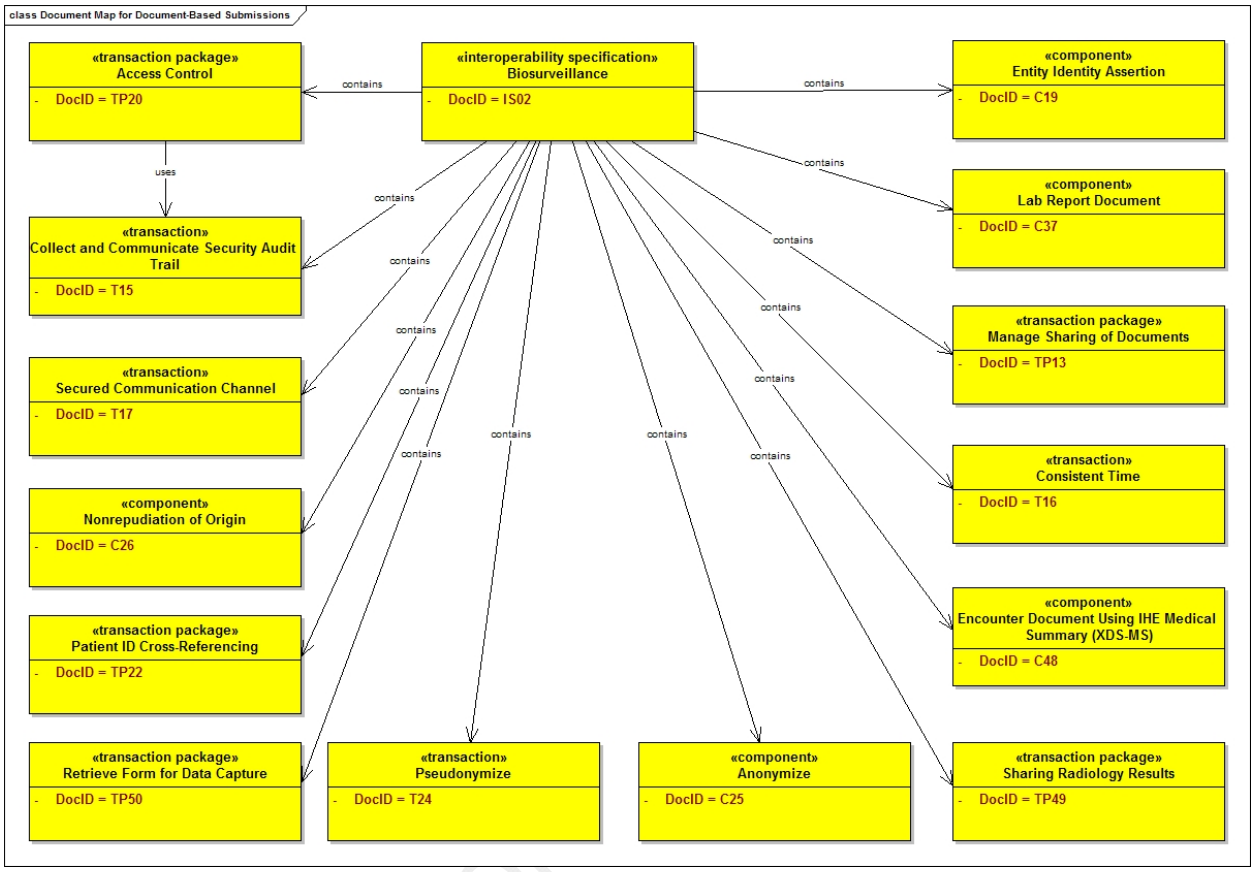
- HITSP/T15 - Collect and Communicate Security Audit Trail Transaction
- HITSP/T16 - Consistent Time Transaction
- HITSP/T17 - Secured Communications Channel Transaction
- HITSP/C19 - Entity Identity Assertion Component
- HITSP/TP30 - Manage Consent Directives Transaction Package

Document-based Patient-level Surveillance Data Sharing (Biosurveillance Documents)

The second functional flow scenario discussed in Section 2.2.3 is a mechanism to automate sharing between care providers of Biosurveillance documents, a class of clinical documents that contain the most relevant portions of information about pseudonymized patient encounter or laboratory testing. This is intended to enable sharing of these documents in near-real time and within 24 hours for a use by Biosurveillance systems, clinicians, epidemiologists and case managers to identify and manage public health threats.

It is expected that the communication of biosurveillance documents in this functional flow scenario will occur in an environment where the public health authorities, physician offices, laboratories, resource suppliers and hospitals are coordinated within a regional health information organization that serves the information sharing needs of a community of care settings. Figure 3.1-2 depicts the documents referenced for this implementation.

Figure 3.1-2 Document Map for Document-based Submissions



This functional flow scenario leverages the registry/repository-based infrastructure specified by the HITSP/TP13 - Manage Document Sharing Transaction Package, and HITSP/TP22 - Patient ID Cross-Referencing Transaction Package.

Several HITSP Security and Privacy Constructs are leveraged for supporting services as well. These include:

- HITSP/T15 - Collect and Communicate Security Audit Trail Transaction
- HITSP/T16 - Consistent Time Transaction
- HITSP/T17 - Secured Communications Channel Transaction
- HITSP/C19 - Entity Identity Assertion Component
- HITSP/TP20 - Access Control Transaction Package
- HITSP/C26 - Nonrepudiation of Origin Component
- HITSP/TP30 - Manage Consent Directives Transaction Package

Functional Flow Transmission Options

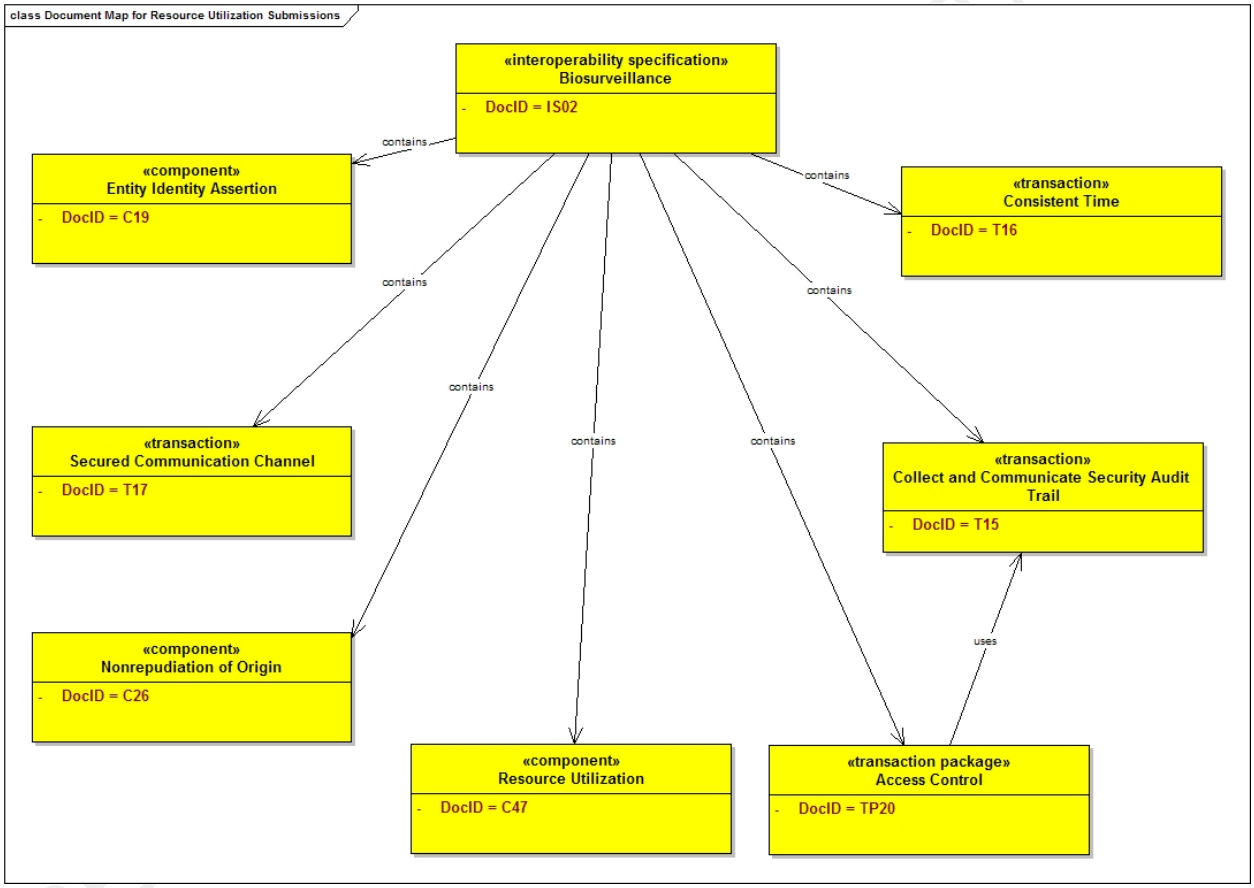
As described in the constraints section, key communication options are available to the BIS using this shared document resource options:

- Notification/retrieve
- Query Option
- Data Monitor Option

Resource Management Data Transfer (Document-based and Message-based) (HITSP- RM)

The third functional flow scenario introduced in Section 2.2.3, is a mechanism to automate the communication of resource availability from a BIO-Data Sender to a BIO-Data Receiver. This is intended to communication of this data in near-real-time and within 24 hours to Biosurveillance systems to identify and manage public health threats. Figure 3.1-3 depicts the HITSP documents referenced for this implementation.

Figure 3.1-3 Document Map for Resource Utilization Submissions



For the Resource Management Data Transfer it is expected that the communication of biosurveillance messages in this functional flow scenario will occur in an environment where organizations such as public health authorities, hospitals, skilled nursing facilities and other inpatient healthcare providers establish secured point-to-point network connections. This may be achieved through either VPN or S/MIME approaches. There is no sharing in this functional flow scenario.

Several HITSP Security and Privacy Constructs are leveraged for supporting services as well. These include:

- HITSP/T15 -Collect and Communicate Security Audit Trail Transaction
- HITSP/T16 - Consistent Time Transaction
- HITSP/T17 - Secured Communications Channel Transaction
- HITSP/C19 - Entity Identity Assertion Component
- HITSP/TP20 - Access Control Transaction Package
- HITSP/C26 - Nonrepudiation of Origin Component

This functional flow scenario leverages message-based communications. The content of these messages are defined in the associated components

NOTE: We have adopted the patient demographics definition from HL7 (a CHI standard) as an interim step and will conform to a HITSP harmonized approach for patient demographics once it becomes available.

Additionally, this Interoperability Specification references Patient Identity cross reference services, although HITSP recognizes that such services are not broadly available, nor is there a national service. There are some available now and more are expected. It is also recognized that cross reference services will be limited to the scope of the service provided - local, regional, etc. We expect these services to be cost-effective. This Interoperability Specification references exchanges between clinical providers and public health authorities. This term is used because the Use Case is expected to expand to include bi-directional information sharing

3.2.1 TECHNICAL ACTOR ROLE DESCRIPTIONS

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

Table 3.2.1-1 Technical Actor Role Descriptions

Technical Actor(s)	Actor Role
Audit Record Repository	This actor provides a repository for audit events. IHE does not specify what analysis and reporting features should be implemented for an audit repository
Audit Record Source	The actor that, on behalf of another actor that performs an action requiring logging, creates and communicates an Audit Record to the Audit Record Repository
Bio-Data Receiver	See Message Receiver
Bio-Data Sender	See Message Sender

Technical Actor(s)	Actor Role
Consent Directive Requester	Accesses consent directive located through a Consent Registry from Consent Repositories. (lack of definition in current public comment version)
Consent Originator	Captures consent directives and may publish the consent directive as a document. It is responsible for sending Manage Consent Directive Requests to a Consent Repository. It also supplies Metadata to the Consent Repository for subsequent registration of the Consent within a Consent Registry
Consent Registry	Responsible for providing location information and sender notification regarding consent directives. The Consent Registry receives a Manage Consent Directive Metadata Request
Consent Repository	Responsible for both the persistent storage of consent directives as well as for their registration with the appropriate Consent Registry. It assigns a Uniform Resource Identifier (URI) and Metadata such as confidentiality codes to the consent directive for subsequent retrieval by an authorized consumer, e.g., for association with published personal health information or for evaluation at a policy decision point
Content Consumer	Responsible for viewing, import, or other processing of content created by a Content Creator Actor
Content Creator	Responsible for the creation of content and transmission to a Content Consumer
Document Consumer	The Document Consumer queries a Document Registry for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors
Document Registry	The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
Document Repository	The Document Repository is responsible for both the persistent storage of documents as well as for their registration with the appropriate Document Registry. It assigns a URI to documents for subsequent retrieval by a Document Consumer The Document Registry maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration
Document Source	The Document Source is the producer and publisher of documents and information. It is responsible for sending documents to a Document Repository. It also supplies metadata to the Document Repository for subsequent registration of the documents with the Document Registry Actor. Also used for point-to-point document exchanges
Form Archiver	The actor responsible for receiving form instance data for archival purposes. For Quality, supports the option to enable manual or cut/paste information capture of patient level quality data content
Form Filler	The actor responsible for retrieving a form from a Form Manager and for submitting form instance data to a Form Receiver. The mechanism by which a unique identification of a form is obtained is outside the scope of the Retrieve Form for Data Capture profile. For Quality, used as an option to enable manual or cut/paste information capture of patient level quality data content. For Quality, Option for CIS to enable manual or cut/paste information capture
Form Manager	The actor that supplies a form based upon a request that supplies unique form identification. For Quality, used as an option to enable manual or cut/paste information capture of patient level quality data content
Form Receiver	The actor that receives form instance data. For Quality, supports the option to enable manual or cut/paste information capture of patient level quality data content
Identity provider	Receives the credentials and identifier from the Entity (principal). It may perform authentication at that point or may require additional authentication from another source (the Service Provider)
Message Receiver	An authorized entity that is receiving resource availability data (e.g. BIS/Emergency Operations Center); Supports message-based communications. Also known as Bio Data Receiver
Message Sender	The holder of resource data who is communicating that data to the message receiver, typically the resource management information system (e.g. Census System/Bed Capacity System) ; Supports message-based information source. Also known as Bio Data Sender

