November 9, 2009
Version 2.4

HITSP Anonymize Component

HITSP/C25

Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Final draft	Biosurveillance Technical Committee	August 16, 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 Health Technical Committee	April 27, 2007
2.0	Ready for Implementation	Population Health Technical Committee	May 11, 2007
2.0.1	Review Copy	Population Health Technical Committee	September 18, 2007
2.0.2	Review Copy	Population Health Technical Committee	December 5, 2007
2.1	Ready for Implementation	Population Health Technical Committee	December 13, 2007
2.1.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	August 20, 2008
2.2	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	August 27, 2008
	Template V2.5	Project Team	June 30, 2009
2.2.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	June 30, 2009
2.3	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	July 8, 2009
2.4	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	November 9, 2009

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

1.1 OVERVIEW

Anonymization, according to the International Organization for Standardization (ISO), is the process that removes the association between the identifying data set and the data subject. The HITSP Anonymize Component provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. This construct defines the Component specification that provides the ability to anonymize patient identifiable information.

1.2 COPYRIGHT PERMISSIONS

1.3 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material.

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.

Table 1 Reference Documents

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
TN900 - Security and Privacy	TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs

1.4 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.

1.4.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also implement all of the required interfaces within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification or Capability with which this construct is associated.

1.4.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for actor scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.

This construct defines the following options that may be selected by the referencing HITSP Interoperability Specification.

Table 1-1 Anonymization Options

Construct Options	Construct & Section
Biosurveillance	HITSP/C25 Anonymize, Section 2.2.1.1
Quality	HITSP/C25 Anonymize, Section 2.2.1.2

To claim conformance with the Biosurveillance Anonymization option, implementation rules specified in Section 2.2.1.1 Biosurveillance must be applied. To claim conformance with the Quality Anonymization option, implementation rules specified in Section 2.2.1.2 Quality must be applied.

2.0 COMPONENT DEFINITION

2.1 CONTEXT OVERVIEW

The HITSP Anonymization Component provides specific instructions for anonymizing data for repurposing.

2.1.1 CONTEXT OVERVIEW FOR BIOSURVEILLANCE

Guidance is provided based upon identification risk assessment. Any further use beyond those defined in the specified contexts shall undergo a privacy risk assessment and assert mitigating privacy protection measures.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation in 45 CFR 164.512(a) states:

> "A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law".

45 CFR 164.512(b) states:

> "A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to: (i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority".

HITSP interprets the rule to permit covered entities to disclose protected health information without authorization for specified public health purposes. However, this permissiveness is not a request to any and all data. In practice, public health supports such data requests with rational supporting justification. This commonly takes the form of state or local legislation declaring the types of data, or specific data elements required for public health. HITSP recommends that all implementations undergo legal review to ensure compliance with local, state, and federal regulations. HITSP supports further harmonization of policy and practices for more uniform biosurveillance data exchange.

Disclosure of patient identifiable data to public health authorities in the context of reportable conditions monitoring is routine; this disclosure is based upon the need to monitor and manage known public health threats. Biosurveillance systems collect a broad variety of healthcare data that may go beyond capturing data to support assessment of known threats. As such, HITSP supports the use of anonymization and pseudonymization approaches to protect individual privacy and confidentiality. This Component specifies anonymization protections for such data collection.

HIPAA defines 18 data elements that must be removed from personal health records in order for those records to be considered anonymized. The AHIC Biosurveillance Data Steering Committee has defined some demographic data elements of interest that need to be retained in order to accurately evaluate the data to detect potential threats to public health. This Component specifies removal and aggregation requirements for data variables submitted to a Biosurveillance Information System (BIS).

2.1.2 CONTEXT OVERVIEW FOR QUALITY

Information collected for quality measurement purposes may be covered by national, state, and local or regional domain policies. These policies may restrict the content, agreements, or provisions surrounding the collection of personal health information for the purposes of quality measurement. An organization

supplying or receiving such data will need to assess such restrictions and protective measures provided by this construct to ascertain compliance. HITSP has identified a list of minimal data elements that will be needed to support the HITEP 52 high priority measures, and limited the inference risks by restricting these data elements to those required for computation of these measures.

2.1.2.1 ANONYMITY LEVELS

International Organization for Standardization (ISO) Health informatics -- Pseudonymisation, Technical Specification number 25237 (ISO TS25237) defines the following level concepts with respect to anonymity.

