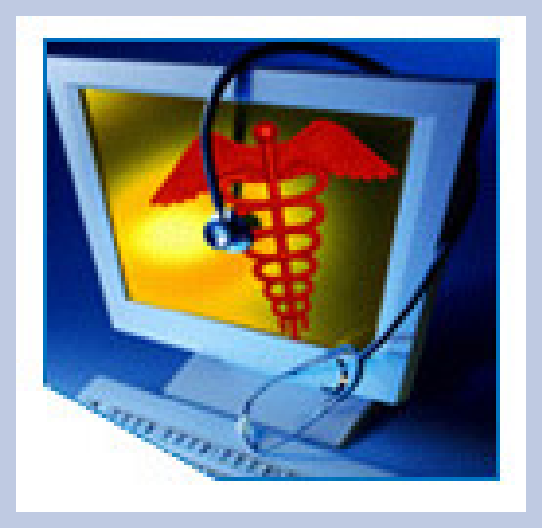
December 13, 2007
Version 2.1

HITSP Pseudonymize Transaction

HITSP/T24



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 18, 2006
1.1	Ready for Public Comment	Biosurveillance Technical Committee	September 12, 2006
1.2	Ready for Implementation Testing	Biosurveillance Technical Committee	October 20, 2006
1.2.1	Review Draft – Released to TC for final review	Population Health Technical Committee	March 28, 2007
1.3	Review Copy	Population Health Technical Committee	April 27, 2007
2.0	Released for Implementation	Population Health Technical Committee	May 11, 2007
2.0.1	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 Pseudonymize Transaction, 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 Transaction Definition.

1.1 OVERVIEW

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

Anonymization, according to the International Organization of Standardization (ISO), is the process that removes the association between the identifying data set and the data subject. Pseudonymization is a particular type of anonymization that both removes the association with a data subject, and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. This enables a process of supplying an alternative identifier, which permits a patient to be referred to by a key that suppresses his/her actual identification information. The purpose of this Transaction is to describe a framework for including Pseudonymization Services in Use Cases that require the use of “dummy” or pseudo references to specific patients or providers. Pseudo-identifiers are intended to allow accessibility to clinical information, while safeguarding any information that may compromise the privacy of the individual patient or provider. Using pseudo-identifiers can assist in compliance with HIPAA regulations regarding suppression of patient identification information.

This Transaction can be used in conjunction with HITSP/TP22 - Patient ID Cross-Referencing. The operation of the Pseudonymization Services in the context of the PIX Actors is described in the present document.

