

# HITSP Anonymize Public Health Case Reporting Data Component

---

HITSP/C87



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
	Template Updated to V2.4	Project Team	July 31, 2008
0.0.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	September 26, 2008
0.0.2	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	December 10, 2008
1.0	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	December 18, 2008
	Template V2.5	Project Team	June 30, 2009
1.0.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	June 30, 2009
1.1	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	July 8, 2009
1.2	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	November 9, 2009



# TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION.....</b>	<b>5</b>
1.1	Overview.....	5
1.2	Copyright Permissions.....	5
1.3	Reference Documents.....	5
1.4	Conformance .....	5
1.4.1	Conformance Criteria .....	5
1.4.2	Conformance Scoping, Subsetting and Options .....	6
<b>2.0</b>	<b>COMPONENT DEFINITION.....</b>	<b>7</b>
2.1	Context Overview .....	7
2.1.1	Component Constraints.....	7
2.1.2	Component Dependencies .....	8
2.2	Rules for Implementing.....	8
2.2.1	Anonymity Levels .....	8
2.2.1.1	Level 1 Anonymity: Removal of Clearly Identifying Data .....	8
2.2.1.2	Level 2 Anonymity: Static Model Based Re-identification Risk Analysis .....	9
2.2.1.3	Level 3 Anonymity: Routine Resource Risk Analysis .....	10
2.2.2	Data Mapping .....	10
2.2.2.1	Level 1 Anonymity Considerations.....	10
2.2.2.2	Level 2 Anonymity Considerations.....	14
2.3	Standards .....	15
2.3.1	Regulatory Guidance.....	15
2.3.2	Selected Standards .....	15
2.3.3	Informative Reference Standards.....	15
<b>3.0</b>	<b>APPENDIX .....</b>	<b>16</b>
	<b>DOCUMENT UPDATES .....</b>	<b>17</b>
3.1	December 10, 2008 .....	17
3.2	December 18, 2008 .....	17
3.3	June 30, 2009.....	17
3.4	July 8, 2009 .....	17



## FIGURES AND TABLES

Table 1-1 Reference Documents .....	5
Table 2-1 Component Constraints .....	8
Table 2-2 Component Dependencies .....	8
Table 2-3 Data Mapping Level 1 Patient Data Elements .....	10
Table 2-4 Regulatory Guidance .....	15
Table 2-5 Selected Standards .....	15
Table 2-6 Informative Reference Standards .....	15



## 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 Public Health Case Reporting Data 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 for Public Health Case Reporting.

Anonymization can not be guaranteed by the use of this construct, and therefore a comprehensive risk assessment should be conducted in the implementation environment.

### 1.2 COPYRIGHT PERMISSIONS

#### COPYRIGHT NOTICE

© 2009 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

### 1.3 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 [www.hitsp.org](http://www.hitsp.org).

**Table 1-1 Reference Documents**

Reference Document	Document Description
<a href="#">HITSP Acronyms List</a>	Lists and defines the acronyms used in this document
<a href="#">HITSP Glossary</a>	Provides definitions for relevant terms used by HITSP documents
<a href="#">TN900 - Security and Privacy Technical Note</a>	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 interface 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.



## 2.0 COMPONENT DEFINITION

### 2.1 CONTEXT OVERVIEW

This construct provides guidance for anonymization and should be implemented with consideration of risk assessment results in the intended operating environment. This construct is intended specifically for the use of anonymizing public health case reporting data, and should not be reused for any other purpose.

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 public health 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. Public health 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.

Under 45 CFR 164.502(d), HIPAA defines 18 data elements that under a Safe Harbor approach must be removed from personal health records in order for those records to be considered anonymized. The Use Case has defined some demographic data elements of interest that need to be retained in order to accurately evaluate the data for public health case reporting. This Component specifies removal and aggregation requirements for data variables submitted to a Public Health Information System.

The selected standard is the ISO Health informatics -- Pseudonymisation, Unpublished Technical Specification # 25237 (ISO TS25237). This standard defines 3 levels of anonymization, with specific requirements for anonymization at each one of those anonymization levels. These requirements are described in Section 2.2.

#### 2.1.1 COMPONENT CONSTRAINTS

The use of this construct assumes that all policy agreements and regulatory requirements applicable to the purpose for which the construct is being used are adhered to by the parties exchanging the



information. In the absence of regulatory requirements, the use of this construct will be possible because of an agreement between the exchange parties.

**Table 2-1 Component Constraints**

Constraint	Constraint Section
With the exception of the data variables described in Table 2-3 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 Public Health System	N/A

## 2.1.2 COMPONENT DEPENDENCIES

**Table 2-2 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 ANONYMITY LEVELS

The ISO Pseudonymisation (ISO TS25237) specification defines the following level concepts with respect to anonymity.