2.1.2.1.1 Level 1 Anonymity: Removal of Clearly Identifying Data

A first, intuitive level of anonymity can be achieved by applying rules of thumb. This method is usually implicitly understood when de-identifying data are discussed. In many contexts, this first level of anonymity may provide a sufficient guarantee.

As an example of Level 1 Anonymity, the HIPAA rule is given. The HIPAA rule requires that for data to be considered de-identified, the following elements should be removed:

- Names (individual, employer, relatives, etc.)
- Address (street, city, county, precinct, zip code – initial 3 digits if geographic unit contains less than 20,000 people, or any other geographical codes)
- Telephone and Fax numbers
- Social Security numbers
- Dates (except for years)
  - Birth date
  - Admission date
  - Discharge date
  - Date of death
  - Ages >89 and all elements of dates indicative of such age (except that such age and elements may be aggregated into a category “Age >90”)
  - E-mail addresses
- Health Plan Beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle Identifiers and Serial Numbers (e.g., VINs, license plate numbers)
- Device Identifiers and Serial Numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric Identifiers (e.g., finger or voice prints)
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

2.1.2.1.2 Level 2 Anonymity: Static Model Based Re-identification Risk Analysis

The second level of anonymity takes into account the global data model and the data flows inside the model. This level includes a static risk analysis that checks for re-identification vulnerabilities by different interface(s). This level may for example include the removal of absolute time references. A reference time marker “T” is defined as the admission of a patient for an episode of care and other events; discharge is expressed with reference to this time marker.

2.1.2.1.3 Level 2 Anonymity Issues with Free-Form Text

Free text and privacy are not very compatible since the notion of “free” denotes the opposite of structured. In Information Technology (IT) terminology, the notions of “data” and “information” are treated separately. Structured data give some indication of what information can be expected where. It is then up to re-identification risk analysis to make assumptions about what can lead to (unacceptable) identification risks, ranging from simple rules of thumb as specified in HIPAA, to analysis of populated databases and inference deductions. In “free text”, as opposed to “structured”, there is no way to begin automated analysis for privacy purposes with a guaranteed outcome (and the derived liabilities). “Free” and “structured” are not necessarily black or white concepts. For example, the presence and position of an information item in a free text document may not be predictable but when it is present, it can be deduced from a pattern (e.g., a sentence like ‘the patient had complaints about …..” or “patient <name> was discharged at …”). Simple pattern parsing or enhanced Natural Language Processing (NLP) can deduce structure in those cases, but perhaps not for the whole text. The notion “free” is more connected to unpredictability of presence or position of information elements. Structure is obtained by the ability to extract data elements either through fixed position, delimiters or tags. Even then, a user may input data elements (e.g., put a patient number where a diagnosis should be put), but the certainty about the content is higher in structured documents. There can be a discussion on how unstructured “free text” is. Policies could define some rules (e.g. define that the free text part shall not contain directly identifiable information such as patient numbers, names, or CFR rule of thumb items such as defined in HIPAA). Parsing and NLP could be applied to separate directly identifying items (e.g. numbers with a certain length, structure or preamble). In some cases, the free text originates from structured text (e.g. an automated letter of discharge from a hospital generated from the hospital’s Healthcare Information System). This makes it easier for the parsing or NLP.

Ultimately, the primary de-identification decision is to:

- Single out what, according to your policy and desired anonymity level, is identifiable information
- Delete what you don’t need
- Keep together (in the payload) what is considered according to the policy as non-identifiable

This is never a black and white decision; hence the need for clearer definition into levels that are referenced in policies. Depending on the ability to single out identifiable information (and thus to structure information), free text makes that zone very grey. The identifiable information structuring selected should be interpreted with respect to privacy: what can lead to identification and what will not.

A hospital policy could specify that investigators cannot put identifiable information into the free text component and define what is meant by identifiable. From a privacy point of view this turns it into structured data with the payload containing free text. The liability for privacy violations is shifted towards the editor of the free text to stick to the agreed policies. From a privacy point of view the baseline on deciding if text is free is the following:

- Parts (possibly) containing identification are known
- Parts denoted as non-identifying should at least not contain nominative information
- Hybrid situations are possible (e.g., the part with identification is structured but the rest unstructured)

2.1.2.1.4 Level 3 Anonymity Routine Resource Risk Analysis

An anonymized resource used for data mining must undergo a routine statistical evaluation for re-identification risks associated with the populated resource. Such risk analysis entails assessments of outliers and analytical linking with external information resources.

