

HITSP Anonymize Immunizations and Response Management Data Component

HITSP/C88



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 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

1.0	INTRODUCTION.....	5
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
2.0	COMPONENT DEFINITION.....	7
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	14
2.3.1	Regulatory Guidance.....	14
2.3.2	Selected Standards	15
2.3.3	Informative Reference Standards.....	15
3.0	APPENDIX	16
4.0	DOCUMENT UPDATES	17
4.1	December 10, 2008	17
4.2	December 18, 2008	17
4.3	June 30, 2009.....	17
4.4	July 8, 2009	17
4.5	November 9, 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 Patient Data Elements	10
Table 2-4 Clinical Data Elements.....	12
Table 2-5 Regulatory Guidance	14
Table 2-6 Selected Standards	15
Table 2-7 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 Immunizations and Response Management Data Component provides specific instructions for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. This Component specification provides the ability to anonymize patient identifiable information for Immunizations and Response Management.

Anonymization cannot 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. If you are already familiar with this information, proceed to Section 2.0.

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

Table 1-1 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 interface(s) 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 immunization 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 immunization registries in the context of communicable disease prevention and control is routine for children. However, in addressing adult immunizations, and in consideration of collection and use of the immunization data in data analysis, HITSP supports the use of anonymization and pseudonymization approaches to protect individual privacy and confidentiality. This Component specifies anonymization protections for such data collection and use.

Under 45 CFR 164.502(d), HIPAA defines 18 data elements that under a Safe Harbor approach must be removed from personally identifiable health records in order for those records to be considered anonymized. The AHIC Use Case has defined some demographic data elements of interest that need to be retained in order to accurately evaluate the data for Immunizations and Response Management. This Component specifies removal and aggregation requirements for data variables submitted to Immunization Registries.

The selected standard is the International Organization for Standardization (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 to be 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 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 Immunization Registry	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 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.

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 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

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 immunizations and response management.

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 exceptions apply to the data variables specified below.

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 Patient Data Elements

Data Element	Definition	Data Type ¹	Data Standards ¹	Anonymization Requirements
Father's Name: First, Middle, Last	The current, assumed legal name of the patient's father			Blind
Father's SSN	This is a number assigned by the Social Security Administration			Blind
Insurance Company	The organization providing health insurance to the patient at the time of the immunization event			Blind
Insurance Plan	Type of insurance plan (e.g., Medicaid, HMO, self pay, etc.)			Blind
Last Update Facility	This field identifies the facility of the last update to a patient's/person's identifying and demographic data, as defined in the PID segment. Receiving systems or users will use this field to determine how to apply the transaction to their systems. If the receiving system (such as a hospital's patient management system) already has a record for the patient/person, then it may decide to only update its data if the source is a "trusted" source. A hospital might consider other hospitals trusted sources, but not "trust" updates from non-acute care facilities			Pass through unmodified

¹ This information is provided for informative purposes only and is not determined by this construct for anonymization



Data Element	Definition	Data Type ¹	Data Standards ¹	Anonymization Requirements
Last Update Time/Date	This field contains the last update date and time for the patient's/person's identifying and demographic data, as defined in the PID segment. Receiving systems will use this field to determine how to apply the transaction to their systems. If the receiving system (such as an enterprise master patient index) already has a record for the person with a later last update date/time, then the Electronic Master Patient Index (EMPI) could decide not to apply the patient's/person's demographic and identifying data from this transaction			Blind
Mother's Maiden Name (not always available in an EHR-s)	This field contains the family name under which the mother was born (i.e., before marriage). It is used to distinguish between patients with the same last name			Blind
Mother's Name: First, Middle, Last	The current, assumed legal name of the patient's mother			Blind
Mother's SSN	This is a number assigned by the Social Security Administration			Blind
Next of Kin Address	This field lists the mailing address of the next of kin/associated party			Blind
Next of Kin DOB	This field contains the next of kin/associated party's date of birth			Blind
Next of Kin Relationship	This field defines the personal relationship of the next of kin	Coded	HL7 2.5 Table 0063 - Relationship	Blind
Next of Kin Telephone	The next of kin/associated party's personal phone numbers			Blind
Patient Address	This field lists the mailing address of the patient	XAD-106	HL7	Blind
Patient Alias Name: First, Middle, Last (former names for management of adoptions and name changes)	This field contains names by which the patient has been known at some time	XP-48	HL7	Blind
Patient Birth Date	This is the date and time of an event	Timestamp	HL7 Timestamp	Aggregate Month/Year
Patient Birth Registration Number	This is a number assigned to the patient by state for birth record purposes			Blind
Patient Birth State/Country	This field contains state and country in which patient was born	Coded	FIPS	Covered in the immunization content file – for tracking, these are all covered; Not being used commonly for matching
Patient Birthing Facility	This is the facility where the patient was born			Pass through unmodified
Patient Ethnicity	A segment of a larger society whose members have a common origin and share a common culture. This field further defines patient ancestry. This is allowed to repeat	Coded	HL7 2.5 Table 189 Ethnicity	Blind
Patient Identifier	This field may be populated with MRN, SSN, Medicaid Number, Local Registry ID, or other identifiers collected			Pseudonym (use HITSP/T24 Pseudonymize)