Technical Actor(s)	Actor Role
Node	The originating or terminating point of information or signal flow in a telecommunications network. This actor is equivalent to the *Secure Node* in the IHE ATNA Transaction
Notification Receiver	Receives notifications of availability for documents in an XDS registry, and may optionally send acknowledgments of them
Notification Sender	Sends notifications of availability for documents in an XDS registry, and receives acknowledgements of these notifications
Patient Identity Source	Sends patient demographic information to the Patient Identifier Cross-Reference Manager. For Quality, used for identification of patient historical information for the patient level quality data
Person Identification Service	Manages identity resolution for persons in support of pseudonymization
PIX Consumer	The Patient Identifier Cross-Reference Consumer either queries for sets of cross-reference patient identifiers. It may also receive notifications about cross-reference changes. For Quality, used for identification of patient historical information for the patient level quality data
PIX Manager	The Patient Identifier Cross-Reference Manager Actor is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains
Pseudonymization and Anonymization Service (P&A Service)	Supplier of alternative identification information that permits a patient to be referred to by a key that suppresses his/her actual identification information
Service Provider	Represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion
Service Provider (SP)	The information resource, representing the information repositories and all capabilities that receive, process, and fulfill authorized requests. The SP includes any local access decision and enforcement components that are part of the distributed capabilities
Service Provider Access Control Service (SP ACS)	Supports and implements the service-side access control capabilities. This is a service provider actor
Service User	The entity represents any individual entity (such as a clinician or an EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an end user, an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transaction
Time Client	Establishes time synchronization with one or more Time Servers using the NTP protocol and either the NTP or SNTP algorithms. Maintains the local computer system clock synchronization with UTC based on synchronization with the Time Servers
Time Server	Provides NTP time services to Time Clients. It is either directly synchronized to a UTC master clock (e.g. satellite time signal) or is synchronized by being grouped with a Time Client to other Time Server(s)
User	The entity that takes on the actor role of initiator or claimant. This is an initiator actor
User Access Control Service (UACS)	The enterprise security service that supports and implements user-side access control capabilities. This is an initiator actor

3.2.2 SEQUENCE DIAGRAM FOR PROCESS FLOW

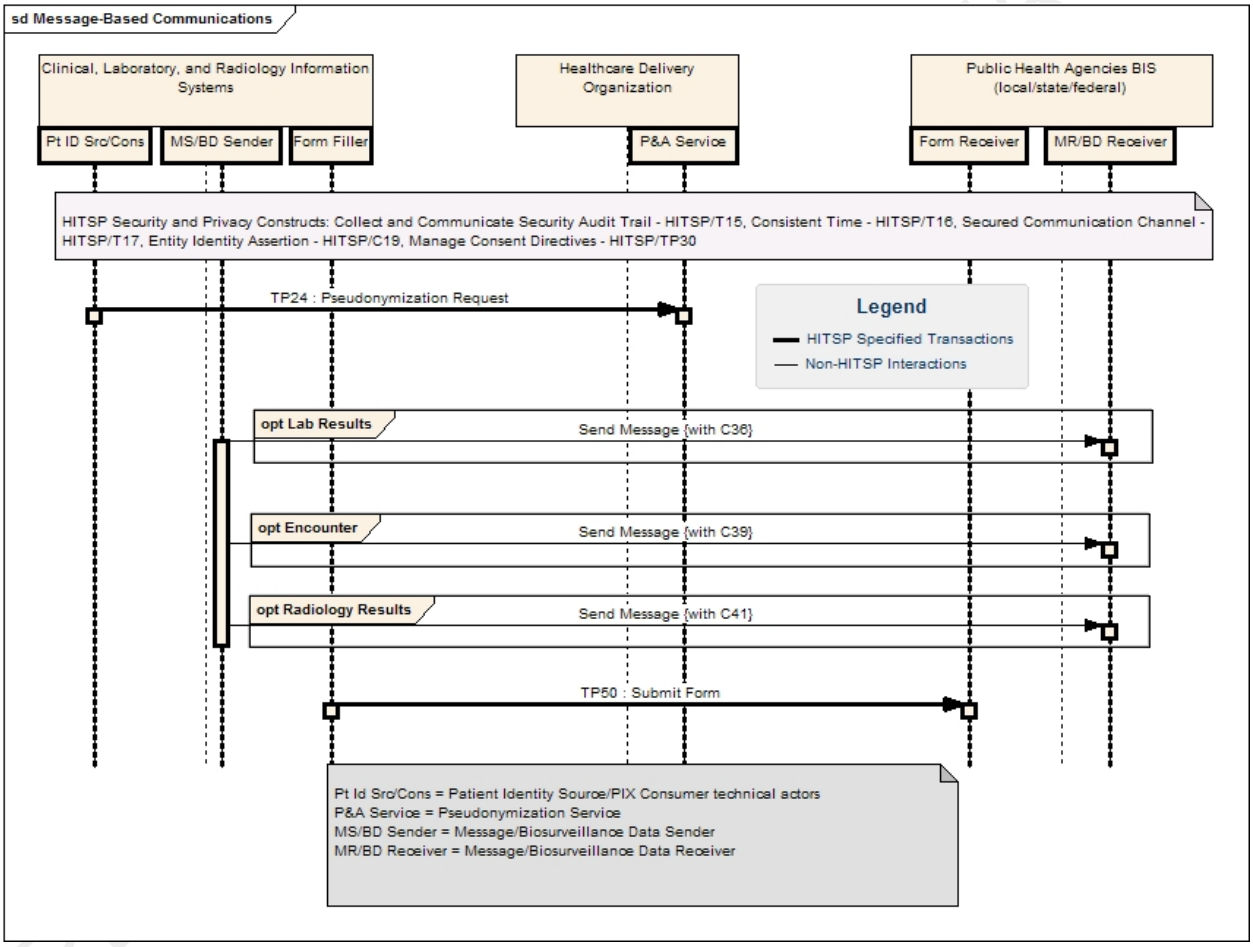
This and the following sections incorporate the comprehensive business and technical requirements and a detailed analysis of the interactions and decisions undertaken for the primary actions in each functional flow scenario. The UML sequence diagrams used in this section incorporates the detailed data requirements for the selected standards (defined in Section 2.2.2) with the technical actors, and their specific and detailed interactions (encapsulated in HITSP constructs). The detailed actor interactions

described in these diagrams show all common or independent actors, data, and the actual transactions from the HITSP constructs that are used for the Interoperability Specification.

3.2.2.1 Message-based Patient-level Surveillance Data

The functional workflow for information retrieval for the Message-Based Patient-level Surveillance Data Communication functional flow scenario is shown in Figure 3.2.2.1-1. This workflow does not include the security transactions. Other dependent transactions such as Audit Trail and Node Authentication and Consistent Time are not shown. Details for these security transactions can be found in the respective Transaction or Transaction Package.

Figure 3.2.2.1-1 Message-based Patient Data Communication Actor Interaction Diagram



The interactions illustrated in the diagram are:

- The Bio Message Sender shall be grouped with the HITSP/T24 - Pseudonymize construct to process pseudonymization and anonymization (P&A) to protect the confidentiality of the patients whose personal health information is sent to the BIS, such that the patients can be re-identified as needed to manage public health threats

- This functional flow scenario can send any of the message options described in Section 3.1.2 of this document

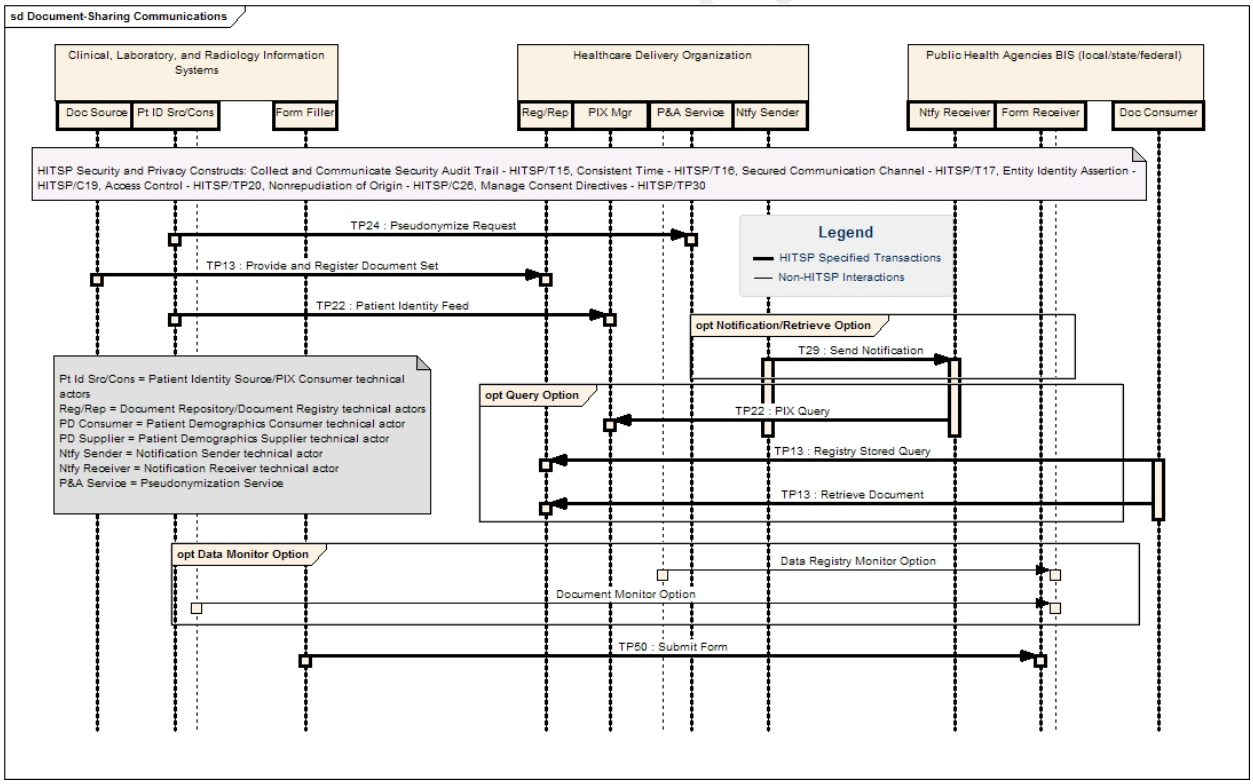
Reportable conditions sent to local public health authorities may necessarily need to be identified and as such, this is to be supported as an option

For the current specification, the acknowledgement is limited to traditional HL7 ACK messages (see gap analysis discussion in Section 4.2 for discussion regarding Biosurveillance use-case-specific acknowledgment requirements).

3.2.2.2 Document-based Patient-level Surveillance Data

The functional workflow for information retrieval for the Document-Based Patient-level Surveillance Data Communication functional flow scenario is shown in figure 3.2.2.2-1. This workflow does not include the security transactions. Other dependent transactions such as Audit Trail and Node Authentication and Consistent Time are not shown. Details for these security transactions can be found in the respective Transaction or Transaction Package.

Figure 3.2.2.2-1 Document-based Patient Data Communication Actor Interaction Diagram



The interactions illustrated in the diagram are:

- Extract/capture a collection of records into a set of documents packaged as an IHE-XDS Submission Set. This submission contains a biosurveillance document, and may contain a number of other

related documents. Biosurveillance documents include data sent to public health authorities for the purposes of detection, monitoring, and managing threats to the public health

- This data are anonymized and pseudonymized and structured as a document of the options described (Laboratory Report, Encounter Summary and Radiology Report Document) and constrained as described by this Interoperability Specification
- This step uses the transactions provided by the IHE-ITI XDS profile to place the records in an IHE-XDS Repository (local or shared)
- The Repository ensures that the documents of the submission set are registered with the IHE-XDS Registry of the XDS Affinity Domain (set of cooperating care delivery institutions)
- The receiving Biosurveillance Information System can then utilize existing query transactions from the IHE-XDS profile to find the URL of the Documents
- Finally, the receiving Biosurveillance Information System may choose to import relevant information from these records into their own BIS system

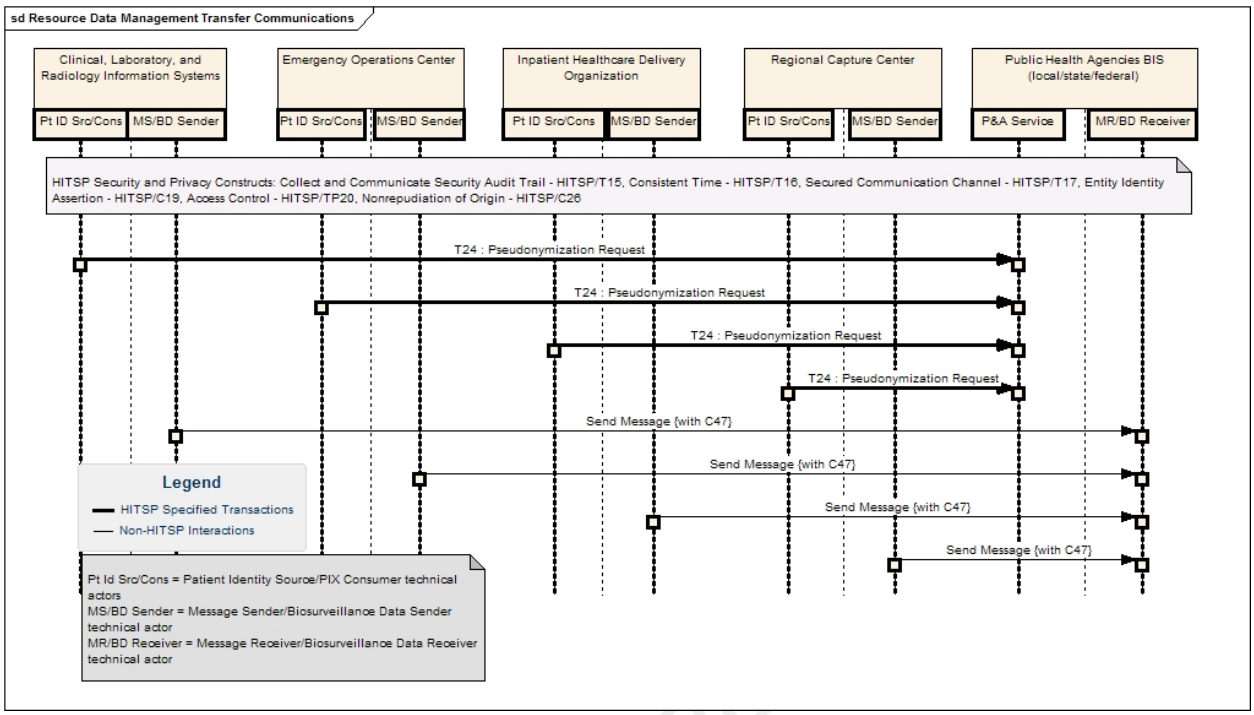
Alternatively:

- A document source monitor option will be available to enable sending document and registry data from the document source to the public health authority
- A registry monitor option will be available to enable sending registry data from the document repository actor to the public health authority so that a query may be later issued from the public health authority
- This will enable a service to be defined with optional rules for selecting and sending data of interest to the BIS

3.2.2.3 Resource Management Data Transfer

The functional workflow for information retrieval for the Resource Management Data Transfer functional flow scenario is shown in figure 3.2.2.3-1 below. This workflow does not include the security transactions. Other dependent transactions such as Audit trail and Node Authentication and Consistent Time are not shown. Details for those security transactions can be found in the respective Transaction or Transaction Package.

Figure 3.2.2.3-1 Resource Management Data Transfer Actor Interaction Diagram



The interactions illustrated in the diagram are:

- Bio Data Sender may first process Pseudonymization and anonymization to assure privacy protection of the patient identifiable data within the message
- Then, the Bio Data Sender communicates the resource availability data to the Bio Data Receiver

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

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

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

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

The following table includes a number of technical actors, each providing a service to complete the full Use Case for extraction of patient level quality data for analysis, aggregation, internal performance monitoring and submission to destination agencies. The technical/business actor mapping is purposely created to be architecturally neutral. In some settings each technical actor will be represented by a different person, group or electronic system. In many settings, one group or electronic system will serve the roles of many technical actors. There are sufficient potential combinations of actors in different architectures that examples could add confusion to this document. Therefore, implementation of individual systems should determine which local architecture components represent which technical actors.