2.1.2.2 USE CASE RISK ASSESSMENTS

In consideration of the HIPAA Rules and ISO Pseudonymisation, Unpublished Technical Specification numberTS25237, the following risks are associated with collecting and retaining an information repository to fulfill the Use Cases addressed by this specification:

2.1.2.2.1 Biosurveillance Identifiers

Table 2-1 illustrates patient identifying data elements subject to Level 1 Anonymity concerns:

Table 2-1 Biosurveillance Patient Identifying Level 1 Data Elements

AHIC Data Variable	HIPAA Concern
Data Linker	Any other unique identifying number, characteristic, or code
Encounter date/time	Dates
Date of Birth	Dates
Deceased date	Dates
Age	Aggregate to >89 where age is >89
Gender	Aggregate: Utilize only gender specifications of M/F/U
Zip	Aggregate to – initial 3 digits if geographic unit if Zip region contains less than 20,000 people

Table 2-2 and Table 2-3 illustrate patient identifying data elements subject to Level 2 Anonymity concerns:

Table 2-2 Biosurveillance Patient Identifying Level 2 Freeform Text Data Elements

AHIC Data Variable Likely to be in the form of Freeform Text
Chief Complaint
Nurse/Triage Note
Test interpretation
Susceptibility Test interpretation

Table 2-3 Biosurveillance Patient Identifying Level 2 Combinatorial Data Elements

AHIC Data Variables Subject to Re-Identification Risk through Combination with other fields
Facility Code
Diagnosis code
Laboratory Result

2.1.2.2.2 Quality Identifiers

Table 2-4 illustrates patient identifying data elements subject to Level 1 Anonymity concerns:

Table 2-4 Quality Patient Identifying Level 1 Data Elements

AHIC Data Variable	HIPAA Concern
Data Linker	Any other unique identifying number, characteristic, or code
Encounter date/time	Dates
Date of Birth	Dates
Sex	Aggregate: Utilize only gender specifications of M/F/U
Zip	Aggregate to – initial 3 digits if geographic unit if Zip region contains less than 20,000 people

AHIC Data Variable	HIPAA Concern
Discharge Date/time	Dates
Deceased Date/time	Dates

Table 2-5 and Table 2-6 illustrate patient identifying data elements subject to Level 2 Anonymity concerns:

Table 2-5 Quality Patient Identifying Level 2 Freeform Text Data Elements

AHIC Data Variable Likely to be in the form of Freeform Text
Test interpretation
Impressions

Table 2-6 Quality Patient Identifying Level 2 Combinatorial Data Elements

AHIC Data Variables Subject to Re-Identification Risk through Combination with other fields
Diagnosis code
Problems
Allergies
Substance Intolerance
Medication Ordered
Authorizing Provider
Medication administered
Medication Administration date/time
Facility Identifier/Name
Provider Identifier
Patient Class
Procedure Ordered
Procedure Performed
Procedure Date/time
Resulted Test
Result Value

2.1.3 COMPONENT CONSTRAINTS

This Component addresses construct constraints for each context requiring anonymization. Currently, this applies to:

- Biosurveillance (addressed in HITSP/IS02 Biosurveillance Interoperability Specification): This Component is constrained to address the AHIC Biosurveillance Data Set variables subject to identification risk. With the exception of the data variables described below, all identifiers from the list of identifiable data variables defined by HIPAA that must be removed to accomplish de-identification are expected to be removed from the documents and messages that are communicated to the BIS
- Quality: This Component is constrained to address the data elements identified in the HITSP/IS06 Quality Interoperability Specification to support the Health Information Technology Expert Panel (HITEP) priority quality measures. With the exception of the data variables described below, all identifiers from the list of identifiable data variables defined by HIPAA that must be removed to accomplish de-identification are expected to be removed from the patient level quality data

documents and messages where anonymization is required by the policy of the implementation environment

Table 2-7 Component Constraints

Constraint Code	Constraint
	Any further use of this construct beyond the contexts listed above shall undergo a privacy risk assessment and assert mitigating privacy protection measures

2.1.4 COMPONENT DEPENDENCIES

Table 2-8 Component Dependencies

Standard/HITSP Component	Depends On (Name of standard/HITSP Component that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
No applicable dependencies			

2.2 RULES FOR IMPLEMENTING

2.2.1 DATA MAPPING

Different jurisdictions and stakeholders will have different requirements and agreements that may not require full anonymization of these data elements (see Context Overview Section 2.1).