Data Element	Definition	Data Type ¹	Data Standards ¹	Anonymization Requirements
Patient Multiple Birth Indicator	This field indicates whether the patient was part of a multiple birth	Coded	HL7 2.5 Table 136 - Yes/No indicator	Pass through unmodified
Patient Multiple Birth Order	This is a number representing the patient's order of birth	Numeric	HL7, CHI	Blind
Patient Name: First, Middle, Last	The current, assumed legal name of the patient	XPN-48	HL7	Blind
Patient Phone Number	The patient's personal phone numbers	XTN-40	HL7	Blind
Patient Primary Language	This is the patient's primary language	Coded	HL7 2.5 Table 296 Primary Language	Pass through unmodified
Patient Race	These values are consistent with the OMB Notice of revised categories for collection of race and ethnicity data (the combined format.) The complete set is available at: http://www.cdc.gov/od/hissb/docs/Race-EthnicityCodeSet.pdf	Coded	HL7 2.5 Table 005 Race	Blind
Patient Sex	This is the Patient's Sex	Coded	HL7 2.5 Table 001 Administrative Sex M Male F Female U Undifferentiated	Pass through unmodified (note: only if administrative sex, otherwise blind)

The following table describes the anonymization requirements for the immunization event data elements.

Table 2-4 Clinical Data Elements

Data Element	Definition	Data Type	Data Standards	Anonymization Requirements
Action Code	This indicates whether the message is related to a new event, modification of a previously submitted event	Coded	HL7 2.3 Table 0323	Pass through unmodified
Amount Administered (dosage amount):	This field records the amount of pharmaceutical administered			Pass through unmodified
Historical Vaccination Flag Indicator	Indicates that an event represents either a current or a historical immunization	Coded	Use CDC HL7 2.3.1 Implementation Guide Table NIP001	Pass through unmodified
Immunization Event Identifier	TBD			Pass through unmodified
Immunization Information Source	Indication of the individual communicating the immunization information	Coded	Use HL7 Table NIP001	Blind
Immunization Recommendations	Indicates vaccines recommended for patient, based on the patient's history and immunization schedule active in the IIS			Blind
Patient Status in the Immunization Home	Indication of the current status of the patient		Include active, inactive, MOGE, and other classifications Table 0441 HL7 User Defined table	Pass through unmodified
Read Date for Take Response	Date the take response was read or observed	Timestamp		Aggregate month/year



Data Element	Definition	Data Type	Data Standards	Anonymization Requirements
Reason for Non-Vaccination	To express concepts such as history of varicella disease indicator			Blind unless coded
Refusal Reason	This indicates the reason the patient or parent refused the vaccine	Coded	NIP002 - Substance refusal reason	Pass through unmodified
Smallpox Take Response Observation:	For specific vaccines such as smallpox: vaccine specific Optional except if referring to specific vaccines for which smallpox is the only current example Y/N/Equivocal /Unknown/loss-to-follow-up	Coded	NIP table 011	Pass through unmodified
Transaction Information Source	Indication of the source of the immunization information communicated (e.g., PHR, IIS, EMR) Indication of the system type communicating the immunization information (e.g., PHR, IIS, EMR)			Pass through unmodified
Treatment Route	Route by which the vaccine is administered to the patient (only selected values listed)	Coded	HL7 2.5 Table 0162 - Route of administration	Pass through unmodified
Vaccination Date	This is the date and time of an event			Pass through unmodified
Vaccine Administration Facility	Name and address of facility where medical substance was administered			Pass through unmodified
Vaccine Administration Provider	This field is intended to contain the name and provider ID of the person physically administering the pharmaceutical			Pass through unmodified
Vaccine Dose Number	This is the dose number of a vaccine, or a combination vaccine. For HITSP, the valid dose number of a vaccine series			Pass through unmodified
Vaccine Dose Valid Flag	Indicates that a dose administered is considered valid based on the immunization schedule active in the IIS		Y/N	Pass through unmodified
Vaccine Expiration Date	This is the date after which the vaccine/batch must not be use			Pass through unmodified
Vaccine Injection Site	This is the site on the patient where vaccine is administered	Coded	HL7 2.5 Table 0163 - Administrative site	Pass through unmodified
Vaccine Lot Number	This is the lot number of the administered vaccine(s), as shown on the vaccine vial, syringe, or box. This is allowed to repeat			Pass through unmodified
Vaccine Manufacturer	This shows the manufacturer of the vaccine administered to the patient in the immunization event. Developed by CDC, this code set assigned a two letter (later three) code to manufacturers existing at the time. For purposes of consistency in maintaining accurate historical immunization records, the codes have remained intact (or additions made) while the manufacturer names have been updated (e.g., due to mergers of acquisitions) to show the current names. Inactive codes and pointers to current codes are indicated in brackets following the manufacturer name. Notes in italics indicate predecessor organization		Use HL7-defined Table 0227 – Manufacturers of vaccines (code=MVX) found in Appendix 1	Pass through unmodified



Data Element	Definition	Data Type	Data Standards	Anonymization Requirements
Vaccine Type	Code indicating which vaccine is being recorded		Use HL7-defined Table 0292 – Vaccines Administered (code=CVX) found in Appendix NOTE: Though CVX code is the standard for many, some registries use CPT codes. Other codes should be mapped to the interoperability standard code	Pass through unmodified
VFC Eligibility	Indicates a class or category of payment method for immunization services provided. This is allowed to repeat		HL7 2.5 Table 0064 - Financial class	Pass through unmodified

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 identified in Section 2.2.2.1 of this document within the AHIC Public Health 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.

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-5 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 2-6 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 www.iso.org

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-7 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 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 details of updates made to this document.

4.1 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

Minor editorial changes were made to this construct.

4.2 DECEMBER 18, 2008

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

4.3 JUNE 30, 2009

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

4.4 JULY 8, 2009

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

4.5 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.