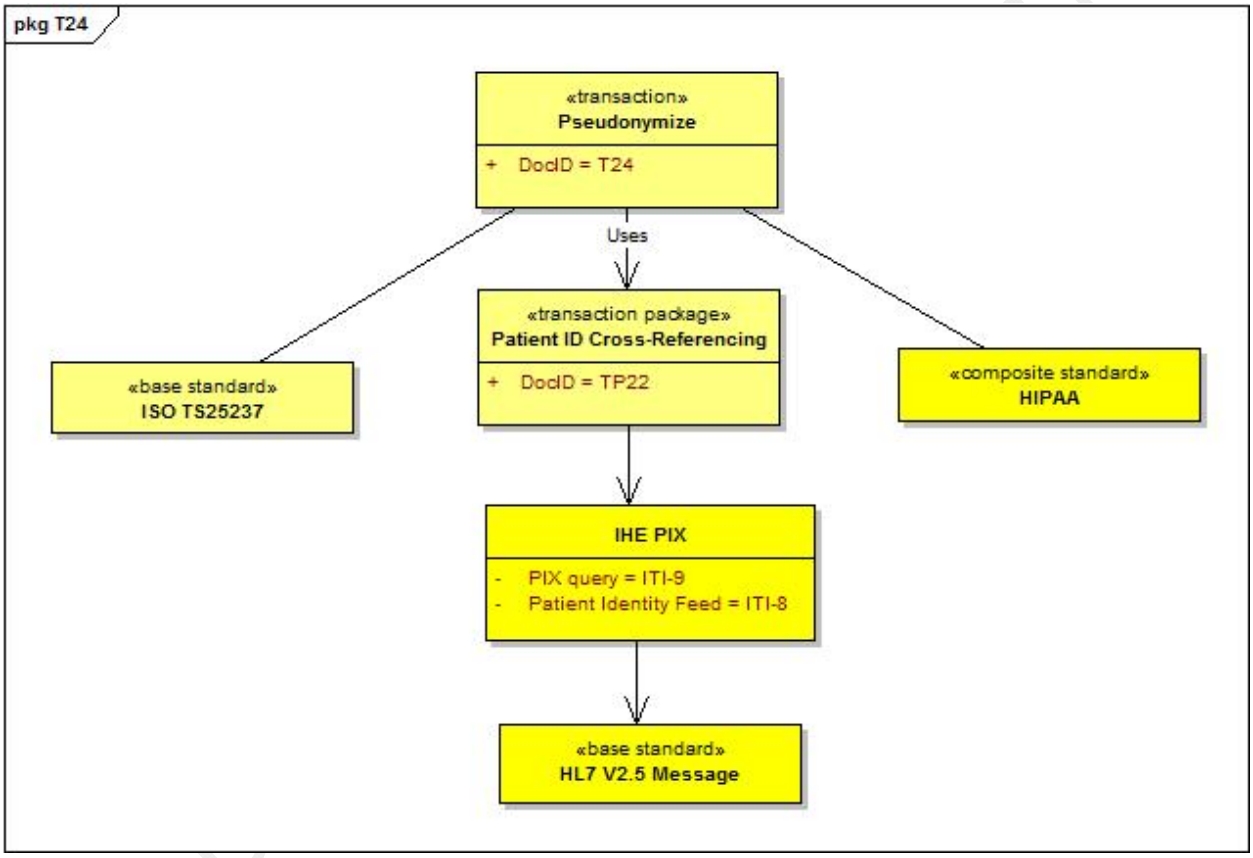
Use Cases for patient identification suppression are described in Section 2.1, “Context Overview.”

1.2 TRANSACTION 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. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). The current Pseudonymize Transaction 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 used to meet the IS requirements. The roadmap in Figure 1.2-1 depicts how this construct

integrates and constrains HITSP constructs and existing standards selected, constrained, or referenced to support the logical grouping of actions that must all succeed or fail as a group, within the defined context of this document. Implementers should read the documents that describe the constructs represented in the diagram for their details and specific uses. The most effective way for a reader to review the construct roadmap for any HITSP specification is to examine the document currently being read (indicated within the roadmap diagram by a bright yellow box) and its relationship with other HITSP documents. Readers should also review supporting Interoperability Specification documentation to understand the context of the specific usage of this document.

Figure 1.2-1 Transaction Construct Roadmap



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

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

Certain materials contained in this Interoperability Specification are reproduced from HL7 Version 2.5 with permission of Health Level Seven, Inc. No part of the material may be copied or reproduced in any form outside of the Interoperability Specification documents, including an electronic retrieval system, or made available on the Internet without the prior written permission of Health Level Seven, Inc. Copies of standards included in this Interoperability Specification may be purchased from the Health Level Seven, Inc. Material drawn from these standards is credited where used.

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 TRANSACTION DEFINITION

Transactions are a logical grouping of actions, including necessary content and context that must all succeed or fail as a group.

2.1 CONTEXT OVERVIEW

This section provides a general description of the Transaction. It includes a detailed definition of the Transaction and the reason for its use. It also provides all the necessary background information that further describes the context in which the Transaction is needed, and the Components or composite standards that the Transaction is based on.

This Transaction is defined to support pseudonymization of protected health information. Pseudonymization is a particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. This may be provided for the patient or a provider. This construct is currently limited to patient-centric transactions where the primary subject of the pseudonymization request is a patient, and where the information about that patient may contain provider identifiers that may need to be Pseudonymized.

The following paragraphs provide further description of this construct from the context of specific Use Cases:

A. Standard Use Case[1]

In the standard Use Case, a Clinical Information System leverages a Patient Identity Source to issue and provide (via the Patient Identity Feed) identification and demographic information about a person to a Person Identifier Cross-Reference (PIX) Manager. A PIX Manager is a type of Person Identification Service. The Person Identification Service registers this patient and/or provider identity information and invokes Pseudonymization Services (a trusted third party) to obtain pseudo-identifying information to be provided to, and used by, Person Identity Consumers. This includes supporting an inquiry about the person in the context of the originating Clinical Information System's domain. The pseudo-identifying information provided for this person in response to the originating Clinical Information System's Patient Identity Feed is unique and distinct from the information provided in response to any other Clinical Information System's Patient Identity Feed.