2.2.1.1 BIOSURVEILLANCE

2.2.1.1.1 Biosurveillance Level 1 Anonymity Considerations

To be compliant with full de-identification, all patient identifying information specified by HIPAA must be removed from the message or document to be submitted for repurposing. For the Biosurveillance context, the following exceptions apply to the data variables specified below.

Table 2-9 Data Mapping Biosurveillance Level 1 Patient Data Elements

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions	Additional Specification for Component
Data Linker	A unique, randomly generated, encoded number that links to patient-level information (i.e. name and address) retained at the facility		NA	NA	Pseudonymized in accordance with the HITSP/T24 Pseudonymization Transaction. Where linking across organizations is not of interest to the quality analysis, this may alternatively use a randomized data linker assigned by the local organization	NA
Encounter Date/Time	Time of the patient presentation for care		NA	NA	Aggregate to: Month/Year only	NA
Date of Birth	Date of Birth limited to month and year for privacy purposes		NA	NA	Aggregate to: Month/Year only	NA
Age	Patient age which may be calculated from full date of birth before the days are removed		NA	NA	Age >89 group	NA

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions	Additional Specification for Component
Gender	Patient sex		NA	NA	Aggregate: Utilize only gender specifications of M/F/U	NA
Zip	Home address		NA	NA	Aggregate to – initial 3 digits if geographic unit if Zip region contains less than 20,000 people	NA
State	Home address		NA	NA	NONE	NA

2.2.1.1.2 Biosurveillance Level 2 Anonymity Considerations

This section describes the Level 2 Anonymity considerations that pertain to the data elements within the AHIC Biosurveillance Data Steering Committee Data Dictionary.

Inference Risk Mitigations:

Freeform data poses a privacy and confidentiality risk because freeform text can contain identifiable information. If one would like to get value out of that data, then they need to develop methods to extract codified information. To be compliant with full de-identification, this approach should be applied to freeform text within the message or document to be submitted for repurposing. For the Biosurveillance context, based upon the AHIC Data Steering Committee Data Dictionary, the following variables would be subject to such protections:

Table 2-10 Biosurveillance Freeform Text Risk Mitigation Data Elements

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/ Pre-conditions	Additional Specification for Component
Chief Complaint	Short description recorded during triage that initiates reason for seeking care		NA	NA	Codify	NA
Nurse Triage Note	Text string written by nurse or healthcare partner		NA	NA	Codify	NA
Test Interpretation	Interpretation of test result including the susceptibility test interpretation		NA	NA	Codify	NA

No stipulation is made in this specification as to the algorithms or process by which the codification is accomplished. Future specifications may address this area further, but until then, the approach is left to the implementer.

Because of the re-identification risks identified in Section 2.1.2.2.1 of this document within the AHIC Biosurveillance Data Set in combination with other fields, the information resource must have access restricted to authorized persons contractually bound or otherwise bound (and subject to sanction) to use the resource for specified purposes. This Component specification recommends that access be restricted to authorized public health authorities and infection control clinical staff associated with healthcare provider organizations.

No stipulation is made in this specification with respect to access control except for the inherent mechanisms provided in the functional flow scenarios in any specification that uses this construct. Future specifications may address this area further, but until then, the approach is left to the implementer.

2.2.1.2 QUALITY

The considerations listed in this section are based upon the data elements identified by HITSP to support the HITEP 52 priority quality measures.

2.2.1.2.1 Quality Level 1 Anonymity Considerations

To be compliant with full de-identification, all patient identifying information specified by HIPAA must be removed from the message or document to be submitted for repurposing. For the Quality Use Case, the following exceptions apply to the data variables specified below.

Table 2-11 Data Mapping Quality Level 1 Patient Data Elements

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/ Pre-conditions	Additional Specification for Component
Pseudonymized Data Linker	A unique, randomly generated, encoded number that links to patient-level information (i.e., name and address) retained at the facility		NA	NA	Pseudonymized in accordance with the HITSP/T24 Pseudonymization Transaction. Where linking across organizations is not of interest to the quality analysis, this may alternatively use a randomized data linker assigned by the local organization	NA
Encounter Date/Time	Time the patient presents for care Emergency Department (ED) arrival time (initial triage time) or the registration time for inpatients, or check-in time for ambulatory settings		NA	NA	No restriction specified. The full date is required for proper quality analysis and measurement	NA
DOB	Date of birth		NA	NA	Aggregate to: Month/Year only	NA
Gender	Patient sex		NA	NA	M/F/U	NA
Discharge Date/Time	Time of Inpatient discharge or release from ED		NA	NA	No restriction specified. The full date is required for proper quality analysis and measurement	NA
Deceased Date/Time	If patient has died, deceased date/time		NA	NA	No restriction specified. The full date is required for proper quality analysis and measurement	NA

2.2.1.2.2 Quality Level 2 Anonymity Considerations

This section describes the Level 2 Anonymity considerations that pertain to the data elements within the dataset identified by HITSP to support the HITEP 52 priority quality measures.