- Level 1 Anonymity: Removal of Clearly Identifying Data
- Level 2 Anonymity: Static Model Based Re-identification Risk Analysis
- Level 3 Anonymity: Routine Resource Risk Analysis

#### 2.2.1.1 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

#### 2.2.1.2 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 interfaces. 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.

##### ***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). 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 Health 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

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)

### 2.2.1.3 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.

## 2.2.2 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). In consideration of the HIPAA Rules and ISO Pseudonymisation (ISO TS25237), the following sections describe anonymization requirements associated with collecting and retaining an information repository for public health case reporting.

### 2.2.2.1 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. The following anonymity rules apply to the data variables specified below.

Note that it is anticipated that facilities will act to shield identities by using contact details (phone number, address, contact person, etc.) that do not identify the facility.

**Table 2-3 Data Mapping Level 1 Patient Data Elements**

Data Element	Definition	Anonymization Requirements
Address	The address (Street, City, State, Zip Code) of the person or facility that diagnosed the subject of the Case Report	Pass through unmodified
Administration of Treatment	Was treatment administered?	Pass through unmodified
Admission Date	Enter the date that the subject of the Case Report was Admitted to the hospital	Aggregate Month/year
Adverse Event (AE) Terms	Definitions pending	Blind
AE Following Prior Vaccination	Description of the adverse event	Blind
Age	The age of the subject of the case report at time of diagnosis	Age < 1 group by 1 month intervals Ages 1 – 88 group by year Age >89 group
Approximate Age of Device	The length of time the device has been in use for the patient	Pass through unmodified
Birth Weight	The weight of the patient at birth	Pass through unmodified
Common Device Name	Common name of the device	Pass through unmodified
Concomitant Medical Product Name	Other medical products in use for the patient to determine proximal relationships	Pass through unmodified
Concomitant Medical Products & Therapy Dates	Other medical products and treatment used proximal to the event	Blind
Contact Person	The name of the person to be contacted for further information	Pass through unmodified
Contact Phone Number	The telephone number fore the contact person	Pass through unmodified
Current Medications (Medwatch concomitant meds)	Other medications in use	Pass through unmodified



Data Element	Definition	Anonymization Requirements
Date Treatment was Administered	The date treatment was administered. For HepB, Date HBV vaccine administered	Blind
Date of Birth	Date of birth	Aggregate to: Month/Year only when age <89 (else blind)
Date of Death	If patient has died, deceased date/time	Aggregate to: Month/Year only unless it is relevant to the event
Date of Event	The date the event first occurred	Aggregate to: Month/Year only unless it is relevant to the event
Date of Test	The date that the laboratory test was performed for the subject of the Case Report	Aggregate Month/yr
Date product returned to manufacturer	If returned to the manufacturer, date of return	Aggregate Month/yr
Date Report Sent	The date the report is submitted	Pass through unmodified
Date Sent to FDA	The date the report was submitted to the FDA – U.S.	Pass through unmodified
Date User Facility/Importer Became Aware of Event	The date the event was first recognized by an observer	Pass through unmodified
Death	Did the subject die as a result of the disease?	Pass through unmodified
Description of Event	A textual description of the event	Blind
Diagnosis Date/Time	The date that the subject of the Case Report was diagnosed with Condition above	Aggregate Month/year
Diagnosis Type	Type of diagnosis being sent (admitting, working, final)	Pass through unmodified
Diagnosis/Injury Code	Diagnosis or diagnoses assigned as a result of the encounter	Pass through unmodified
Discharge Date	Enter the date that the subject of the Case Report was Discharged from the hospital	Aggregate Month/year
Estimated Delivery Date	Estimated date of delivery (or est. date of confinement [EDC])	Pass through unmodified
Ethnicity	The ethnicity of the subject of the case report	Blind
Event Abated after use stopped or dose reduced	Indication that the event resolved/abated after usage stopped or dose reduced	Pass through unmodified
Event Device Problem Code	The locally determined code to identify the problem for subsequent follow up	Pass through unmodified
Event Reappeared after reintroduction	Indication if the reaction reoccurred after rechallenging the patient to the suspected substance	Pass through unmodified
Expiration Date	The expiration date of the product	Pass through unmodified
Facility Identifier	Unique facility identifier	Pass through unmodified
Facility/Importer Name	The name of the facility that the healthcare provider diagnosed the subject of the Case Report	Pass through unmodified
Gender	Administrative sex	Aggregate: Utilize only gender specifications of M/F/U
Hospital Name	Name of hospital the case was admitted	Pass through unmodified
Hospitalization	If the subject of the case report was hospitalized	Pass through unmodified
If explanted give date	Date device was removed (if removed)	Aggregate month/yr
If implanted give date	Date of implantation of the device (if implanted)	Aggregate month/yr
Single use device that was reprocessed and reused on patient	Indication if the device is a single-use device that was cleaned/reprocessed and is reused on the affected patient	Pass through unmodified
Location where Event Occurred	The location type of the event – e.g., home, hospital, other facility, etc	Pass through unmodified