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

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
Clinical Information System, Laboratory Information Systems, Radiology Information Systems (Message Sender/ Bio Data Sender, Document Source)	Each of the actors is optional, but at least one must exist. There is a dependency on the source/recipient supporting the exchange				
	Patient Identity Source	C[101]	HITSP/TP22	PIX Identity Feed	R
	PIX Consumer	C[101]	HITSP/TP22	PIX Query	R
				PIX Update Notification	O
	Document Source	C[102] C[105]	HITSP/TP13	Provide & Register Document Set-b	C[202]
				Provide & Register Document Set	C[202]
	Document Consumer	O	HITSP/TP13	Registry Stored Query	C[203]
				Retrieve Document Set	C[203]
				Stored Query	C[203]
				Retrieve Document	C[203]
	Document Repository	O	HITSP/TP13	Provide and Register Document Set-b	C[204]
				Register Document Set-b	C[204]
				Retrieve Document Set	C[204]
				Register Document Set	C[204]
				Provide & Register Document Set	C[204]
				Retrieve Document	C[204]
	Document Registry	O	HITSP/TP13	Patient Identity Feed	R
				Registry Stored Query	C[205]
				Provide & Register Document Set-b	C[205]
				Stored Query	C[205]
				Provide & Register Document Set	C[205]
				Provide & Register Document Set (offline mode)	[C202]

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
	Message Sender	C[104] C[105]	HITSP/IS02	Send Message	R
				Receive Ack	R
	Message Receiver	C[104] C[106]	HITSP/IS02	Receive Message	R
				Send Ack	R
	Form Filler	C[109] C[105]	HITSP/TP50	Retrieve form	R
				Submit form	R
				Archive form	O
				Retrieve clarifications	O
	Form Manager (Option for CIS supporting form management locally)	O	HITSP/TP50	Retrieve form	R
				Retrieve clarifications	R
	Form Receiver (Option for CIS supporting form management locally)	O	HITSP/TP50	Submit form	R
	Form Archiver (Option for CIS supporting form management locally)	O	HITSP/TP50	Archive Form	R
	Notification Receiver	O	HITSP/T29	Receive Notification	R
				Send Acknowledgement	O
	Content Creator	R	HITSP/C39	Encounter Message Component	C[201]
		R	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		R	HITSP/C35	Lab Result Terminology	C[206]
		R	HITSP/C36	Lab Result Message	C[207]
		R	HITSP/C37	Lab Report Document	C[207]
		R	HITSP/C41	Radiology Result Message	C[208]
		R	HITSP/TP49	Sharing Radiology Results	C[208]
		R	HITSP/C47	Resource Utilization	C[209]
		R	HITSP/TP30	Consent Document Component	R
		C[108]	HITSP/T24	Pseudonymization Request	R
		C[109]	HITSP/C25	Anonymize	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	O	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
	Identity provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
Healthcare Delivery Organization (Regional Health Information Organizations (RHIO))	PIX Manager	R	HITSP/TP22	Patient Identity Feed	R
				PIX Query	R
				PIX Update Notification	R
				Pseudonymization Request	R
	Content Creator	O	HITSP/C39	Encounter Message Component	C[201]
		O	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		O	HITSP/TP30	Consent Document Component	R
		C[108]	HITSP/T24	Pseudonymization Request	R
		C[109]	HITSP/C25	Anonymize	R
	Document Registry	R	HITSP/TP13	Patient Identity Feed	R
				Registry Stored Query	C[205]
				Provide & Register Document Set-b	C[205]
				Stored Query	C[205]
				Provide & Register Document Set	C[205]
	Document Repository	O	HITSP/TP13	Provide and Register Document Set-b	C[204]
				Register Document Set-b	C[204]
				Retrieve Document Set	C[204]
				Register Document Set	C[204]
				Provide & Register Document Set	C[204]
				Retrieve Document	C[204]
	Person Identification Service	C[108]	HITSP/T24	Person Identity Feed	R
				Person Identity Cross-Reference Query	R
				PIX Update Notification	R
				Pseudonymization Request	R
	Initiating Gateway	O	HITSP/TP13	ITI-38: Cross Gateway Query	R
				ITI-39: Cross Gateway Retrieve	R
	Responding Gateway	O	HITSP/TP13	ITI-38: Cross Gateway Query	R
				ITI-39: Cross Gateway Retrieve	R
	Pseudonymization Service	C [108]	HITSP/T24	Pseudonymization Request	R
	Message Sender	O	HITSP/IS02	Send Message	R
				Receive Ack	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
Public Health Agencies (Local/State/Federal)	Message Receiver	O	HITSP/IS02	Receive Message	R
				Send Ack	R
	Notification Sender	O	HITSP/T29	Send Notification	R
			HITSP/T29	Receive Acknowledgement	O
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
	Each of the actors are optional, but at least one must exist. There is a dependency on the source/recipient supporting the exchange				
	Document Consumer	C[102] C[106]	HITSP/TP13	Registry Stored Query	C[203]
				Retrieve Document Set	C[203]
				Stored Query	C[203]
				Retrieve Document	C[203]
	Content Creator	O	HITSP/C39	Encounter Message Component	C[201]
		O	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		O	HITSP/TP30	Consent Document Component	R
		C[108]	HITSP/T24	Pseudonymization Request	R
		C[109]	HITSP/C25	Anonymize	R
	Content Consumer	O	HITSP/C39	Encounter Message Component	C[201]
		O	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		O	HITSP/TP30	Consent Document Component	R
	Message Receiver	C[104] C[106]	HITSP/IS06	Receive Message	R
				Send Ack	R
	Form Receiver	C [109] C[106]	HITSP/TP50	Submit Form	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
Regional Capture Center	Each of the actors are optional, but at least one must exist. There is a dependency on the source/recipient supporting the exchange				
	Message Sender	O	HITSP/IS02	Send Message	R
				Receive Ack	R
	Message Receiver	O	HITSP/IS02	Receive Message	R
				Send Ack	R
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O
Emergency Operations Center (EOC)	Each of the actors are optional, but at least one must exist. There is a dependency on the source/recipient supporting the exchange				
	Message Receiver	O	HITSP/IS02	Receive Message	R
				Send Ack	R
	Content Creator	O	HITSP/C39	Encounter Message Component	C[201]
		O	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		O	HITSP/TP30	Consent Document Component	R
		C[108]	HITSP/T24	Pseudonymization Request	R
		C[109]	HITSP/C25	Anonymize	R
	Content Consumer	O	HITSP/C39	Encounter Message Component	C[201]
		O	HITSP/C48	Encounter Document Using IHE Medical Summary (XDS-MS) Component	C[201]
		O	HITSP/TP30	Consent Document Component	R

Business Actor	Technical Actor(s)	Actor Optionality*	Construct	Transaction/Content	T/C Optionality*
	Audit Record Source	R	HITSP/T15	Record Audit Event in Repository	R
	Audit Record Repository	R	HITSP/T15	Record Audit Event in Repository	R
	Time Client	R	HITSP/T16	Maintain Time	R
	Time Server	O	HITSP/T16	Maintain Time	R
	Node	R	HITSP/T17	Secured Communication Channel	R
	Service User	R	HITSP/C19	Convey Assertion	R
				Provide Assertion	O
	Identity Provider	O	HITSP/C19	Provide Assertion	R
				Verify Assertion	O
	Service Provider	O	HITSP/C19	Convey Assertion	R
				Verify Assertion	O

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

Actor Optionality Conditions

C[102] – Required for document sharing functional flow

C[103] – Required for Clinical Information System

C[104] – Required for message-based functional flow

C[105] – Business Actor shall support at least one of these technical actors to communicate outbound content

C[106] – Business Actor shall support at least one of these technical actors to receive or retrieve inbound content

C[107] – Required for Laboratory Information System

C[108] – Required where pseudonymization is required by the jurisdiction or information sharing agreements

C[109] – Required where anonymization is required by the jurisdiction or information sharing agreements

C[108] – Required for Radiology Information System

Transaction/Content (T/C) Optionality Conditions

C[201] – For Clinical Information System, shall support either HITSP Encounter Message Component or Encounter Document Using IHE Medical Summary (XDS-MS) Component or both

C[202] – The Actor shall support at least one of these transactions

C[203] – The Document Consumer shall support either XDS.a transactions, XDS.b transactions or both Where Identity Assertion is required, the Document Consumer shall support XDS.b (Registry Stored Query, Retrieve Document Set)

C[204] – The Document Repository shall support either XDS.a transactions, XDS.b transactions or both. Where Identity Assertion is required, the Document Repository shall support XDS.b (Provide & Register Document Set-b, Register Document Set-b, Retrieve Document Set)

C[205] – The Document Registry shall support either XDS.a transactions, XDS.b transactions or both. Where Identity Assertion is required, the Document Repository shall support XDS.b to query the registry (Registry Stored Query)
C[206] - For Laboratory Information System, shall support HITSP Laboratory Terminology Component
C[207] - For Laboratory Information System, shall support HITSP Laboratory Message Component, Laboratory Report Document or both
C[208] - For Radiology Information System, shall support HITSP Radiology Message Component, Sharing Radiology Results or both
C[209] - For systems reporting bed availability, system shall support HITSP Resource Utilization Component

3.2.4 CONSTRUCT DEPENDENCIES

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

Table 3.2.4-1 Construct Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource/ Provide and Register (EMR Document Sources))	HITSP/C48 - Encounter Document	Each HITSP-Document Sharing (DS) Actor shall support the HITSP/C48 - Encounter Document with additional constraints as specified to support the biosurveillance requirements	Required for the communication of biosurveillance encounter report information and lab/radiology order information from hospital and ambulatory EMRs
HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource/Provide and Register (Laboratory Document Sources))	HITSP/C37 - Lab Report Document	HITSP-DS Actor shall support the HITSP/C37- Lab Report Document content profile	Required for communication of discharge summary information from hospital and ambulatory EMRs
HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource/Provide and Register (Document Sources))	HITSP/TP22 - Patient ID Cross-Referencing	HITSP-DS Actor shall support the HITSP/TP22- PIX as part of the HITSP/T24 - Pseudonymize	Required for consistently assigning the pseudo-identity to a patient across multiple provider locations
HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource/Provide and Register (Document Source))	HITSP/T24 - Pseudonymize	Each actor implementing the document sharing of patient data functional flow scenario shall be grouped with the HITSP/T24 - Pseudonymize	Used to protect confidentiality of patients whose personal health information is sent to the BIS while assuring that patients can be re-identified if needed to manage public health threats

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
HITSP/T24 - Pseudonymize	HITSP/TP22 – Patient Identity Cross-referencing (PIX)	HITSP/T24 Actor shall support the IHE-PIX Integration Profile as part of the HITSP-Pseudonymize construct to uniquely identify a Patient across enterprises	Required for consistently assigning the pseudo-identity to a patient across multiple provider locations
HITSP/TP13 - Manage Sharing of Documents	HITSP/C26 - Nonrepudiation	Grouping	Required to support Nonrepudiation of origin
HITSP/T29 - Notification of Document Availability	HITSP/C26 - Nonrepudiation	Grouping	Required to support Nonrepudiation of origin
HITSP/T15 - Collect and Communicate Audit Trail	HITSP/T16 - Consistent Time	Pre-condition	Pre-requisites for Use Cases
HITSP/TP13 - Manage Sharing of Documents	HITSP/T15 - Collect and Communicate Audit Trail	Pre-condition	Required to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis
HITSP/T17 - Secured Communication Channel	HITSP/T15 - Collect and Communicate Audit Trail	General	Identification and management of audit trigger events and audit event outputs
HITSP/TP30 - Manage Consent Directives	HITSP/T17 - Secured Communication Channel	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/T16 - Consistent Time	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/T15 - Collect and Communicate Audit Trail	Pre-condition	Pre-requisites for Use Cases
HITSP/TP30 - Manage Consent Directives	HITSP/C19 - Entity Identity Assertion	General	Pre-requisites for Use Cases

3.2.5 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

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

Table 3.2.5-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
N/A	HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource/Provide and Register)	The policy of the implementation environment MAY require HITSP Manage Document Sharing Document Integrity Option	General	This enables fulfillment of the Use Case requirement 1.3.2.2 Verify integrity of the transmission contents from the identified source

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
N/A	HITSP/C48 – Encounter Document using IHE Medical Summary (XDS-MS)	Constrain Medical Summary documents to minimal clinical and anonymized demographic dataset from AHIC Data Steering Committee data dictionary clinical data elements	Pre-condition	Required to conform to the AHIC domain requirements for Biosurveillance data
N/A	HITSP/C37 – Lab Report Document	Constrain Laboratory Report Document to minimal laboratory result dataset from AHIC Data Steering Committee data dictionary laboratory result data elements	Pre-condition	Required to conform to the AHIC domain requirements for Biosurveillance data
N/A	HITSP/C39 – Encounter Message	Constrain Encounter Summary message to minimal clinical and anonymized demographic dataset from AHIC Data Steering Committee data dictionary clinical data elements	Pre-condition	Required to conform to the AHIC domain requirements for Biosurveillance data
N/A	HITSP/C36 – Lab Result Message	Constrain Laboratory Result Message to minimal laboratory result dataset from AHIC Data Steering Committee data dictionary laboratory result data elements	Pre-condition	Required to conform to the AHIC domain requirements for Biosurveillance data
N/A	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Data sent to the shared document repository and recorded in the shared registry must be Anonymized unless otherwise permitted through legal and out-of-band arrangements	Pre-condition	Required to protect the confidentiality of the patients whose personal health information is sent to the BIS such that the patients can be re-identified as needed to manage public health threats
NA	HITSP/C48 Encounter Document using IHE Medical Summary (XDS-MS)	Medical Summary Document Constraints – Vocabulary (See Section 3.2.1)	Pre-condition	Required for optimum harmonization and interoperability of document content
NA	HITSP/C48 Encounter Document using IHE Medical Summary (XDS-MS)	Medical Summary Documents may be generated at any time during the patient visit, and not restricted to patient discharge	Pre-condition	Required to conform to Use Case constraint of providing biosurveillance information in with a periodicity of no longer than 24 hours

