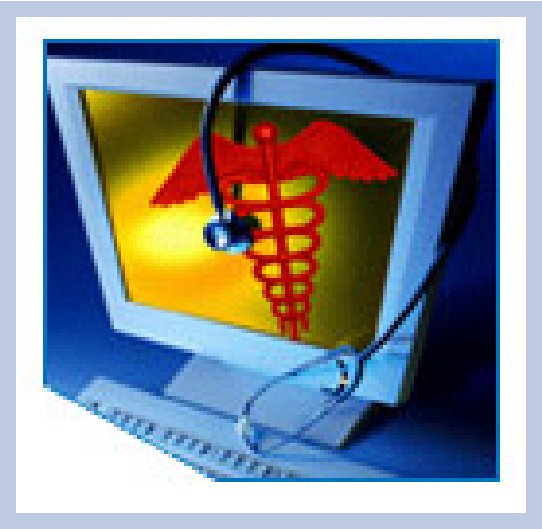
December 13, 2007
Version 2.1

HITSP Anonymize Component

HITSP/C25



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

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 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

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Anonymize Component, 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 this specification, acknowledges the copyright protections that pertain, and provides links to key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Component Definition.

1.1 OVERVIEW

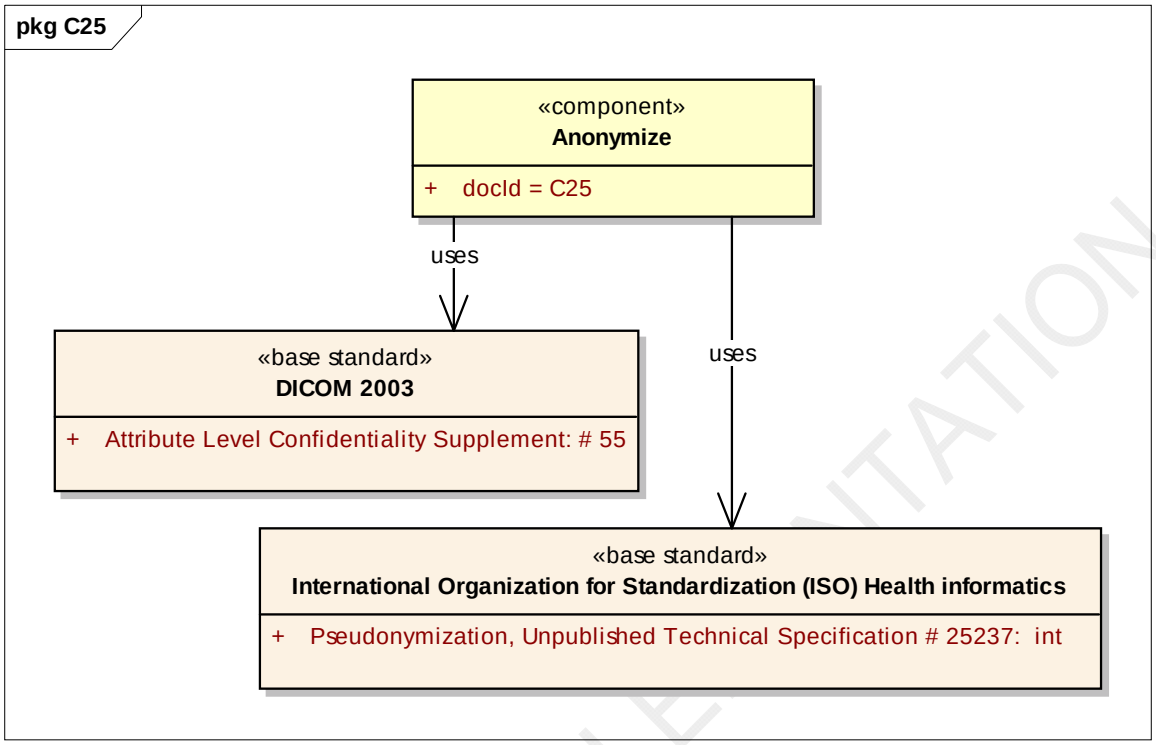
This section describes the contents of this specification and provides a high level definition of this Component and background information about the underlying standards that the Component is based on.

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 COMPONENT CONSTRUCT ROADMAP

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 that will satisfy the requirements imposed by a given Use Case. The IS groups specific actions and actors to describe the relevant contexts using HITSP constructs that further identify and constrain standards where necessary. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). The current Anonymize Component specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 (Interoperability Specification Construct Roadmap) from the relevant IS to better understand the context, dependencies, and relationships between the constructs that are used to meet the IS requirements. The roadmap in Figure 1.2-1 depicts primary standards that are selected, constrained, or referenced to define the atomic constructs used in an information exchange, or to meet an infrastructure requirement. Implementers should read the documents that describe the standards represented in the diagram for their details and specific uses.