Data Element	Definition	Anonymization Requirements
Manufacture Name, City and State	Manufacturer of the device	Pass through unmodified
Medical Device Catalog #	Catalog number of the device	Pass through unmodified
Medical Device Lot #	Lot number of the device	Pass through unmodified
Medical Device Model #	Model number of the device	Pass through unmodified
Medical Device Other #	Other identifiers for the device	Blind
Medical Device Serial #	Serial number of the device	Blind
Name and Address of Reprocessor	Name and address of the individual/organization reprocessing the single use device	Pass through unmodified
Name of Condition	The name of the condition diagnosed for the subject of the Case Report	Pass through unmodified
Name of Organization Collecting Specimen	Name of organization collecting specimen which may be different from the organization performing the laboratory analysis	Pass through unmodified
Name of Treatment	Name of the treatment	Blind
NDC# or Unique ID	The unique identifier for the product	Pass through unmodified
Number of Siblings	The number of siblings	0,1,2,3 or greater
Occupation	The occupation of subject of the case report. Enter as much detail as possible (e.g., teacher in pre-school facility)	Blind
Occupation of Reporter	The role of the reporter (e.g., physician, nurse, administrator, etc.)	Pass through unmodified
Operator of Device	The individual managing the device	Pass through unmodified
Ordered Test Code	The identifier code for the requested observation/test/battery	Pass through unmodified
Outcome Attributed to AE	Textual description of the outcome associated with the adverse event	Blind
Patient Address (street name, city, state, zip code)	The address of the subject of the case report	Aggregate to initial 3 digits if geographic unit if Zip region contains less than 20,000 people
Patient Class	General type of patient, e.g., Inpatient, Outpatient, Emergency	Pass through unmodified
Patient Country	The country of the address of the subject of the case report	Pass through unmodified
Patient County	The county of the address of the subject of the case report	Blind
Patient identifier	The identifier for the patient, may be a pseudonymized identifier	An alternate identifier that is a pseudonym (use HITSP/T24 Pseudonymize)
Patient Name (first, MI, Last)	The name (preferably legal) of the subject of the case report	Blind
Patient Recovered Diagnosis	Final determination of reaction – diagnosis	Blind
Patient Telephone	The telephone of the subject of the case report	Blind (if phone number is needed can be obtained through facility contact with justification)
Performing Laboratory	Laboratory that produced the test result. This may be a reference laboratory identifier	Pass through unmodified
Pre-existing physician diagnosed allergies, birth defects. Medical conditions	Allergies, conditions existing prior to the use of the suspected agent	Blind
Pregnancy Status	Whether the subject of the case report was pregnant at time of diagnosis	Pass through unmodified
Previous Event Report Details	Definitions pending	Blind



Data Element	Definition	Anonymization Requirements
Previous Vaccine Date Given	The date the vaccination dose suspected was administered	Pass through unmodified
Previous Vaccine Lot #	The lot number of the vaccine dose	Pass through unmodified
Previous Vaccine Manufacturer	The manufacturer of the vaccine dose	Pass through unmodified
Previous Vaccine Route/Site	The route of administration of the vaccine dose	Pass through unmodified
Previous Vaccine Type	The type of vaccine	Pass through unmodified
Product available for evaluation?	Indication if the product is still available to be evaluated	Pass through unmodified
Product Diagnosis for Use	The reason the product was initially used	Blind
Product Dose	The dose of the product administered	Pass through unmodified
Product Frequency	The frequency with which the product was administered	Pass through unmodified
Product Lot #	The product lot number	Pass through unmodified
Product Route Used	The route of administration of the product (e.g., oral, intravenous, intramuscular, etc.)	Pass through unmodified
Product Therapy Dates	Duration of therapy with the product	Blind
Race	The race(s) of the subject of the case report	Blind
Reason for Non-Evaluation	Definitions pending	Blind
Recovered	Did the subject recover from the disease?	Pass through unmodified
Report Date	The date that the Case Report is being sent	Pass through unmodified
Report Date/Time	Date/time of report	Pass through unmodified
Report sent to	The organization to which the report is submitted	Pass through unmodified
Report sent to FDA	Indication if the report is submitted to the Food and Drug Administration (FDA) – U.S.	Pass through unmodified
Report Source	The originator of the report	Pass through unmodified
Reported Previously	Indication if the information is supplemental to update in event already reported	Pass through unmodified
Reporter Address (street name, city, state, zip code)	The address of the reporter	Pass through unmodified
Reporter Email	The email contact information for the reporter	Pass through unmodified
Reporter Name	The name of the person or facility sending the Case Report	Pass through unmodified
Reporting Laboratory Identifier	Identifier for laboratory that is sending the result. This laboratory may be sending results received back from reference laboratories	Pass through unmodified
Responsible Physician/Healthcare Provider Name	Physician of Record for the Patient	Pass through unmodified
Result Unit	Unit for numeric result context	Pass through unmodified
Resulted Test	The identifier code for the specific test component resulted	Pass through unmodified
Results Status	Status of report (preliminary, final, corrected)	Pass through unmodified
Signs and Symptoms	The signs and symptoms experienced by the patient	Blind
Source of Specimen	The physical body location from where the specimen for the lab report was taken from the subject	Pass through unmodified
Specimen Collection Date	The date that the specimen for the laboratory test was taken from the subject of the Case Report	Aggregate month/yr
Suspect Medical Device Brand Name	Brand name of the suspect device	Pass through unmodified
Suspect Product Name	Product name	Pass through unmodified
Symptom/Illness Onset Date/Time	This is the range of time of which the problem was active for the patient; for PH: The date that the subject began having symptoms of condition being reported	Blind