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
NA	HITSP/C48 Encounter Document using IHE Medical Summary (XDS-MS)	Medical Summary Documents should contain some machine-readable content	Pre-condition	Used to assure machine-consumable information for large volume information exchange and processing
NA	HITSP/TP13 – Manage Sharing of Documents (Shared Document Resource)/ Query Registry Transaction Stored Query Transaction Retrieve Document Transaction	Support queries and stored queries for documents which do not require a patient id as a query parameter	General	Asserted to enable public health information retrieval support to enable pull of repository data to the BIS or to ask public health questions of the data
NA	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	HITSP/C26 - This assures the validity of the information source, submitter, data transmission, and authorization; Document Consumer of the query registry is responsible for verification of integrity, authenticity	Pre-condition	Asserted to fulfill the Use Case requirement to 'Verify authenticity of transmission contents'
NA	HITSP/TP13 – Manage Sharing of Documents (Query Registry)	HITSP/C26 - This assures the validity of the information source, submitter, data transmission, and authorization; Document Consumer of the query registry is responsible for verification of integrity, authenticity, using OCSP, ANSI X9.31, and CRL	Post-condition	Asserted to fulfill the Use Case requirement to 'Verify authenticity of transmission contents'
NA	HITSP/TP13 – Manage Sharing of Documents (Query Registry)	HITSP/TP30 should be referenced to record the OID of the authorization policy under which the patient data are disclosed to the authorized public health authority	Post-condition	Asserted to record authorized disclosure in compliance with HIPAA
NA	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	HITSP/TP30 should be referenced to record the OID of the authorization policy under which the patient data are disclosed to the authorized public health authority	Pre-condition	Asserted to record authorized disclosure to public health authority in audit logs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
NA	HITSP/T15 Collect and Communicate Audit Trail	HITSP/T15 should be constrained to record the OID of the authorization policy under which the patient data are disclosed to the authorized public health authority	Post-condition	Asserted to record authorized disclosure to public health authority in audit logs
NA	HITSP/TP22 Patient Identity Cross-referencing (Uniquely identify a Patient across enterprises)	Constrain to return single value for pseudonymization steps	General	In order to link pseudo identifiers across entities
XDSDocumentEntry.eventCodeList	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	The metadata element should be required when there is a known condition as required by or of interest to public health authorities, and must contain a value from a controlled vocabulary describing the reportable condition.	Pre-condition	The list of codes aims to represent the main clinical acts documented
XDSDocumentEntry 'confidentialityCode'	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Extend the usage to signify when patient information in the document and corresponding metadata has been pseudonymized Attribute: confidentialityCode Optionality: R[1] Vocabulary: Need to assign a unique OID and code values to indicate pseudonyminization	Pre-condition	This code indicates the level of confidentiality for the corresponding document
object type XDSDocumentEntry, attributes 'healthcareFacilityTypeCode' and 'practiceSettingCode'	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Both have requirement level of R. This could potentially be a problem, unless we can expand the definition of these attributes	Pre-condition	These attributes do not quite conceptually align with all possible data sources for biosurveillance data
object type XDSDocumentEntry, attributes 'parentDocumentId' and 'parentDocumentRelationship'	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Are potentially applicable to biosurveillance, useful in the general sense for document management. Requirement level of R2 suits the biosurveillance Use Case	Pre-condition	These attributes are useful in the general sense for document management

[1] Per IHE Metadata source/query codes, R2 refers to 'Required if Known'

Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, General)	Purpose (Reason for this constraint)
object type XDSDocumentEntry	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Requirement for attributes 'patientId' and 'sourcePatientID'	Pre-condition	In many data sources for biosurveillance, patients may not be involved at all. If they are, the id should be pseudonymized. We need something like 'sourceId' in this case as a substitute
object type XDSDocumentEntry, attributes 'serviceStartTime' and 'serviceStopTime'	HITSP/TP13 - Manage Sharing of Documents (Provide and Register)	Do not have an intuitive context for all biosurveillance data sources	Pre-condition	We'd need to expand/explain their definition when the data source is not from an EMR system
object type XDSDocumentEntry	HITSP/TP13 - Manage Sharing of Documents (Provide andRegister)	Several sub-attributes are required for attribute 'sourcePatientInfo': source patient id list, patient name, patient gender, patient birthdate, patient address.	Pre-condition	When the biosurveillance data source does not pertain to a patient, most of these are useless. Other sub-attributes of the HL7 v2.5 PID Segment can come into play: Species Code, Breed Code, Strain, Production Class Code, County Code (assuming this is equivalent to UN – level 2 region identification). In the case of patients, XDS does not enforce many requirements on the sub-components for these sub attributes. Address could contain nothing more than a street name or a country. In this case, data from XDS would not be plottable on a map or useful for geographic simulation

In support of Biosurveillance, Table 3.2.5 -2 describes the constraints placed on several of the elements of the XDSDocumentEntry object type from HITSP/TP13 – Manage Sharing of Documents (based on IHE XDS).

Table 3.2.5-2 XDSDocumentEntry Element Constraints

XDS Metadata Attribute	Optionality	Extended Discussion	Source Type
XDSDocumentEntry.eventCodeList	R[2]	See 3.2.5.1	Coded in Affinity Domain with Transform (CADT)
XDSDocumentEntry.confidentialityCode	R	See 3.2.5.2	Fixed by Affinity Domain (FAD)
XDSDocumentEntry.patientID and XDSSubmissionSet.patientID	R	See 3.2.5.3	Source document Attribute with Transformation (SAT)
XDSDocumentEntry.sourcePatientID and XDSSubmissionSet.sourcePatientID	R	See 3.2.5.4	Source document Attribute with Transformation (SAT)

3.2.5.1 XDSDocumentEntry.eventCodeList

An XDSDocumentEntry.eventCodeList metadata element that contains a value from a controlled vocabulary describing reportable conditions should be required when there is a known condition as required by, or of interest to, public health authorities. Other XDSDocumentEntry.eventCodeList metadata elements may also be present using local codes or other controlled terminology, however, these are outside of the scope of this specification. The eventCodeList could contain, for instance, a value from the Nationally Notifiable Diseases and Other Conditions of Public Health Importance Event Code List published by the Centers for Disease Control and Prevention. See www.cdc.gov for more details.

The vocabulary shall be identified by the OID representing the coding system from which these events are pulled present in the codingScheme data element.

```
<rim:Classification
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="theDocument" nodeRepresentation="eventCode">
   <rim:Name>
          <rim:LocalizedString value="eventCodeDisplayName"/>
   </rim:Name>
   <rim:Slot name="codingScheme">
          <rim:ValueList>
                 <rim:Value>2.16.840.1.114222.4.5.255</rim:Value>
          </rim:ValueList>
   </rim:Slot>
</rim:Classification>
```

The population of this code is not in any way circumventing, defining, or changing state/federal requirements reporting. Vocabulary and reporting compliance need to be validated and audited independent of this specification.

[2] This metadata element is optional in the XDS Provide and Register Transaction, but required for use with the Biosurveillance specifications.

3.2.5.2 XDSDocumentEntry.confidentialityCode

The confidentialityCode attribute shall contain the following OID when the submitted document has been pseudonymized according to HITSP/T24 - Pseudonymize Transaction: 2.16.840.1.113883.3.88.5.2.1

3.2.5.3 XDSDocumentEntry.patientID and XDSSubmissionSet.patientID

The XDSDocumentEntry.patientID and XDSSubmissionSet.patientID attributes shall contain either the actual patient identifier used by the XDS registry, or shall contain a pseudonymized identifier generated during the HITSP/T24- Pseudonymize Transaction.

3.2.5.4 XDSDocumentEntry.sourcePatientID and XDSSubmissionSet.sourcePatientID

The XDSDocumentEntry.sourcePatientID and XDSSubmissionSet.sourcePatientID attributes shall contain either the actual patient identifier used by the document source, or shall contain a pseudonymized identifier generated during the HITSP/T24 - Pseudonymize Transaction.

4.0 STANDARDS SELECTION

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

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

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

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

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

4.1 LIST OF STANDARDS

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

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

4.1.1 REGULATORY GUIDANCE

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

Table 4.1.1-1 Regulatory Guidance

Standard	Description
Clinical Laboratory Improvement Amendments (CLIA) of 1988	Establishes quality standards for all laboratory testing to ensure the accuracy, reliability, and timeliness of patient test results regardless of where the test is performed. The Centers for Medicare and Medicaid Services (CMS) regulates all laboratory testing (except research) performed on humans in the U.S. based on CLIA. For more information visit www.fda.gov and www.cms.hhs.gov
Health Insurance Portability and Accountability Act (HIPAA) -- Administrative Simplification	A listing of national standards plus rules adopted by federal regulation for electronically communicating specified administrative and financial healthcare transactions, and protecting the security and privacy of healthcare information, as applied to the three types of defined covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct any of the specified healthcare transactions. See the Code of Federal Regulations, Title 45, Parts 160, et. seq. for more information

4.1.2 SELECTED STANDARDS

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

Table 4.1.2-1 Selected Standards Linked to HITSP Constructs

Standard Name	HITSP Construct	Remarks/ Minor Gaps
American Medical Association (AMA) Current Procedural Terminology (CPT®) Fourth Edition (CPT-4)	HITSP/C41- Radiology Results Message	
American Society for Testing and Materials (ASTM) Standard Guide for Electronic Authentication of Health Care Information: # E1762-95(2003)	HITSP/C26 - Nonrepudiation	
European Telecommunications Standards Institute (ETSI) Technical Specification TS 101 903: XML Advanced Electronic Signatures (XadES)	HITSP/C26 - Nonrepudiation	
Federal Information Processing Standards (FIPS) Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas Publication # 5-2, May, 1987	HITSP/C39 - Encounter Message HITSP/C41- Radiology Results Message	
Health Level Seven (HL7) Clinical Document Architecture Release 2 (CDA R2)	HITSP/C37 - Lab Report Document HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
Health Level Seven (HL7) U.S. Realm - Interoperability Specification: Lab Result Message to EHR (ORU^R01) (HL7 Version 2.5.1) September, 2007	HITSP/C36 - Lab Result Message	
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	HITSP/ TP20 - Access Control	
Health Level Seven (HL7) Version 2.5[3]	HITSP/C39 - Encounter Message HITSP/C41 - Radiology Result Message HITSP/C47 - Resource Utilization Message HITSP/TP22 - Patient ID Cross-Referencing	
Health Level Seven (HL7) Version 2.5.1[4]	HITSP/C35 - Lab Result Terminology HITSP/C36 - Lab Result Message	

[3] HITSP references HL7 2.5.1 messaging for lab results reporting and HL7 2.5 for other messages. Future maintenance work will move toward referencing a single HL7 version across HITSP documents.

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	HITSP/TP30 - Manage Consent Directives	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	HITSP/C41 - Radiology Result Message	IHE RFD IHE XDS IHE PIX IHE ATNA IHE CT
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	HITSP/T15 - Collect and Communicate Security Audit Trail HITSP/T17 - Secured Communication Channel	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	HITSP/T24 - Pseudonymize	IHE RFD IHE XDS IHE PIX IHE ATNA IHE CT
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Consistent Time (CT) Integration Profile	HITSP/T16 - Consistent Time	
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	IHE XDS
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement - ITI-25 Notification of Document Availability (NAV) Jun 28, 2005	HITSP/T29 - Notification of Document Availability	IHE NAV
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	HITSP/C19 - Entity Identity Assertion Component	IHE XUA
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	IHE XDS
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	IHE XDS.b

[4] HITSP references HL7 2.5.1 messaging for lab results reporting and HL7 2.5 for other messages. Future maintenance work will move toward referencing a single HL7 version across HITSP documents.

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Supplement 2007 - 2008 Basic Patient Privacy Consents (BPPC) – Trial Implementation	HITSP/TP30 - Manage Consent Directives	IHE BPPC
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	HITSP/C26 - Nonrepudiation of Origin	IHE DSG
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	HITSP/TP13 - Manage Sharing of Documents HITSP/TP30 - Manage Consent Directives	IHE XCA
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) 2007 – 2008 Supplement, Retrieve Form for Data Capture (RFD)	HITSP/TP50 - Retrieve Form for Data Capture	IHE RFD
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	HITSP/TP22 - Patient ID Cross-Referencing	
Integrating the Healthcare Enterprise (IHE) Laboratory Technical Framework Volume 3 (LAB TF-3) Document-based Transactions, Revision 2.0 - For Trial Implementation, August 16, 2007	HITSP/C37 - Lab Report Document	IHE LAB-TF
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	IHE XDS-MS
Integrating the Healthcare Enterprise (IHE) Radiology Technical Framework Revision 8.0	HITSP/TP49 - Sharing Radiology Results	IHE XDS-I
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	HITSP/C39 - Encounter Message	
International Classification of Diseases, 10th Revision, Related Health Problems (ICD-10-CM)	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) HITSP/C39 - Encounter Message	
International Classification of Diseases, 9th Revision, Clinical Modifications (ICD-9-CM)	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) HITSP/C41- Radiology Results Message HITSP/C39 - Encounter Message	

Standard Name	HITSP Construct	Remarks/ Minor Gaps
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) HITSP/C39 - Encounter Message HITSP/C35 - Lab Result Terminology HITSP/C36 - Lab Result Message HITSP/C41- Radiology Results Message	For Nursing Triage Notes and Chief Complaints, this Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT.
International Organization for Standardization (ISO) Health informatics -- Pseudonymisation, Unpublished Technical Specification # 25237	HITSP/C25 - Anonymize HITSP/T24 - Pseudonymize	
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	HITSP/T16 - Consistent Time	
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	HITSP/T16 - Consistent Time	
Logical Observation Identifiers Names and Codes (LOINC®)	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) HITSP/C35 - Lab Result Terminology HITSP/C39 - Encounter Message	
National Uniform Billing Committee (NUBC) Uniform Bill Version 1992 (UB-92) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	HITSP/C39 - Encounter Message	
National Uniform Billing Committee (NUBC) Uniform Bill Version 2007 (UB-04) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS)	
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	HITSP/TP20 - Access Control	
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	HITSP/TP20 - Access Control	

Standard Name	HITSP Construct	Remarks/ Minor Gaps
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	HITSP/TP20 - Access Control	
Unified Code for Units of Measure (UCUM)	HITSP/C48 - Encounter Document Using IHE Medical Summary (XDS-MS) HITSP/C39 - Encounter Message HITSP/C35 - Lab Result Terminology	

4.1.3 INFORMATIVE REFERENCE STANDARDS

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

Table 4.1.3-1 Informative Reference Standards

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

Standard Name	Description/Reason for Use
American Society for Testing and Materials (ASTM) Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org
American Society for Testing and Materials (ASTM) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, with the Privacy Act of 1974 (1)." For more information visit www.astm.org
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org
International Organization for Standardization (ISO) Health informatics -- Information technology -- Text and office systems - Office Document Architecture (ODA) and interchange format, Technical Report on ISO 8613 implementation testing, Technical Specification # ISO/IEC CD 10183 -- Part 3: Testing procedure	Specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system. For more information visit www.iso.org

Standard Name	Description/Reason for Use
International Organization for Standardization (ISO) Health informatics -- Privilege management and access control(PMAC), Technical Specification #22600 -- Part 1: Overview and policy management, July 2006	Supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org
International Organization for Standardization (ISO) Health informatics – Functional and Structural Roles (ISO SF Roles), Technical Specification #21298 , Draft May, 2007	This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed 1. Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare actors 2. Directory services: structural roles are usefully recorded within directories of health care providers (see for example, ISO TS 21091 Health Informatics – Directory services for security, communications, and identification of professionals and patients) 3. Audit trails: functional roles are usefully recorded within audit trails for health information applications 4. Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary For more information visit www.iso.org

4.2 GAPS WHERE THERE ARE NO STANDARDS

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

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

The gap is only relative to the specific Biosurveillance Use Case event. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross team validation of the gap, provisional recommendations and peer review by the team.