A second Clinical Information System may issue an Identity Feed to the Person Identification Service containing identification and/or demographic information about the same person within a different domain. As with the first Patient Identity Feed described above, the Person Identifier Cross-Reference Manager

[1] Future considerations are necessary to generalize the purpose, the types of HL7 Feeds that may be leveraged, and to harmonize with the HITSP Security and Privacy TC ongoing and pending efforts in identity management.

will register this information and invoke Pseudonymization Services to obtain pseudo-identifying information (in the context of this second Clinical Information System's domain). This information is then provided to the Person Identity Consumers that inquire about the person, including the originating Clinical Information Systems. The pseudo-identifying information provided for this person in response to this second Clinical Information System's Person Identity Feed is unique and distinct from the information provided to any other Clinical Information System's Person Identity Feed, including that of the first Clinical Information System.

Person Demographics are not returned. They are only used to get pseudonymization data. To address times when supplied demographics differ from the Record Locator Service, the implementation approach needs to be defined. In cases where demographic information is not available (e.g., for a laboratory receiving an order), the Record Locator Service will have to support definition of a pseudonymized identifier without demographic data.

Relationships among Real and Pseudo-identifiers

The Person Identity Cross-Reference Manager maintains associations among all identifiers for a person, both real and pseudo-identifiers, in all domains. Pseudo-identifiers will be provided in response to any Get Person Identifier request by any domain having a relationship with the Person Identity Cross-Reference Manager. However, note that only the Person Identity Cross-Reference Manager is aware of the relationships among all the "real" identities of the person. Each data source (e.g. Clinical information System) only knows the "real" identifying information that it assigns and maintains, while the data target (e.g. public health agency, quality measurement system) does not know any "real" identifying information.

B. Public Health Extension

As an extension of the standard Use Case given immediately above, a Public Health Agency may receive information about individual patients within its jurisdiction, from documents or transactions. This Use Case extension supports the scenario where there is a reason to maintain such information in a pseudonymized information resource (e.g. for Biosurveillance). In this extension, the Patient Identifier Cross-Reference (PIX) Manager (from HITSP/TP22 - Patient Identifier Cross-Referencing) is an instantiation of a Person Identification Service. Prior to the transmission of the information about individual patients, the Patient Identifier Cross-Reference Manager (PIX Manager) can be directed to invoke the Pseudonymization Services to allot a third set of pseudo-identifying information to be transmitted to the Public Health Agency. This will suppress the actual identification of the patient.

C. Quality Extension

As an extension of the standard Use Case given above, a Quality Measure and Reporting Enterprise may receive information about individual patients from documents or transactions. The information sent may also include provider information. This Quality Extension supports the case where there is a reason to communicate pseudonymous information related to the patient, the provider, or both. In this extension, the Patient Identifier Cross-Reference (PIX) Manager (from the HITSP/TP22 - Patient Identifier Cross-Referencing) is an instantiation of a Person Identification Service for the patient. To suppress the actual

identification of the patient, prior to the transmission of the information sent to the Quality Measure and Reporting Enterprise, the Patient Identifier Cross-Reference (PIX) Manager can be directed to invoke the Pseudonymization Services to allot a third set of pseudo-identifying information to be transmitted to the Quality Measure and Reporting Enterprise. For suppressing the identification of the provider, prior to the transmission of the information sent to the Quality Measure and Reporting Enterprise, the Person Identification Service can be directed to invoke the Pseudonymization Service to allot a third set of pseudo-identifying information to be transmitted to the Quality Measure and Reporting Enterprise.