Data Element	Definition	Anonymization Requirements
Telephone	The phone number of the person or facility that diagnosed the subject of the Case Report	Pass through unmodified
Telephone	The phone number of the person or facility sending the Case Report	Pass through unmodified
Test Interpretation	Interpretation of test result, including the susceptibility test interpretation	Blind
Test Method	Testing method used to arrive at the specific result: The name of the laboratory test	Pass through unmodified
Test Result	The test result of the laboratory test including any applicable result units of measure	Pass through unmodified
Test Status	Status of the test result	Blind
Therapy Dates	Dates of treatment with the suspected agent	Blind
Type of Event and/or Issue	Definitions pending	Blind
Type of Follow-Up	Definitions pending	Blind
Type of Remedial Action	Definitions pending	Blind
Type of Report	The type of report (e.g., Drug Event Report, Healthcare Associated Infection Report, etc.)	Pass through unmodified
Type of Reportable Event	Seriousness of the event	Blind
Type of Reporter	The role of the reporter with respect to the patient (e.g., treating or consulting clinician, case manager, etc.)	Pass through unmodified
User Facility/Importer Report Number	The number of the report assigned by the reporting facility	Pass through unmodified
Vaccine # Previous Doses	The number of previous doses of the vaccine type	Pass through unmodified
Vaccine Purchased With	Indication of vaccination source (e.g., special program such as Vaccine for Children, state or provincial programs, etc)	Pass through unmodified
Weight	The weight of the patient at the time of the report	Pass through unmodified (There is no clear cut rule as weight or age/height related w.r.t. upper/lower thresholds)

#### 2.2.2.2 LEVEL 2 ANONYMITY CONSIDERATIONS

This section describes the Level 2 Anonymity considerations that pertain to the data elements.

##### ***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. 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 within the Public Health Data Set identified in Section 2.2.2 of this document, 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.



## 2.3 STANDARDS

### 2.3.1 REGULATORY GUIDANCE

**Table 2-4 Regulatory Guidance**

Regulation	Description
Health Insurance Portability and Accountability Act (HIPAA) Code of Federal Regulations (CFR) Title 45, Part 164, Section 502(d) (CFR§164.502(d)) Uses and disclosures of protected health information: general rules	This is a specific reference to 45 CFR 164.502(d) which specifies the general rules for uses and disclosures of de-identified protected health information

### 2.3.2 SELECTED STANDARDS

**Table 2-5 Selected Standards**

Standard	Description
International Organization for Standardization (ISO) Health Informatics -- Pseudonymisation, Published Technical Specification # 25237	Health Informatics – Pseudonymisation. Approved as a Technical Specification March, 2007. For more information visit <a href="http://www.iso.org">www.iso.org</a>

### 2.3.3 INFORMATIVE REFERENCE STANDARDS

**Table 2-6 Informative Reference 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. For more information visit <a href="http://medical.nema.org">medical.nema.org</a>



### 3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.





## DOCUMENT UPDATES

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

### 3.1 DECEMBER 10, 2008

The changes in this construct address the following comments received during the Public Comment and Inspection Testing period (September 29 – October 24, 2008).

The associated comment numbers for these updates are as follows:

5560, 5561, 5562, 5595, 5596

The full text of the comments along with the Technical Committee's disposition can be reviewed on [HITSP Public Web Site](#).

### 3.2 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

### 3.3 JUNE 30, 2009

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

### 3.4 JULY 8, 2009

Upon approval by the HITSP Panel on July 8, 2009, this document is now Released for Implementation.

### 3.5 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.