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

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Event Description	Identified Gaps	Recommended Resolution
1.1.1.0	Filter existing data to identify data required by Public Health Agencies	LAB *Terminology* Orders/Results (Test Batteries) Possible Gap: indication /presumptive diagnosis/ reason for test - NOT a gap for current data dictionary, gap for domain Standardization of data definitions to ensure accurate filtering	Work with LOINC and SNOMED to achieve the appropriate level of granularity Link test orders to test results Work with ICD and SNOMED to review Vocabulary requirements for presumptive DX CMS-validated mapping between SNOMED-CT and ICD9-CM (while more clinical granularity as provided by SNOMED, current systems are using ICD-9-CM for morbidity coding) Approach HL7 and OASIS IHC to coordinate standards development efforts for formalizing rule specification for consistent screening of cohort selection Monitor / contribute/ review IHE Retrieve Form for Data Capture (RFD) to assure biosurveillance needs are met for reportable filters
1.2.1.0	Filter existing data to identify data required by public health agencies		
1.1.2.0	Anonymize data required by Public Health Agencies	LAB, VISIT, UTILIZATION *Functionality/ workflow/ process* Freeform text records, e.g., notes, specimen description, etc. may contain information that can identify an individual. Method for abstracting concepts from freeform text records that will not effect anonymization is needed We need additional guidance on policy that is inclusive of the entire U.S. needs	Encourage open source and publicly available software contributions of free-text parsers to extract and encode data of interest (codify) at the source to protect the anonymity of the payload data, e.g., Eclipse Open Healthcare Frameworks Monitor / contribute / review ISO TC215 Health Informatics Pseudonymisation standard Refer to AHIC Security/Privacy group
1.2.2.0	Anonymize data required by Public Health Agencies		

Event Code	Event Description	Identified Gaps	Recommended Resolution
1.1.3.0	Format data required by Public Health Agencies	LAB *Terminology* Granular ontology of body sites Definitions for indication/ presumptive DX/reason for test Standardized use of laboratory terminology standards is a gap because laboratories and hospitals often use local codes to describe laboratory tests and test results instead of adhering to vocabulary standards such as LOINC and SNOMED *Functionality /workflow/ process* - need to define dataset to be send VISIT *Terminology* - Possible Gaps -need to have more detail on the essential data set. There may be gaps in the vocabulary (e.g. ED Acuity) LAB, VISIT, UTILIZATION *Context* – need for information model for visit data Message – there is a need for a message standard that can appropriately represent the required utilization data *Functionality/ workflow/ process* - need for a method for transformation, mapping between different standards and local/custom codes. UMLS / SNOMED mapping may be incomplete for this Use Case need to define to whom to send data need to define term “transform” (i.e., from what to what?)	LAB Review context standards (see statements below) Monitor/ contribute / review the HL7 specimen segment development Review the data dictionary and volume/frequency requirements to better assess potential vocabulary gaps Encourage open source and publicly available software to help facilitate mapping from local codes to selected vocabulary standards Support both messaging and structured document approaches for submitting data to BIS Monitor/ contribute / review IHE Laboratory Documents (IHE CDA-2) to assure biosurveillance needs are met Provide tools and other services that assist hospitals and laboratories in standardizing their laboratory messaging and vocabulary. This includes properly mapping laboratory information into the agreed to standard messages and translating local codes to standardized codes Provide tools that can securely transport laboratory messages to the intended recipient. Example: Eclipse Open Healthcare Frameworks to identify status Define conformance measures for laboratory reporting standards. Regenstrief is developing a tool called "HL7-Lint" which examines messages for conformance to HL7, and identifies some of the most common HL7 errors (e.g. units in the wrong field, etc.). This tool is used to examine messages from new data providers as an initial step in the message-standardization and term-mapping process. Further steps are needed to review tool requirements for fulfillment of domain testing /coordinate with LOINC Work with LOINC to develop a richer set of orderable laboratory test panels within the LOINC coding system. Work with the Council of State Territorial Epidemiologists Public Health Informatics Subcommittee to define a common national standard specification for laboratory data reporting GENERAL Monitor / contribute / review HL7 CTS (Nascent Standard) and HL7 PHER SIG to assure that biosurveillance needs are met Work with CSTE/CDC to harmonize public health reporting requirements mandated by state laws (reportable conditions) and identified by CDC (notifiable conditions) with regards to presumptive or confirmed cases of diseases/conditions Work with AHIC to define biosurveillance data set.
1.2.3.0	Format data required by Public Health Agencies		
1.1.4.0	Identify Public Health Agencies that must be notified	LAB, VISIT UTILIZATION There is a need to define dataflow between clinical care and local, state and federal public	Work with AHIC to define dataflow between clinical care and local, state and federal public health agencies for biosurveillance

Event Code	Event Description	Identified Gaps	Recommended Resolution
1.2.4.0	Identify Public Health Agencies that must be notified	health agencies for biosurveillance	
1.1.5.0	Transmit relevant data to Public Health Agencies	Additional security standards refinement and profiling are needed. LAB, VISIT, UTILIZATION Need to define biosurveillance data set	Monitor / contribute/ review ISO TC215 Health Informatics WG4 NWIP Audit Monitor / contribute/ review IHE PCC Patient Consent/Authorizations profile for access to medical records in the current cycle to assure support for consent override for public health purposes, which would be included in a disclosure log
1.2.5.0	Transmit relevant data to Public Health Agencies		
1.3.1.0	Provide listing of required biosurveillance data	LAB, VISIT, UTILIZATION Need to define biosurveillance data set Generation of required data listing is a paper/human process today Gaps in *Context, Information Exchange* and *Functionality /Process/ Workflow*	See Data Dictionary Recommendations above Work with HL7 V3 PH to review communication protocols between actors Communicate the gap to National Center for Health marketing at CDC to request a review of the problem
1.3.2.0	Receive biosurveillance data	LAB, VISIT, UTILIZATION - *Functionality/Process/Workflow*– need consistency in the level of acknowledgement (ACK)	Recommend that the biosurveillance technical framework include implementation guidance to assure a consistent process for ACK. Use RFC 2298 and RFC 2852 See security recommendations in 1.1.5.0 (overlaps)
RESOLVING GAPS: Work with SDOs / Profiling Organizations When relevant *current work* is identified: Establish Technical Committee (TC) Liaison to monitor, inform, and participate in the development process to assure that the work fills the gap When relevant *pending work* is identified: Work with organization to request acceleration Establish TC Liaison to inform and contribute to the new standard/profile development process to assure that the work is established to fill the gap Adjust the Biosurveillance Interoperability Specification roadmap to accommodate estimated timeline for completion When *no current/pending efforts* are identified: Work with organization(s) to request new standard/profile Establish TC Liaison to inform, and contribute to the new standard/profile development process to assure that the work is established to fill the gap Adjust the Biosurveillance Interoperability Specification roadmap to accommodate estimated timeline for completion of pending work When *multiple organizations have current/pending* work: Request joint development and concurrent harmonization to assure that the work is filling the gap and not introducing duplications Establish TC Liaison with each affected organization to inform, harmonize, and contribute to the concurrent development process to assure that the work fills the gap without introducing duplications Adjust the Biosurveillance Interoperability Specification roadmap to accommodate estimated timeline for completion of pending work			

4.3 STANDARD OVERLAPS

This section describes the instances where there are overlaps among standards for the Use Case. The overlap is only relative to the specific Use Case event. Overlaps refer to instances wherein some of the requirements are met by multiple standards. The overlap is only relative to the specific Biosurveillance

Use Case event. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross Technical Committee validation of the overlap, provisional recommendations and peer review by the Technical Committee's.

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

Table 4.3-1 Standard Overlaps

Event Code	Event Description	Standard Overlap	Recommended Resolution
1.1.2.0 1.2.2.0	Anonymize data required by Public Health Agencies	See access control below	See access control Below
1.1.3.0 1.2.3.0	Format data required by Public Health Agencies	UTILIZATION *Information Exchange* - Bed availability - HL7 V2.x: 4 candidate messages - Potential overlap: OASIS HAVE LAB *Information Exchange* – Lab Results *Message* – Result Interpretation - DICOM / HL7 *Terminology* - Specimen / Body Site: - HL7 / foundational model of anatomy / LOINC / SNOMED / DICOM *Terminology* – Presumptive Diagnosis: - HL7 / SNOMED / ICD9/ ICD10 VISIT *Information Exchange* – Visit data messages - Potential Overlap HL7/X12 *Terminology* - Presumptive Diagnosis: - HL7 / SNOMED / ICD9/ ICD10 LAB, VISIT, UTILIZATION *Information Context* - Possible Overlap for information models - ASTM / HL7 / DICOM / ADA / ISO	Work with HL7 to assess recommendations for bed/resource availability: address at the next meeting of HL7 name a liaison to carry the issue compare to OASIS HAVE HL7 Order Result is recommended for human results interpretation, whereas DICOM is recommended for machine - generated results Review and assess relevant work to express Specimen Site and Presumptive DX Work with SDOs to harmonize standards, e.g. define mapping translations from one message-type to the other Identify the appropriate information model Review best practices in laboratory data management such as CAP, JCAHO, CDC, National Patient Safety Laboratory Guidelines, CMS, CLSI, NACB, and centers of laboratory excellence
1.1.5.0 1.2.5.0	Transmit relevant data to Public Health Agencies	***Multiple security standards identified do not represent overlapping standards in security.*** These standards and profiles may vary based upon architecture. ASTM E2085 and E2086 provide guidance for selection of engineering standards, but do not include guidance on newer technologies. See access control below	Review and update ASTM E2085 and E2086 to include guidance for new WS, ISO, and engineering standards. See access control below

Event Code	Event Description	Standard Overlap	Recommended Resolution
access control	Manage and Control Data Access	Overlap: ANSI/INCITS 359 for RBAC Possible Overlap: ANSI/INCITS 359 with ASTM E1985	Recommend review and harmonization of ASTM E1985 with ANSI/INCITS 359
RESOLVING DUPLICATION AND OVERLAPS: When overlap is *within* the standard: work with SDO to resolve internal issue (e.g. HL7 bed availability) When overlap is *across* standards: work with affected SDOs through joint meetings (e.g. SNOMED/LOINC) translation mapping for data standards (e.g. CCR/CDA-2) request SDOs to jointly conduct harmonization (e.g. SNOMED/LOINC) Apply evaluation criteria (e.g. current use, ease of implementation for Use Case, etc) to select standards for Interoperability Specification until harmonization between identified overlapping standards is complete Once harmonization is complete, update the Interoperability Specification accordingly			

4.4 RESOLUTION PLAN SUMMARY

Following the discussion on the standards gaps and overlaps in Section 4.2 and 4.3, Table 4.4-1 shows the summary of the resolution plans that HITSP has established to address those standards gaps and overlaps that were identified.

Table 4.4-2 Resolution Plan

Date	Task to be accomplished and who is involved
Filter Data Required by Public Health Authorities	
2005/2006	Monitored / contributed/ reviewed IHE Retrieve Form for Data Capture (RFD) to assure biosurveillance needs were met for reportable filters and supplemental data elements for conditions reported to public health agencies
2006/2007	IHE-RFD work product was developed in full consideration of HITSP contribution and clinical Use Cases. Work product adopted as part of this specification. Recommend to work with continuing efforts in the 2006-2007 project year to automate mapping of source data elements from Clinical Information System to form content Work with LOINC and SNOMED to achieve the appropriate level of granularity Link test orders to test results Work with ICD and SNOMED to review vocabulary requirements for presumptive DX CMS-validated mapping between SNOMED-CT and ICD9-CM (while more clinical granularity as provided by SNOMED, current systems are using ICD-9-CM for morbidity coding) Approach HL7 and OASIS IHC to coordinate standards development efforts for formalizing rule specification for consistent screening of cohort selection Monitor and contribute to IHE efforts to establish tracking capabilities for specimens as they move from the local level to the state level and federal level (IHE PCC Case Management PH Lab profile; Also will need to monitor and contribute to the IHE-XCA through HITSP Cross-TC efforts and IHE-RFD tagging items.) Refer the SNOMED/Reportable conditions mapping request to Foundations Committee, including clarification of reportable conditions definition An IHE RFD profile update regarding security considerations for RFD is under way. The TC will monitor and contribute to this IHE effort
2007/2008	The HITSP Population TC is monitoring three IHE work items that address content filtering: IT Infrastructure Publish and Subscribe, Patient Care Coordination Care Focused Care Management, and Quality Care Management/Content Infrastructure

Date	Task to be accomplished and who is involved
Anonymize Data Required by Public Health Agencies	
2005/2006	While DICOM Supplement 55 is published, it but references radiology research within an organization; The pseudonymization and anonymization principles addressed in this specification conform to the ISO TC215 /DTS 25237. HITSP recognizes that ISO/DTS 25237 is a draft standard and informal Liaison relationship is established to Monitor, contribute, and review the development of the ISO TC215 Health Informatics Pseudonymisation technical specification Re-identification out of scope in current Use Case, and given the interim status of DTS 25237, re-identification specification is deferred. HITSP anticipates that this ISO TC215 technical specification will address re-identification methodologies for re-identification
2006/2007+	HITSP will continue to monitor, contribute, and review the development of the ISO TC215 Health Informatics Pseudonymisation technical specification ISO/DTS 25237. Updates will be made to this HITSP specification to conform to any changes that impact this specification Re-identification is a policy issue and that the action be the responsibility of the pseudonymization services. ISO TC215/TS 25237 is expected to address re-identification. This HITSP specification will be updated to include re-identification methodologies in conformance with the ISO TC215 specification
Harmonize OASIS HAVE and HL7	
2005/2006	Joint meetings were started in May 2006. As a result, a plan was developed to integrate the HAVE Concepts into the HL7 messaging structure to capture bed availability from HL7 enabled environments. This approach has been detailed in this Interoperability Specification
2006/2008	OASIS HAVE Specification is under public comment and review. Anticipate this to be a final approved standard by mid-year 2008 *Need for Further Harmonization* In order to facilitate improvements in future healthcare utilization information interchange standards, HITSP recommends that OASIS and HL7 work collaboratively to develop a single, unified resource utilization specification, including both information exchange and terminology standards, to meet the needs of Biosurveillance and other stakeholders
Laboratory Report Document Support for Biosurveillance	
2005/2006	Liaisons from HITSP worked with IHE to develop the Laboratory Report Document HL7-CDA-2 implementation specification. The committee has reviewed the document out now for public comment, and updates will be made to account for these contributions in September. The results of this initiative have been incorporated into this Interoperability Specification. No additional gap is identified at this time for this document
Support Both Messaging and Structured Document Approaches for Submitting Data to BIS	
2005/2006	Both messaging and structured document approaches have been incorporated into this Interoperability Specification Document-based information sharing is included in this Interoperability Specification to align and maintain consistency with other HITSP efforts in Electronic Health Record and Consumer Empowerment. The document-based information sharing approach has not previously been considered for secondary use of data as required by Biosurveillance or other secondary use systems (e.g., clinical trials, aggregate performance measurements, disease management and population health)
2006/2007+	Evaluate expansion of specification to support additional messaging and document structures so as to enable broader options and sources for collecting Biosurveillance data The Technical Committee identified several areas for further evaluation prior to endorsing full document-based data sharing for Biosurveillance activities. These areas for evaluation include: Methodology and criteria for publish and subscribe capability such that subscription filtering can be modified in real time as the situation requires Document Sharing Service requirements to meet the needs of public health and, potentially other forms of secondary data use Extent of usable information within documents; i.e., structured Vs human readable text, and the extent of natural language processing required to enable document sharing as a viable Biosurveillance solution. The evaluation should include the extent to which document-based sharing encapsulates message-based standards that correlate with the message-based functional flow as detailed elsewhere in this document Implementation sites are encouraged to explore and research these areas of concern to provide additional evidence for more robust usage of document-based information sharing for secondary usage of data