Figure 1.2-1 Component Construct Roadmap



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

1.4 REFERENCE DOCUMENTS

This section contains links to key reference documents and background material.

The HITSP Interoperability Specification Overview provides the 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.

The conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications are contained in the HITSP Conventions List.

The acronyms used in this document are contained in the HITSP Acronyms List.

The HITSP Glossary provides definitions for relevant terms used by HITSP documents.

The HITSP Harmonization Framework describes the current framework within which the Interoperability Specifications are built.

A Technical Note, TN900 - Security and Privacy, has been 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 COMPONENT DEFINITION

A Component defines atomic constructs used to support an information exchange or to meet an infrastructure requirement. This is accomplished by:

(a) Referencing one or more underlying standards
(b) Specifying constraints and other rules for using the standards

2.1 CONTEXT OVERVIEW

This section provides a general description of the Component. It includes a detailed definition of the Component and the reason for its use. It also provides all the necessary background information that further describes the context in which the Component is needed, and the base or composite standard that the Component is based on. 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 164.519(b) 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.”

The HITSP Population Health Technical Committee 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. The Population Health Technical Committee recommends that all implementations undergo legal review to ensure compliance with local, state, and federal regulations. The Population Health Technical Committee 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, the Population Health Technical Committee 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. The Population Health Technical Committee 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 -- Pseudonymization, Unpublished Technical Specification # 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 actors. 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-FormText

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 gives 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 Pseudonymization, Unpublished Technical Specification #TS25237, 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 2.1.2.2.1-1 illustrates patient identifying data elements subject to Level 1 Anonymity concerns:

Table 2.1.2.2.1-1 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 2.1.2.2.1-2 and 2.1.2.2.1-3 illustrate patient identifying data elements subject to Level 2 Anonymity concerns:

Table 2.1.2.2.1-2 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 2.1.2.2.1-3 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 2.1.2.2.1-1 illustrates patient identifying data elements subject to Level 1 Anonymity concerns:

Table 2.1.2.2.2-1 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 2.1.2.2.1-2 and Table 2.1.2.2.2-3 illustrate patient identifying data elements subject to Level 2 Anonymity concerns:

Table 2.1.2.2.2-2 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 2.1.2.2.2-3 Quality Patient Identifying Level 2 Combinatorial Data Elements

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

2.1.3 COMPONENT CONSTRAINTS

This section describes the constraints that limit the context in which the Component 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.

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

- Biosurveillance: 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 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 2.1.1-1 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

This section describes any specific mapping criteria for the standards underlying the Component. It elaborates on the relationships between different standards used by this Component, and how they map to each other. Additional required mapping criteria not currently enforced by the underlying standards, and any specific elements that are required for this mapping to succeed, are also provided.

Table 2.1.2-1 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

The following section documents the content of the Component. It provides the basic elements and secondary standards that are supported by this Component and the constraints that are being placed on those standards. Specifically, it describes the subset or constraints that are required for this Component, and the minimum attributes of the Component as it relates to the base or composite standards on which it is based.

2.2.1 DATA MAPPING

This section describes the specific data elements used by this Component. Due to the potentially large number of data elements in a particular standard, only the fields that HITSP is constraining differently from the standard will be described here.

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 2.2.1.1.1-1 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
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 2.2.1.1.2-1 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 the Population Health Technical Committee 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 2.2.1.2.1-1 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

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions	Additional Specification for Component
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 the Population Health Technical Committee 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 the Population Health Technical Committee to support the HITEP 52 priority quality measures, the following variables would be subject to such protections:

Table 2.2.1.2.2-1 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 Quality Interoperability Specification.

2.2.2 GUIDELINES AND EXAMPLES

This section provides additional guidelines and examples that support the underlying base or composite standards for this Component. It describes how these specifications differ from the underlying standards, and provides guidelines and examples for implementation.

No additional detail provided at this time.

2.3 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 following standards are used to implement this Component specification:

Table 2.3-1 List of Standards

Standard	Description
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. Visit http://medical.nema.org/ for more information.
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.
International Organization for Standardization (ISO) Health Informatics -- Pseudonymization, Unpublished Technical Specification # 25237	Health Informatics – Pseudonymisation. Approved March 2007. Visit http://www.iso.org for more information.

3.0 TECHNICAL IMPLEMENTATION

3.1 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.

3.1.1 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 be constrained as specified in this construct, and implement at least one of the required transactions associated with the actor to be supported from **Error! Reference source not found.** within the scope, subset or implementation option that is selected from the referencing Interoperability Specification.

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

3.1.2 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 3.1.2-1 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.

4.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

5.0 CHANGE HISTORY

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

5.1 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

5.2 DECEMBER 13, 2007

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