Pseudonymization through the trusted third party can support re-identification. Where the implementation requires re-identification, such as to support case investigation and other public health event detection and management, it is expected that re-identification will be executed in accordance with ISO/TS 25237. Reasons for re-identification (per ISO/TS 25237) that should be considered in future specifications include:

- Verification and validation of data integrity
- Checking for suspected duplicate records
- Enabling requests for additional data
- Linking to supplement research information variables
- Compliance audits
- Informing data subjects or their care providers of significant findings
- Facilitating follow-up research
- Law enforcement

2.1.1 TRANSACTION CONSTRAINTS

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

Table 2.1.1-1 Transaction Constraints

Constraint
Patient Identity Consumers may not receive real identifiers. They may receive only pseudo-identifiers, for patient records outside their own domain.
Systems may be integrated to allow organizations implementing HITSP/T23 - Patient Demographics Query to receive pseudonymized identification information. This is done by binding a PDQ actor to a PIX actor in one of the following groupings: PDQ Patient Demographics Supplier with PIX Patient Identifier Cross-Reference Manager PDQ Patient Demographics Supplier with PIX Patient Identifier Cross-Reference Consumer PDQ Patient Demographics Consumer with PIX Patient Identifier Cross-Reference Consumer Implementation considerations for each of these groupings are discussed in IHE IT Infrastructure Technical Framework, Volume 3 [IHE ITI-TF-2 V3.0] Appendix M, “Using Patient Demographics Query in a Multi-Domain Environment”

2.1.2 TECHNICAL ACTORS

This section describes the technical actors that need to be integrated in order to meet the interoperability requirements for this Transaction. A technical actor represents an entity internal to a software application, which is engaged in one or more specific Transactions to support a specific aspect of a real world information interchange (e.g., set of message exchanges). The table below lists the technical actors involved in the Transaction, a definition of their roles, an indication of their optionality, the specific Transactions and content with which they are involved, and the optionality of the associated transactions and/or content.

Table 2.1.2-1 Technical Actors

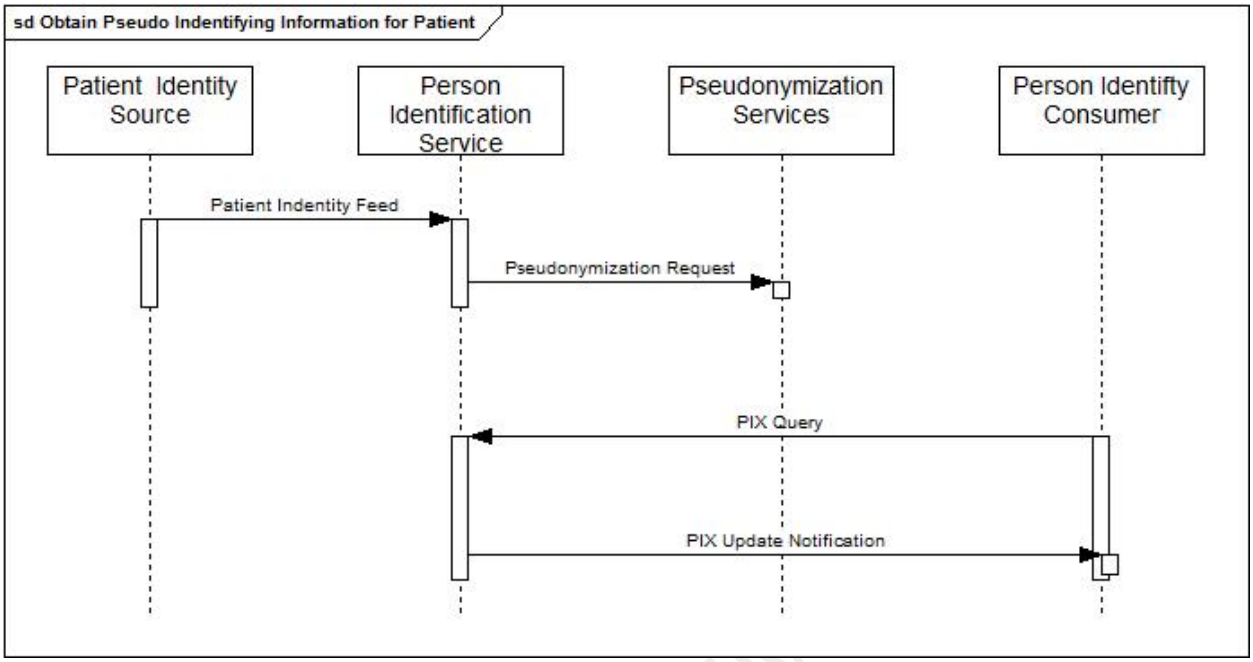
Actor	Description	Used in Construct/ Standard	Transaction/Content	T/C Optionality
Patient Identity Source	Sends patient demographic information to the Patient Identifier Cross-Reference (PIX) Manager. Patient demographic information sent may also contain provider identifiers for pseudonymization processing.	TP22	PIX Identity Feed	R
Person Identification Service (for patient-centric transactions, this is the Patient Identifier Cross-reference (PIX) Manager)	System that maintains a cross-domain person and/or patient index including all known identifiers (real and pseudo) for each person and/or patient, within all domains with which it communicates.	TP22	Patient Identity Feed	R
		TP22	PIX Query	R
		TP22	PIX Update Notification	R
		T24	Pseudonymization Request	R
Pseudonymization Services	Module or service that can be invoked by Patient Identifier Cross-Reference (PIX) Manager (see next section) to return pseudo-identifier upon request	T24	Pseudonymization Request	R
Person Identity Consumer (for patients, this is Patient Identity Consumer)	System that wishes to know alternate identifiers (real and pseudo) for person and/or patients within its domain or pseudo-identifiers for person and/or patients outside its domain.	TP22	PIX Query	R
			PIX Update Notification	O