Date	Task to be accomplished and who is involved
2007/2008	Participated in IHE white paper development for infrastructure to support Health Information Re-use. Submitted a profile proposal to IHE for Publish and Subscribe capabilities to support Health Information Re-use, including public health surveillance. This profile is accepted and is under development
Need to Have More Detail on the Essential Data Set	
2005/2006	HITSP communicated the need for a Biosurveillance Data Dictionary to ONC. In response to this request, the AHIC Biosurveillance Data Steering Committee has been established. This group began meeting in June 2006. Liaisons were established between this steering committee and HITSP. These two groups worked in parallel to comply with early data dictionary requirements in the current implementation specification HITSP has indicated through the liaisons that further specificity is needed to accommodate the request for Laboratory and Radiology Orders. These will be moved to address in the 2006-2007 project year
2006/2007+	HITSP will work with the AHIC Biosurveillance Data Steering Committee to expand the data dictionary and to expand the Interoperability Specification to address additional data elements and data sources identified by this steering committee HITSP will work with the AHIC Biosurveillance Data Steering Committee to identify more sophisticated query support for the shared document resource functional flow scenario to enhance the functionality of the implementation in support of identification, monitoring, and management of public health threats Monitor / contribute/ review IHE PCC Patient Consent/Authorizations profile for access to medical records in the current cycle to assure support for consent override for public health purposes, which would be included in a disclosure log
2005/2006	This work has been completed. The resulting IHE-BPPC has been included in this technical specification for the purposes of supporting audit and verification of authorization to collect PHI for biosurveillance purposes
Resolve an Overlap between HL7 and DICOM	
2005/2006	This work is completed: HITSP Guideline developed to address this overlap as follows: When human analysis is to be provided, an HL7 Order Result is the appropriate means to deliver the data When machine analysis is to be provided, DICOM is the most appropriate For attachments to Order Results, use HL7 for human analysis and DICOM for machine analysis and for images. DICOM has a variety of image object specifications, ranging from the "Secondary Capture" object used as the most generic container through specific objects for CT and MR to highly specialized objects such as the Ophthalmic OCT image and Intravascular Ultrasound objects. The specific object type to be used depends on the kind of image being attached More specific guidance as to appropriate DICOM content can typically be found in part 3, and more specific guidance as to appropriate vocabulary for that content can be found in part 16 - e.g., Basic Diagnostic Imaging Report (TID 2000), Chest CAD analysis (TID 4100), etc
Semantic Interoperability	
2005/2006	HITSP has identified semantic interoperability to be highly important to the progress of work in Biosurveillance having developed the following statement: 'Improving data standardization processes is a crucial step in achieving the long-term goal of semantic interoperability. An initial step toward achieving this goal is to establish a framework for exchanging clinical information, whether the data are currently in freeform text or standardized, machine-readable format.'

Date	Task to be accomplished and who is involved
2006/2007+	HITSP recognizes that this is a highly complex area, with a long-term timeline. This TC will establish Liaisons with existing efforts in semantic interoperability. These liaisons will work through HL7 and OASIS to propagate this work into standards. Continuous evaluation will be done for each new Interoperability Specification development to embrace these standards as they are developed The usefulness of near real-time biosurveillance information depends on the degree to which data collected from disparate sources are semantically interoperable. Semantic interoperability – the communication of full and commonly understood meaning across systems – will be optimized through achievement of the following objectives: Precise definition of the concepts being communicated, taking context into account where appropriate; Identification of common term sets used to communicate those concepts; Where multiple term sets exist for a concept, mapping of identical or synonymous terms across term sets These objectives can be achieved in phases, the first of which is the enumeration of standards for messaging between actors in the biosurveillance scenarios, which has been done in the 2006 HITSP Biosurveillance initiative. On an ongoing basis, concepts within these messaging standards should be enumerated, and appropriate vocabulary selection and mapping performed. This identification and mapping process will not be completed within the first annual cycle. The steps needed to achieve these ultimate objectives must be integrated into the HITSP development roadmap
Publish and Subscribe	
2005/2006	Recommend that IHE review and identify a mechanism for publish and subscribe in support to public health
2006/2007	Work with IHE to develop a mechanism for publish and subscribe in support to public health
2007/2008	Work with IHE on the Publish and Subscribe Profile
XDS Stored Query Gap	
2005/2006	Gap - Request IHE-ITI Change Proposal to add stored query support; Add constraint for 2005/2006 cycle
2007/2008	As part of the IHE IT Infrastructure Publish and Subscribe Profile, supporting stored queries are under review
Penetration of Clinical Information Systems	
2006/2007+	Gap - Process issue – gap is in clinical systems – clinical systems are in ordering/administrative issues/process – system investment issue/clinical – identified as a challenge in original Use Case – penetration of clinical systems is an issue: Continue to expand support for additional clinical data information exchange standards and document types

Date	Task to be accomplished and who is involved
Codify Data from Freeform Text	
2005/2006	HITSP has identified codification of freeform text to be highly important to the progress of work in Biosurveillance having developed the following statement: Clinical data are often recorded in an unstructured, freeform text format. In order to maximize the value of freeform text data for use in biosurveillance systems, translation into standardized, machine-readable codes is necessary. As a near-term incremental proposal, HITSP recommends that sending or receiving systems assume responsibility for translating freeform text data for the AHIC -defined biosurveillance data set Improving data standardization processes is a crucial step in achieving the long-term goal of semantic interoperability. An initial step toward achieving this goal is to establish a framework for exchanging clinical information, whether the data are currently in freeform text or standardized, machine-readable format The data elements identified in the AHIC Biosurveillance Use Case that are routinely captured as freeform text include: • Chief complaints • Nursing / Triage Notes • Radiology impressions • Microbiology results Due to the volume of freeform text data requiring standardization, human review of all data are infeasible and automated text processing techniques, such as natural language processing (NLP) are needed to translate data into standardized formats. Further research addressing the challenges inherent in automated mapping of freeform text to SNOMED, ICD-9/10, LOINC and other terminologies is needed. HITSP recommends that developing and disseminating standards and best practices for automated text processing techniques should be a priority. This technology has applicability to other areas outside of Biosurveillance, and would include processes for establishing semantic context, negation, exclusion criteria, and others.' Methods for standardizing chief complaints and nursing notes are needed. A nursing terminology that provides a standardized terminology framework, such as the Clinical Care Classification, for documenting coding and tracking nursing care in any healthcare setting may be applicable for this purpose. HITSP recommends that SDOs in nursing and other clinical domains harmonize and present the benefits for biosurveillance and other secondary use efforts to provide value in long term semantic interoperability efforts Diagnosis/injury code and associated cause may be addressed in ICD-9 and associated E-codes, but further study is needed.
2006/2007+	HITSP recognizes that this is a highly complex area, with a long-term timeline. This TC will establish Liaisons with existing efforts in semantic interoperability. These liaisons will work through HL7 and OASIS and other SDOs to propagate this work into standards. Continuous evaluation will be done for each new Interoperability Specification development to embrace these standards as they are developed Monitor and contribute to IHE Patient Care Coordination Technical Framework update to release 2.0. Update relevant references and constraints to these documents
2007/2008 Resolution Update	A consensus discussion for HITSP resolved that: " This Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT." This resolution was originally reached by consensus of the ER-EHR Work Group members, as well as the Subject Matter Experts that were invited to join the discussion. These Subject Matter Experts included nursing terminology experts from the key stakeholder groups including the ANA-CNPII, ICNP, Clinical Care Classification, Omaha System, SNOMED, as well as vendors and representatives of other clinical disciplines. The resolution will be included in the ER-EHR Interoperability Specification and for consistency across HITSP should also be used as a minor update to the Biosurvelliance and Quality Interoperability Specifications. It will also be considered for reuse in all of our subsequent work

Date	Task to be accomplished and who is involved
Identify Communication Recipients	
2005/2006	Our specification assumes point-to-point and as a result is not applicable Our assumption is that there is more than 1 recipient of biosurveillance data in subsequent HITSP cycles Scoped out as an architecture/infrastructure issue
2006/2007+	Assess use of ISO TC215 ISO/TS21091 and other standards to facilitate communication among recipients
2007/2008	Monitor and contribute to HITSP Consumer Empowerment efforts in this area
Nursing Terminology	
2005/2006	Recommend to provide a patient care documentation terminology by nursing SDOs and other clinical domains for the representation of the benefits of the healthcare process in biosurveillance and for other secondary use and semantic interoperability efforts
2007/2008 Resolution Update	A consensus discussion for HITSP resolved that: " This Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT." This resolution was originally reached by consensus of the ER-EHR Work Group members, as well as the Subject Matter Experts that were invited to join the discussion. These Subject Matter Experts included nursing terminology experts from the key stakeholder groups including the ANA-CNPII, ICNP, Clinical Care Classification, Omaha System, SNOMED, as well as vendors and representatives of other clinical disciplines. The resolution will be included in the ER-EHR Interoperability Specification, and, for consistency across HITSP should also be used as a minor update to the Biosurvelliance and Quality Interoperability Specifications. It will also be considered for reuse in all of our subsequent work
Radiology/Laboratory Order Message	
2005/2006	HITSP has developed the following statement for review and consideration by the AHIC Biosurveillance Data Steering Committee: Pre-existing information contained in clinical orders may be used as early warning indicators for events of public health significance. Because clinical orders contain information describing patients and the types of clinical tests requested, the Biosurveillance Use Case for laboratory and radiology orders seeks to "re-use" this pre-existing information, and consequently represents a "secondary" use of such data The Biosurveillance order Use Case is dependent on the primary Use Case developed for Laboratory and Radiology ordering. The selection of messages to be used for Laboratory and Radiology orders should be driven by the primary Use Case for orders, not a more limited secondary Biosurveillance Use Case. Consequently, we advocate that Biosurveillance should not dictate the order message(s) used to convey Laboratory and Radiology orders. Rather, the Biosurveillance work group should ensure that the information necessary for public health surveillance is included in order messages. We propose that any preliminary document developed for the Biosurveillance Use Case would maximally identify candidate messages that could contain the information of interest, and the location of the desired information in each transaction Also of crucial importance is that the most common order message used for both Laboratory and Radiology orders today (the ORM^O01) has been temporarily retained for backward compatibility, but not recommended for use in HL7 2.5. Subsequently, the 2.5 order messages that may be selected by HITSP may *not* be the most universally implemented message for orders. For Biosurveillance to take advantage of the information found in orders, we must focus on where surveillance information can be found in a variety of order message types, not just a single order message type that is dictated for a Biosurveillance Use Case To be broadly applicable, the Biosurveillance Use Case should leverage clinical order transactions commonly exchanged among clinical healthcare stakeholders, as well as public health entities. It should be noted that the laboratory order message selected by PHIN is intended for a narrow Use Case for messaging orders between public health laboratories, which has limited application to the Biosurveillance and EHR Use Cases
2006/2007+	HITSP will continue to work with AHIC Biosurveillance Data Steering Committee to enhance support for additional data element added to the data dictionary
2006/2007	Provided an SDO referral documenting the Lab Order issues

Date	Task to be accomplished and who is involved
Terminology and Data Value Issues	
2005/2006	Identified issues
2006/2007+	Work with SDOs to resolve gaps and overlaps in this area:
	Date and Time Illness Onset : This remains a gap for which HITSP issues a recommendation to HL7 and ASTM to align concepts and vocabulary and produce a harmonized result
2006/2007	Provided an SDO referral documenting the terminology and data value issues
Laboratory and Radiology Test Orders	
	Order number :This remains a gap for which HITSP issues a clarification request from HL7 to attain a broadly accepted meaning for order number;
	Order test name :This remains a gap for which HITSP issues a recommendation to LOINC, SNOMED-CT, and CPT to develop and harmonize a suitable coded value set to express order test name
	Collection method :This remains an overlap for which HITSP issues a recommendation to subset SNOMED-CT for clarification and for SNOMED and HL7 to align subset with HL7 Table 488
	Ordered test and Resulted test :Lack of a universal vocabulary remains a major gap for which HITSP issues a recommendation that SNOMED-CT, LOINC, CPT, HCPCS and others (encouraging commercial vendor participation) work together to establish a suitable and harmonized vocabulary
	Standards Evaluation Process
2005/2006	HITSP conducted assessment of demographic and clinical encounter data using the USHIK metadata registry. The TC Recommends further use of USHIK metadata registry in comparison and evaluation of standards in future work as part of the standards evaluation/selection process. (www.ushik.org/hitsp)
2006/2007+	Utilize the USHIK metadata registry to assist in comparison and evaluation of standards as part of the standards evaluation/selection process. Provided an SDO referral documenting the terminology and test order issues
Policy Gap	
2005/2006	This approach has been incorporated into this Interoperability Specification. Refer to AHIC Security/Privacy group
2006/2007	Identify a liaison to the AHIC Security/Privacy group to carry the policy gap issue forward and to harmonize with TC efforts
Addition of Security Constructs	
2007/2008	The revisions in this construct are intended to leverage the security and privacy Transaction Packages, Transactions, and Constructs to fulfill Use Case requirements and possible policy-driven requirements. The construct modifications are under review in conjunction with the review of these security constructs. This document should be reviewed in conjunction with any changes to the security and privacy constructs

5.0 TECHNICAL IMPLEMENTATION

5.1 CONFORMANCE

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

5.1.1 CONFORMANCE CRITERIA

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

Claims of conformance to this specification must be made using the following language:
This product conforms to HITSP's Biosurveillance specification, available at www.hitsp.org.