Inference Risk Mitigations:

Freeform data pose a privacy and confidentiality risk because freeform text can contain identifiable information. If one would like to attain value from the data, then they need to develop methods to extract codified information. To be compliant with full de-identification, this approach should be applied to freeform text within the message or document to be submitted for aggregate quality analysis. For the

Quality Use Case, based upon the Data Dictionary identified by HITSP to support the HITEP 52 priority quality measures, the following variables would be subject to such protections:

Table 2-12 Quality Freeform Text Risk Mitigation Data Elements

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions	Additional Specification for Component
Test Interpretation	Interpretation of test result by the laboratory, including the susceptibility test interpretation		NA	NA	Codify	NA
Impressions	Interpretation of study, by provider of service including diagnosis and impressions		NA	NA	Codify	NA

No stipulation is made in this specification as to the algorithms or process by which the codification is accomplished. Future specifications may address this area further, but until then, the approach is left to the implementer.

Because of the re-identification risks identified in Section 2.1.2.2.2 of this document within the Quality Data Set in combination with other fields, the information resource must have access restricted to authorized persons contractually bound or otherwise bound (and subject to sanction) to use the resource for specified purposes. This Component specification recommends that access be restricted to the source organization, or quality measurement processing entities that have engaged in a Business Associate Agreement (BAA) with healthcare provider organizations. This information is also subject to sensitive health information protections by law and program implementations as established at the federal, state and program levels.

No stipulation is made in this specification with respect to access control except for the inherent mechanism provided in the functional flow scenarios described in the HITSP/IS06 Quality Interoperability Specification.

2.2.2 GUIDELINES AND EXAMPLES

No additional detail provided at this time.

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-13 Regulatory Guidance

Standard	Description
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

2.3.2 SELECTED STANDARDS

Table 2-14 Selected Standards

Standard	Description
International Organization for Standardization (ISO) Health Informatics -- Pseudonymisation, Technical Specification #25237	Health Informatics – Pseudonymisation. Approved March 2007. For more information visit www.iso.org

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-15 Informative Reference Standards

Standard Name	Description/Usage
Digital Imaging and Communications in Medicine (DICOM) Attribute Level Confidentiality Supplement: #55	Adds a mechanism for selective protection of individual attributes within arbitrary DICOM service-object pair (SOP) instances. It may be used to achieve protection of identifying information, e.g. a reversible anonymization or pseudonymization of DICOM SOP instances while continuing to use unmodified lower level message and protocol services for network transfer, storage, and media exchange of composite image information objects. For more information visit medical.nema.org

3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

4.0 DOCUMENT UPDATES

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

4.1 DECEMBER 5, 2007

- Restructured the entire document to conform to the revised 2007 Component Template
- Expanded the applicable scope to include the Quality Use Case in addition to the Biosurveillance Use Case in the following sections
  - Context Overview
  - Component Constraints (including risk analysis)
  - Data Mapping
- Added Unified Modeling Language (UML) Diagram for Roadmap

4.2 DECEMBER 13, 2007

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

4.3 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References.

The following was designated as Regulatory Guidance:

- Health Insurance Portability and Accountability Act (HIPAA) -- Administrative Simplification

The following standard was designated as Selected:

- International Organization for Standardization (ISO) Health Informatics -- Pseudonymisation, Unpublished Technical Specification # 25237

The following standard was designated as Informative Reference:

- Digital Imaging and Communications in Medicine (DICOM) Attribute Level Confidentiality Supplement: # 55

4.4 AUGUST 27, 2008

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

4.5 JUNE 30, 2009

Minor editorial changes were made to this document. Removed boilerplate text for simplification. The term “actor” was replaced with “interface”.

4.6 JULY 8, 2009

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

4.7 NOVEMBER 9, 2009

Updated Section 2.1.1 with new language regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation in 45 CFR 164.512(a).

Updated International Organization for Standardization (ISO) Health informatics -- Pseudonymisation, Technical Specification #25237 (ISO TS25237) to reflect the published status, previously the standard was listed as unpublished.