NOTE: Optionality **=** "R" for Required, "R2" for Required if known, "O" for Optional, or "C" for Conditional. Conditional footnotes are further described below.

2.1.3 ACTOR INTERACTIONS

The following sections document the content of the Transaction and the basic process flows that are supported by the Transaction. It describes the underlying events that fulfill the Transaction, the sequence and timing of the events, and the specific actors involved. Process flow diagrams are provided to illustrate the process relationships.

Figure 2.1.3-1 Actor Interactions



To obtain pseudo-identifying information for a person, a Person Identification Service invokes Pseudonymization Services via a remote procedure call (RPC). The Person Identification Service passes *person demographic information* to the Pseudonymization Services. The Pseudonymization Services then use a cryptographic algorithm to map the person demographic information that is subsequently returned to the caller.

The following sections provide additional detail regarding the processes and conditions within each of the identified technical actors that are identified above.

2.1.4 PRE-CONDITIONS

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

Table 2.1.4 -1 Pre-conditions

Pre-condition
It is expected that the security framework under which this Transaction operates is in accordance with the Interoperability Specification that references this construct. Therefore all applicable HITSP Security and Privacy constructs are implemented as required.
Patient Identifier Cross-Reference Manager will have established a relationship of trust with the Pseudonymization Services.
The Patient Identity Source will be known both to the Patient Identifier Cross-Reference (PIX) Manager and to the Pseudonymization Services.

.

2.1.4.1 PROCESS TRIGGERS

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

Table 2.1.4.1-1 Process Triggers

Process Trigger
Pseudonymization is needed for patient and/or provider.

2.1.5 POST-CONDITIONS

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

Table 2.1.4-1 Post-conditions

Post-condition
No applicable post-conditions.

2.1.5.1 REQUIRED OUTPUTS

This section identifies the required outputs that must be produced at the end of the Transaction in order for the Transaction to be deemed successfully completed. This includes the format and usage of the required output.

Table 2.1.5.1-1 Required Outputs

Required Output	Format/Usage
An alternative identifier that permits a patient to be referenced by a key that suppresses his/her actual identification information is supplied.	Not specified at this time.