5.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

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

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

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

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

5.1.3 TEST METHODS

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

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

6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF STANDARDS

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

Table 6.1-1 Description of Standards

Standard Name	Description
American Medical Association (AMA) Current Procedural Terminology (CPT®) Fourth Edition (CPT-4)	A uniform coding system used primarily to identify medical services and procedures furnished by physicians and other healthcare professionals. For more information visit www.ama-assn.org
American Society for Testing and Materials (ASTM) 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 non-repudiation 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
Federal Information Processing Standards (FIPS) Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas Publication # 5-2, May, 1987	A set of two-digit numeric codes and a set of two-letter alphabetic codes for representing the 50 states, the District of Columbia and the outlying areas of the United States, and associated areas. The standard covers all land areas under the sovereignty of the United States, the freely associated states of Federated States of Micronesia and Marshall Islands, and the trust territory of Palau. For more information visit www.itl.nist.gov. NOTE: ASC X12 transactions and ASC X12N Implementation Guides do not allow use of this standard; instead they require use of the U.S. Postal Service's National Zip Code and Post Office Directory -- which provides similar alphabetic code values

Standard Name	Description
Health Level Seven (HL7) Clinical Document Architecture Release 2 (CDA R2)	The HL7 Clinical Document Architecture is an XML-based document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA is one instantiation of HL7's Version 3.0 Reference Information Model (RIM) into a specific message format. Of particular focus for HITSP Interoperability Specifications are message formats for Laboratory Results and Continuity of Care (CCD) documents. Release 2 of the HL7 Clinical Document Architecture (CDA) is an extension to the original CDA document markup standard that specifies the structure and semantics of clinical documents for the purpose of exchange. CDA R2 includes a prose document in HTML, XML schemas, data dictionary, and sample CDA documents. CDA R2 further builds upon other HL7 standards beyond just the Version 3.0 Reference Information Model (RIM) and incorporates Version 3.0 Data Structures, Vocabulary, and the XML Implementation Technology Specifications for Data Types and Structures. For more information visit www.hl7.org
Health Level Seven (HL7) U.S. Realm - Interoperability Specification: Lab Result Message to EHR (ORU^R01) (HL7 Version 2.5.1) September, 2007	This guide contains the necessary specifications for clinical laboratory results reporting to EHRs for use in the U.S. Realm. For more information visit www.hl7.org
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. For more information visit www.hl7.org
Health Level Seven (HL7) Version 2.5.1	The HL7 Version 2.5.1 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 4, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. They are also used in HL7 order messages. For more information visit www.hl7.org
Health Level Seven (HL7) Version 3.0 Privacy Consent related specifications RCMR_RM010001 - Data Consent	The Data Consent RMIM captures the data and associations needed to (1) record or report a consumer's consent or dissent to authorize the access, collection, use, or disclosure of personally identifiable information; (2) convey a provider's request or intent to override a patient's recorded consent or dissent; (3) convey a type of consent directive associated with a privacy policy; or (4) to record or report a consumer's consent directive, which is to be applied to future access, collection, use or disclosure of personally identifiable information. For more information visit www.hl7.org

Standard Name	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise User Assertion (XUA)	The Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the user identity of an authenticated principal (user, application, system...) in transactions that cross enterprise boundaries. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the entities, and others that may have chosen to use a third party to perform the authentication. The latest version of the IHE framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement Volume 3 – Document Digital Signature (DSG) Content Profile	Specifies the use of digital signatures for documents that are shared between organizations. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 3.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev.3.0 for Final Text, specifies the IHE transactions defined and implemented as of December 9, 2006. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Consistent Time (CT) Integration Profile	The Consistent Time Integration Profile (CT) provides a means to ensure that the system clocks and time stamps of the many computers in a network are well synchronized. This profile specifies synchronization with a median error less than 1 second. This is sufficient for most purposes. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE CT Integration Profile, and other transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) Supplement - ITI-25 Notification of Document Availability (NAV) Jun 28, 2005	The capability for automation of critical workflows used in healthcare has been greatly advanced by the introduction of the Cross-Enterprise Document Sharing Integration Profile. However, without point-to-point notification of document availability, these workflows still require manual interactions between parties using document sharing. The Notification of Document Availability Integration Profile (NAV) introduces a mechanism allowing notifications to be sent point-to-point to systems and users within an affinity domain, eliminating the need for manual steps or polling mechanisms. This basic mechanism is only intended to facilitate the common part of a large range of workflows related to notifying a remote party (user or system) that one or more documents have been registered in an XDS Registry and may be retrieved if the notified party wishes. For further information, visit www.ihe.net

Standard Name	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. Section 10, Cross-Enterprise Document Sharing facilitates the registration, distribution and access across health enterprises of patient electronic health records. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b)	The Cross-Enterprise Document Sharing-B Profile (XDS.b) supplement provides a new implementation choice for the Cross-Enterprise Document Sharing (XDS) Integration Profile based on use of the Web Services and ebXML Reg/Rep standards that is consistent with current developments and best practices in the industry. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement [ITI-18]	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The Registry Stored Query Transaction Trial Implementation Supplement specifies an IHE transaction that provides optimization and implementation simplification. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 XCA Supplement	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The trial implementation version of the XCA Supplement to the ITI-TF, rev. 4.0 Final Text, specifies the IHE transactions that support access between communities in a manner compatible with the XDS Integration profile. This supplement is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Patient Identifier Cross-Referencing Integration Profile (PIX)	The Patient Identifier Cross-referencing Integration Profile (PIX) is targeted at healthcare enterprises of a broad range of sizes (hospital, a clinic, a physician office, etc.). It supports the cross-referencing of patient identifiers from multiple Patient Identifier Domains via the following interactions: 1)The transmission of patient identity information from an identity source to the Patient Identifier Cross-reference Manager. 2) The ability to access the list(s) of cross-referenced patient identifiers either via a query/ response or via update notification. By specifying the above transactions among specific actors, this integration profile does not define any specific enterprise policies or cross-referencing algorithms. By encapsulating these behaviors in a single actor, this integration profile provides the necessary interoperability while maintaining the flexibility to be used with any cross-referencing policy and algorithm as deemed adequate by the enterprise.. The latest version of the IHE Technical Framework is available at www.ihe.net
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles, offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 4.0 for Final Text, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net

Standard Name	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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (TF) 2007 – 2008 Supplement, Retrieve Form for Data Capture (RFD)	provides a method for gathering data within a user's current application to meet the requirements of an external system. RFD supports the retrieval of forms from a form source, display and completion of a form, and return of instance data from the display application to the source application. The profile relies upon XForms technology to support negotiation between the form display and form provider systems, so that iterative exchanges can deal with issues like form selection, completion of a series of forms, partial completion of forms, returning to forms partially filled out in earlier sessions. RFD also supports archiving a copy of the completed form
Integrating the Healthcare Enterprise (IHE) Laboratory Technical Framework Volume 3 (LAB TF-3) Document-based Transactions, Revision 2.0 - For Trial Implementation, August 16, 2007	The IHE Laboratory Technical Framework introduces a content Integration Profile Sharing Laboratory Reports (LAB TF-3) that describes a clinical laboratory report as a human-readable electronic document. This document, which may also contain data in a machine-readable format and contains the complete set of final results produced by a clinical laboratory in fulfillment of one or more test orders for a patient. This document is focused on the sharing of sets of laboratory results in the form of a laboratory report structured document, and is not intended to address ordering or return of laboratory results to the ordering provider. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Patient Care Coordination (PCC), Revision 3.0, 2007 - 2008, Cross-Enterprise Sharing of Medical Summaries (XDS-MS) Integration Profile	The IHE Patient Care Coordination Technical Framework (PCC TF) defines specific implementations (called Integration Profiles) of established standards to deal with integration issues that cross providers, patient problems or time. The Cross Enterprise Document Sharing of Medical Summaries (XDS-MS) Integration Profile enables sharing of health information between enterprises of a regional health network, and further describes how to map content in a CDA medical document into registry metadata. In the registry, healthcare providers publish pointers to documents stored in distributed repositories. Other healthcare providers may search and retrieve these and other documents. For more information visit www.ihe.net
Integrating the Healthcare Enterprise (IHE) Radiology Technical Framework Revision 8.0	The IHE Radiology Technical Framework specifies the Cross-Enterprise Document Sharing for Imaging (XDS-I) Integration Profile which enables sharing of imaging documents such as radiology images and reports across healthcare enterprises. XDS-I extends XDS by sharing, locating and accessing DICOM instances from its original local sources, e.g. for radiologists or oncologists. For more information visit www.ihe.net
International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS)	The International Classification of Diseases, 10th Revision, Procedure Coding System (ICD-10-PCS), describes the classification of inpatient procedures for statistical purposes and for the indexing of healthcare records by procedures. ICD-10-PCS is a procedural coding system managed by the Centers for Medicare and Medicaid Services (CMS). For more information visit www.cms.hhs.gov. Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values

Standard Name	Description
International Classification of Diseases, 10th Revision, Related Health Problems (ICD-10-CM)	The International Classification of Diseases, 10th Revision, Clinical Modification (ICD-10-CM), describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases. The National Center for Health Statistics (NCHS), the Federal agency responsible for use of the International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) in the United States, developed a clinical modification of the classification for morbidity purposes. For more information visit www.cdc.gov/nchs. Note: While ICD-10 is not deployed in US installations, we recognize the need to move toward new releases of coded values
International Classification of Diseases, 9th Revision, Clinical Modifications (ICD-9-CM)	The International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM), Volumes I, II (diagnoses) and III (procedures) describes the classification of morbidity information for statistical purposes and for the indexing of healthcare records by diseases and procedures. For more information visit www.cdc.gov/nchs
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	SNOMED CT consists of a technical design, core content architecture, and Core content. SNOMED CT Core content includes the technical specification of SNOMED CT and fully integrated multi-specialty clinical content. The Core content also includes a concepts table, description table, relationships table, history table, ICD-9-CM mapping, and Technical Reference Guide. Additionally, SNOMED CT provides a framework to manage language dialects, clinically relevant subsets, qualifiers and extensions, as well as concepts and terms unique to particular organizations or localities. For more information visit www.ihtsdo.com
International Organization for Standardization (ISO) Health informatics -- Pseudonymisation, Unpublished Technical Specification # 25237	Health Informatics – Pseudonymisation. Approved as a Technical Specification March, 2007. For more information visit www.iso.org
Internet Engineering Task Force (IETF) Network Time Protocol (Version 3) Specification, Implementation and Analysis, "Request for Comment" (RFC) # 1305, March, 1992	Describes the Network Time Protocol (NTP): the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet operating at rates from mundane to lightwave. For more information visit www.ietf.org
Internet Engineering Task Force (IETF) Simple Network Time Protocol (SNTP) Version 4, "Request for Comment" (RFC) # 2030, October, 1996	Describes the Simple Network Time Protocol (SNTP) Version 4, which is an adaptation of the Network Time Protocol (NTP). SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP Version 4 involves no changes to the NTP specification or known implementations, but is rather a clarification of certain design features of NTP. For more information visit www.ietf.org
Logical Observation Identifiers Names and Codes (LOINC®)	A database of universal identifiers for laboratory and other clinical observations. The laboratory portion of the LOINC database contains the usual categories of chemistry, hematology, serology, microbiology (including parasitology and virology), and toxicology; as well as categories for drugs and the cell counts typically reported on a complete blood count or a cerebrospinal fluid cell count. Antibiotic susceptibilities are a separate category. The clinical portion of the LOINC database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments, and other clinical observations. For more information visit www.loinc.org
National Uniform Billing Committee (NUBC) Uniform Bill Version 1992 (UB-92) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	A code set identifying status of patient discharge on an institutional claim (e.g., inpatient, outpatient, hospice, home care). For more information visit www.nubc.org
National Uniform Billing Committee (NUBC) Uniform Bill Version 2007 (UB-04) Current UB Data Specification Manual Field 22, Patient Discharge Status, Codes	A code set identifying status of patient discharge on an institutional claim (e.g., inpatient, outpatient, hospice, home care). For more information visit www.nubc.org

Standard Name	Description
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 OASIS Standard; ITU-T X.1141	SA SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Toke Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XCML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit www.oasis-open.org
Unified Code for Units of Measure (UCUM)	A code system intended to include all units of measures being contemporarily used in international science, engineering, and business. The purpose is to facilitate unambiguous electronic communication of quantities together with their units. The focus is on electronic communication, as opposed to communication between humans. For more information visit aurora.regenstrief.org

6.2 BIOSURVEILLANCE GLOSSARY

There is an additional glossary for the Biosurveillance Interoperability Specifications.

6.3 AHIC MINIMUM DATA SET USHIK CROSS-REFERENCE

6.3.1 CROSS-REFERENCE TABLE KEY

Table 6.3.1-1 Data Elements Cross-Reference

DATA ELEMENTS CROSS REFERENCE	
Data Element	Definition
AHIC Data Element	Data element name/identifier as listed by American Health Information Community and the Biosurveillance Data Steering Group (BDSG).
HITSP-Selected Standards	The Standard(s) from which the element(s) chosen by HITSP originate
SDO Name	SDO's Name for the elements(s) or Terminology(ies) chosen by HITSP
Link	If not loaded into USHIK, the link to other online source
SDO Source Definition	Definition or description of the elements(s) or Terminologies chosen by HITSP

SDO Datatype	Datatype of the intended standard element
SDO Codes & Representations	Chosen Standard's representation or code set for the element

6.3.2 BASE FACILITY DATA ELEMENTS

Table 6.3.2-1 Base Facility Data Elements

BASE FACILITY DATA ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Facility Identifier	HIPAA National Provider Identifier	National Provider Identifier	www.cms.hhs.gov/NationalProvIdentStand/	10-position all-numeric identification number assigned by the NPS to uniquely identify a healthcare provider.	Numeric	N10
Facility Name		None Available			String	Example: St. Joseph's Hospital
Facility Location	FIPS 55-3 [NIST] GNIS [USGS]	None Available	www.itl.nist.gov	None	2 character alpha	Example: TX
Number of Facility Beds	HL7-defined	None Available	http://www.hl7.org	None	HL7-defined numeric data type	Example: 530
Number of Licensed Beds	HL7-defined	None Available	http://www.hl7.org	None	HL7-defined numeric data type	Example: 205

6.3.3 DAILY FACILITY SUMMARY REPORT ELEMENTS

Table 6.3.3-1 Daily Facility Summary Report Elements

DAILY FACILITY SUMMARY REPORT ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Admissions last 24 hours	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 150
Discharges last 24 hours	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 150
Deaths last 24 hours	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 4
Clinical Status	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	

DAILY FACILITY SUMMARY REPORT ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Facility Status	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	
Facility Operations	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	
Staffing	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	
Decontamination Capacity	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	
EMS Traffic Status	HAVE values as in AHIC definition [OASIS]				To be determined when HAVE becomes a final standard	
EMS Capacity	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: triageRed 5 triageYellow 10 triageGreen 30 triageBlack 50 commentText None
EMS Census	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: triageRed 3 triageYellow 7 triageGreen 25 triageBlack 45 commentText None
Adult ICU	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 50
Medical Surgical	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 100
Burn	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 40
Pediatric ICU	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 50
Pediatrics	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 100
Negative Flow Isolation	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 15
Available Ventilators	HL7-defined	None Available	www.hl7.org	None	HL7-defined numeric data type	Example: 200

6.3.4 PATIENT DATA ELEMENTS

Table 6.3.4-1 Patient Data Elements

PATIENT DATA ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Pseudonymized Data Linker	None Available	None Available	None	None	Alphanumeric	Example: 123ABC
Encounter Date/Time	HL7 V2.5	None Available	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
DOB (month and year of birth)	HL7 V2.5	None Available	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Age	UCUM	None Available	aurora.regenstrief.org/UCUM/	None	None	Examples: 40 a 18 mo
Gender	HL7 V2.5	Administrative Sex	tinyurl.com/zbhls	This field contains the patient's sex. Refer to User-defined Table 0001 - Administrative Sex for suggested values	IS (Coded value for user defined tables)	A Ambiguous F Female M Male N NOT APPLICABLE O OTHER U Unknown
Zip	U.S. Postal Service Zip Code	None Available	zip4.usps.com/zip4/	None	String	Examples: 12345 12345-1234
State	Federal Information Processing Standards (FIPS 55-3) [NIST]	None Available	www.itl.nist.gov/fipspubs/fip55-3.htm	None	2-character alpha	Examples TX

PATIENT DATA ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Date/time last update	HL7 V2.5	None Available	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000

6.3.5 CLINICAL DATA ELEMENTS

Table 6.3.5-1 Clinical Data Elements

CLINICAL DATA						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Diagnosis/Injury Code	ICD9-CM, SNOMED-CT	None Available	www.cms.hhs.gov www.nlm.nih.gov/research	None	Code	ICD9-CM Examples: 0010 00581
Diagnosis Type	HL7 V2.5	Diagnosis Type	tinyurl.com/enojf	This field contains a code that identifies the type of diagnosis being sent. Refer to User-defined Table 0052 - Diagnosis type for suggested values. This field should no longer be used to indicate ""DRG"" because the DRG fields have moved to the new DRG segment. User-defined Table 0052 - Diagnosis type	IS (Coded value for user defined tables)	A - Admitting F - Final W – Working
Diagnosis Date/Time	HL7 V2.5	None Available	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Discharge Disposition	Universal Billing Codes (UB-92/NUBC CURRENT UB DATA SPECIFICATIONS MANUAL)	None Available	www.nubc.org	None	Code	

CLINICAL DATA						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Patient Class	HL7 V2.5	Patient Class	tinyurl.com/ezyhd	This field is used by systems to categorize patients by site. It does not have a consistent industry-wide definition. It is subject to site specific variations. Refer to User-defined Table 0004 - Patient Class for suggested values.	IS (Coded value for user defined tables)	B Obstetrics C Commercial Account E Emergency I Inpatient N Not applicable O Outpatient P Preadmit R Recurring patient U Unknown
Date and Time Illness Onset	LOINC code: '11368-8^Illness/Injury Onset Date/time^LN'	None Selected	www.regenstrief.org/loinc/	None	String	LOINC String with an HL7 formatted Time Stamp or a textual explanation. Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Chief Complaint	This Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT	None Available	www.nlm.nih.gov/research www.regenstrief.org/loinc/	None	Free-Form String or LOINC Tagged	Example: 11292-0^ED Chief Complaint – Patient Reported^LN'

CLINICAL DATA						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Temperature	LOINC code '8310-5^BODY TEMPERATURE^LN'; UCUM	None Available	www.regenstrief.org/loinc/ www.hl7.org aurora.regenstrief.org/UCUM	None	HL7-defined numeric data type	Example: 37 CEL
Pulse Oximetry	LOINC code: '19960-4^PULSE OXIMETRY^LN' ; UCUM	None Available	www.regenstrief.org/loinc/ www.hl7.org aurora.regenstrief.org/UCUM	None	HL7-defined numeric data type	Example: 93.9
Nursing/Triage Notes	This Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Pre-condition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT	None Available	www.nlm.nih.gov/research www.regenstrief.org/loinc/	None	String	Example: 34120-6^INITIAL EVALUATION NOTE^LN Patient skipped lunch.
Provider Identifier	None Available	None Available	None	None	Alpha-numeric	Example: 123ABC

6.3.6 LABORATORY/MICROBIOLOGY TEST ORDER ELEMENTS

Table 6.3.6-1 Laboratory/Microbiology Test Order Elements

LABORATORY/MICROBIOLOGY TEST ORDER ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Order number	None Available	None Available	None	None	None	None

LABORATORY/MICROBIOLOGY TEST ORDER ELEMENTS						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Test/Procedure Name	None Available	None Available	None	None	None	None
Test/Procedure Code	LOINC DICOM	None Available	www.regenstrief.org/loinc/	None	Alpha-numeric	None

6.3.7 LABORATORY/MICROBIOLOGY RESULT DATA

Table 6.3.7-1 Laboratory/Microbiology Result Data

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Reporting Laboratory Identifier	CLIA Unique Laboratory ID [FDA]	CLIA ID#	www.fda.gov/cdrh/clia/ www.cms.hhs.gov	None	Alpha-numeric	Example: 05D0571145
Performing laboratory	CLIA Unique Laboratory ID [FDA]	CLIA ID#	www.fda.gov/cdrh/clia/ www.cms.hhs.gov	None	Alpha-numeric	Example: 05D0571145
Report date/time	HI7 defined	None	None	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Report status	HL7 V2.5	Result Status	http://tinyurl.com/mzyyl	This field contains the status of results for this order. This conditional field is required whenever the OBR is contained in a report message. It is not required as part of an initial order. There are two methods of sending status information. If the status is that of the entire order,	ID (Coded Value)	A Some, but not all, results available C Correction to results F Final results; results stored and verified. Can only be changed with a corrected result. I No results available; specimen received, procedure incomplete O Order received; specimen not yet received P Preliminary: A verified early result is available, final results not yet obtained

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
				use ORC-15-order effective date/time and ORC-5-order status. If the status pertains to the order detail segment, use OBR-25-result status and OBR-22-results rpt/status chng - date/time. If both are present, the OBR values override the ORC values. This field would typically be used in a response to an order status query where the level of detail requested does not include the OBX segments. When the individual status of each result is necessary, OBX-11-observ result status may be used.		R Results stored; not yet verified S No results available; procedure scheduled, but not done X No results available; Order canceled. Y No order on record for this test. (Used only on queries) Z No record of this patient. (Used only on queries)
Collection date	None specified	None	None	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Collection method	HL7 V2.5 SNOMED-CT	Specimen Collection Method	tinyurl.com/qyb7z www.nlm.nih.gov/research	Describes the procedure or process by which the specimen was collected. Any nationally recognized coding system might be used for this field including SNOMED; alternatively the HL7 defined table 0488 may be used. Veterinary medicine may choose the tables supported for the components of this field as decided by their industry.	CWE (coded with exceptions)	ANP Plates, Anaerobic BAP Plates, Blood Agar BCAE Blood Culture, Aerobic Bottle BCAN Blood Culture, Anaerobic Bottle BCPD Blood Culture, Pediatric Bottle BIO Biopsy CAP Capillary Specimen CATH Catheterized CVP Line, CVP EPLA Environmental, Plate ESWA Environmental, Swab FNA Aspiration, Fine Needle KOFFP Plate, Cough LNA Line, Arterial LNV Line, Venous MARTL Martin-Lewis Agar ML11 Mod. Martin-Lewis Agar MLP Plate, Martin-Lewis NYP Plate, New York City PACE Pace, Gen-Probe PIN Pinworm Prep

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
						PNA Aterial puncture PRIME Pump Prime PUMP Pump Specimen QC5 Quality Control For Micro SCLP Scalp, Fetal Vein SCRAPS Scrapings SHA Shaving SWA Swab SWD Swab, Dacron tipped TMAN Transport Media, Anaerobic TMCH Transport Media, Chlamydia TMM4 Transport Media, M4 TMMY Transport Media, Mycoplasma TMOT Transport Media, TMP Plate, Thayer-Martin TMPV Transport Media, PVA TMSC Transport Media, Stool Culture TMUP Transport Media, Ureaplasma TMVI Transport Media, Viral VENIP Venipuncture WOOD Swab, Wooden Shaft
Specimen Source	SNOMED –CT	None Available	www.nlm.nih.gov/research	None	None	

Specimen	HL7 V2.5 Specimen Type Codes OR
	SNOMED-CT Specimen Codes
		Specimen Type	tinyurl.com/owx7w	This field describes the precise nature of the entity that will be the source material for the observation.
				
				Any physical entity that may have observations made about it may qualify as a specimen. The entry in this attribute describes the specific entity as precisely as possible, whether that is a complex organism (e.g., an ostrich) or a specific cellular mass (e.g., a specific muscle biopsy).
				
				This attribute corresponds to the first component of OBR.15 – Specimen Source and SAC.6 – Specimen Source component 1 – Specimen
					CWE (coded with exceptions)	ABS Abscess
						PELVA Abscess, Pelvic
						PERIA Abscess, Perianal
						RECTA Abscess, Rectal
						SCROA Abscess, Scrotal
						SUBMA Abscess, Submandibular
						SUBMX Abscess, Submaxillary
						TSTES Abscess, Testicular
						AIRS Air Sample
						ALL Allograft
						AMP Amputation
						GASAN Antrum, Gastric

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
				source name or code. These components, and the SPS data type, were deprecated upon the development of this segment.		
Ordered test code	LOINC code associated with test/procedure	None Available	www.regenstrief.org/loinc/ www.nlm.nih.gov/research	None	Code	None
Resulted test	LOINC Laboratory Test Identifiers	None Available	www.regenstrief.org/loinc/	None	Code	None
Result	SNOMED-CT,	None Available	www.nlm.nih.gov/research	None	Code, Numeric (hl7 TS), or Text	None
Method type	HL7 V3	Observation Method	www.hl7.org	A code that provides additional detail about the means or technique used to ascertain the observation.	HL7 Coded (CE)	Example: For Microbiology Sensitivity testing methods, MIC (Minimum Inhibitory Concentration) or KB for Kirby-Bauer (example provided by the Technical Committee)
Result unit	UCUM	None Available	aurora.regenstrief.org/UCUM	None	None	None
Test interpretation	HL7 V2.5	Abnormal Flags	tinyurl.com/k28v2	This field contains a table lookup indicating the normalcy status of the result. We strongly recommend sending this value when applicable. (See ASTM 1238 - review for more details). Refer to User-defined Table 0078 - Abnormal flags for valid entries. When the laboratory can discern the normal status of a textual report, such as chest X-ray reports or microbiologic culture, these should be reported as N when normal and A when abnormal. Multiple codes, e.g., abnormal and worse, would be separated by a repeat delimiter, e.g., A~W. User-	IS (Coded value for user defined tables)	< Below absolute low-off instrument scale > Above absolute high-off instrument scale A Abnormal (applies to non-numeric results) AA Very abnormal (applies to non-numeric units, analogous to panic limits for numeric units) B Better--use when direction not relevant D Significant change down H Above high normal HH Above upper panic limits I Intermediate. Indicates for microbiology susceptibilities only. L Below low normal LL Below lower panic limits MS Moderately susceptible. Indicates for microbiology susceptibilities only. N Normal (applies to non-

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
				defined Table 0078 - Abnormal flags		numeric results) Null No range defined, or normal ranges don't apply R Resistant. Indicates for microbiology susceptibilities only. S Susceptible. Indicates for microbiology susceptibilities only. U Significant change up VS Very susceptible. Indicates for microbiology susceptibilities only. W Worse--use when direction not relevant
Test status	HL7 V2.5	Result Status	tinyurl.com/mzyyl	This field contains the status of results for this order. This conditional field is required whenever the OBR is contained in a report message. It is not required as part of an initial order. There are two methods of sending status information. If the status is that of the entire order, use ORC-15-order effective date/time and ORC-5-order status. If the status pertains to the order detail segment, use OBR-25-result status and OBR-22-results rpt/status chng - date/time. If both are present, the OBR values override the ORC values. This field would typically be used in a response to an order status query where the level of detail requested does not include the OBX segments. When the individual status of each result is necessary, OBX-11-observ result status may be used	ID (Coded Value)	A Some, but not all, results available C Correction to results F Final results; results stored and verified. Can only be changed with a corrected result. I No results available; specimen received, procedure incomplete O Order received; specimen not yet received P Preliminary: A verified early result is available, final results not yet obtained R Results stored; not yet verified S No results available; procedure scheduled, but not done X No results available; Order canceled. Y No order on record for this test. (Used only on queries) Z No record of this patient. (Used only on queries)
Ordering Provider Identifier	HIPAA National Provider Identifier	National Provider Identifier	www.cms.hhs.gov	10-position all-numeric identification number assigned by the NPS to uniquely identify a	Numeric	N10

LABORATORY/MICROBIOLOGY RESULTS						
AHIC Data Element	HITSP-Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
				healthcare provider		

6.3.8 RADIOLOGY RESULT DATA

Table 6.3.8-1 Radiology Result Data

RADIOLOGY RESULT DATA						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
Study ID/Radiology Number	None Available	None	None	None	String	None
Study date and time	None Available	None	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Report date/time	None Available	None	www.hl7.org	None	HL7 Timestamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000
Report Status	HL7 V2.5	Result Status	tinyurl.com/mzyyl	This field contains the status of results for this order. This conditional field is required whenever the OBR is contained in a report message. It is not required as part of an initial order. There are two methods of sending status information. If the status is that of the entire order, use ORC-15-order effective date/time and ORC-5-order status. If the status pertains to the order detail segment, use OBR-25-result status and OBR-22-results rpt/status chng - date/time. If both are present, the OBR values override the ORC values. This field would typically be used in a response to an	ID (Coded Value)	A Some, but not all, results available C Correction to results F Final results; results stored and verified. Can only be changed with a corrected result. I No results available; specimen received, procedure incomplete O Order received; specimen not yet received P Preliminary: A verified early result is available, final results not yet obtained R Results stored; not yet verified S No results available; procedure scheduled, but not done X No results available; Order canceled. Y No order on record for this test. (Used only on queries)

RADIOLOGY RESULT DATA						
AHIC Data Element	HITSP- Selected Standards	SDO Name	Link	SDO Definition	SDO Datatype	SDO Codes & Representations
				order status query where the level of detail requested does not include the OBX segments. When the individual status of each result is necessary, OBX-11-observ result status may be used.		Z No record of this patient. (Used only on queries)
Test Performed	AMA CPT+ Textual Description which can include modification					
Impressions	LOINC tag: '19005-8^X-RAY IMPRESSION^LN'	None Available	www.regenstrief.org/loinc/	None	String	None
Date / Time Revised	HL7	None Available	www.hl7.org	None	HL7 Time-stamp (TS)	Format: YYYY[MM[DD[HH[MM[SS[.S[S[S[S]]]]]]]]][+/-ZZZZ] Examples: 19700101 197001010000 19700101000000

7.0 CHANGE HISTORY

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

7.1 MAY 11, 2007

This document is now Released for Implementation.

7.2 DECEMBER 5, 2007

The changes in this cycle address the following updates:

- Updates for adoption of OASIS HAVE specification
- Updates for use of HITSP/C36 – Lab Result Message for Acknowledgements (acknowledgements are part of the HL7 Lab IG which is used by HITSP/C36)

7.3 DECEMBER 13, 2007

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

7.4 MARCH 19, 2008

This document has been updated to include the HITSP Security and Privacy constructs and has been updated to reflect the new template.

This Interoperability Specification has been updated to reflect the following nursing terminology consensus statement:
This Interoperability Specification will use the CHI recommended SNOMED CT as a reference terminology to communicate interoperable information among and between systems, with the HITSP Interoperability Specification Precondition that the sending and using systems must use formal coded nursing terminologies such as the Clinical Care Classification (CCC) System and the Omaha System that are integrated in SNOMED CT.

7.5 MARCH 27, 2008

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

The following changes have been made to the construct:

- Modified the following standard names/descriptions in Table 2.3-1 List of Standards to provide more clarity and specificity for the optionality described in HITSP/TP13:
  - Removed high level reference to IHE ITI-TF Revision 4

- Added specific reference to Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Section 10 Cross-Enterprise Document Sharing (XDS.a)
- Modified Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Volume 2 Supplement 2007 – 2008 Cross-Enterprise Document Sharing-B (XDS.b) description by moving extraneous content into the narrative of HITSP/TP13
- Modified Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 - Registry Stored Query Transaction for XDS Profile Supplement standard name by adding [ITI-18] for additional clarity

In addition, a table of Guiding Regulations has been added to Section 4.1.

7.6 AUGUST 20, 2008

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

References to C37 have been updated to reflect the correct document title: HITSP/C37 - Lab Report Document

7.7 AUGUST 27, 2008

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