2.1.6 DATA FLOWS

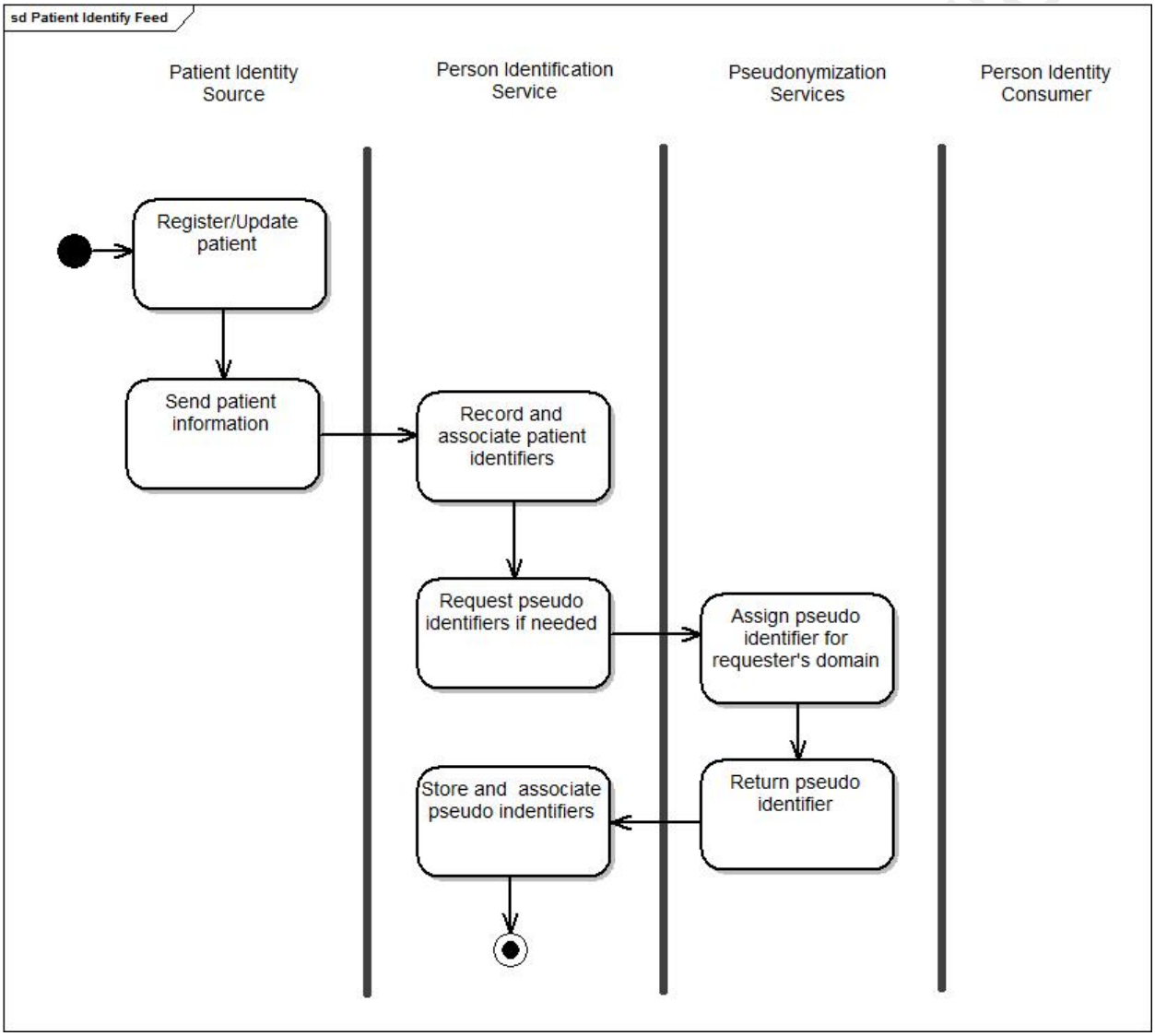
This section describes the basic data flows that are supported by this Transaction. It also describes the format of the data, the data sources, and the relevant actors involved in the successful flow of data for the Transaction. Any prevailing pre and post conditions are identified, as well as the purpose of each data post-condition associated with each Transaction. Any data that need to be made available to particular actors are highlighted, as well as the conditions and processes that will use the data to achieve the stated post-conditions.

The subsections below describe the inclusion of the Pseudonymization Services within the PIX related transactions. Additional details of the data flows of the Patient Identity Feed, PIX Query, and PIX Update Notification may be found in HITSP/TP22 - Patient ID Cross-Referencing.

2.1.6.1 PATIENT IDENTITY FEED

Figure 2.1.6.1-1 below describes the inclusion of the Pseudonymization Services within the Patient Identity Feed transaction. Additional details of the data flow may be found in HITSP/TP22 - Patient ID Cross-Referencing.

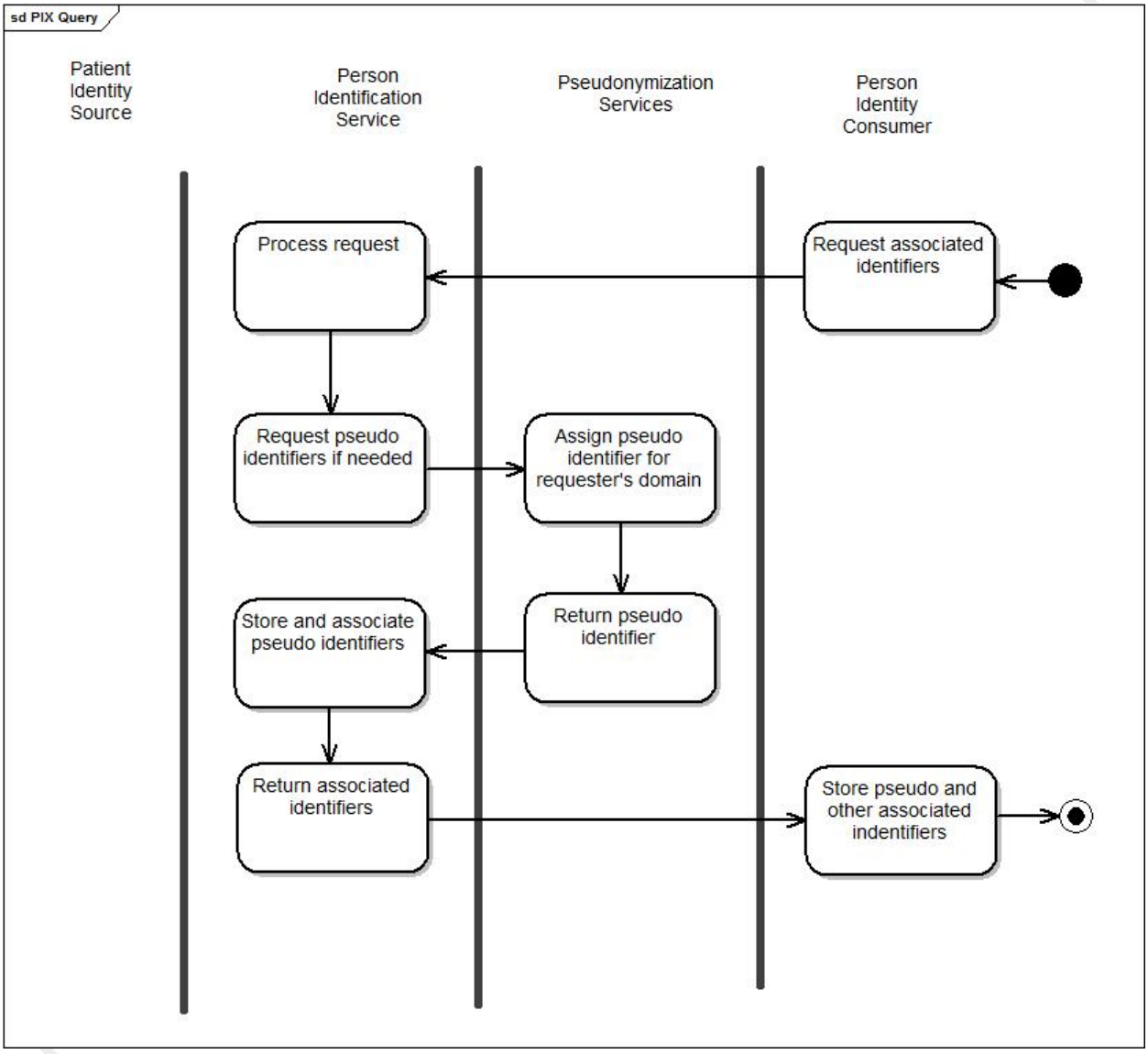
Figure 2.1.6.1-1 Patient Identity Feed



2.1.6.2 PIX QUERY

Figure 2.1.5.2-1 below describes the inclusion of the Pseudonymization Services within the PIX Query transaction. Additional details of the data flow may be found in HITSP/TP22 - Patient ID Cross-Referencing.

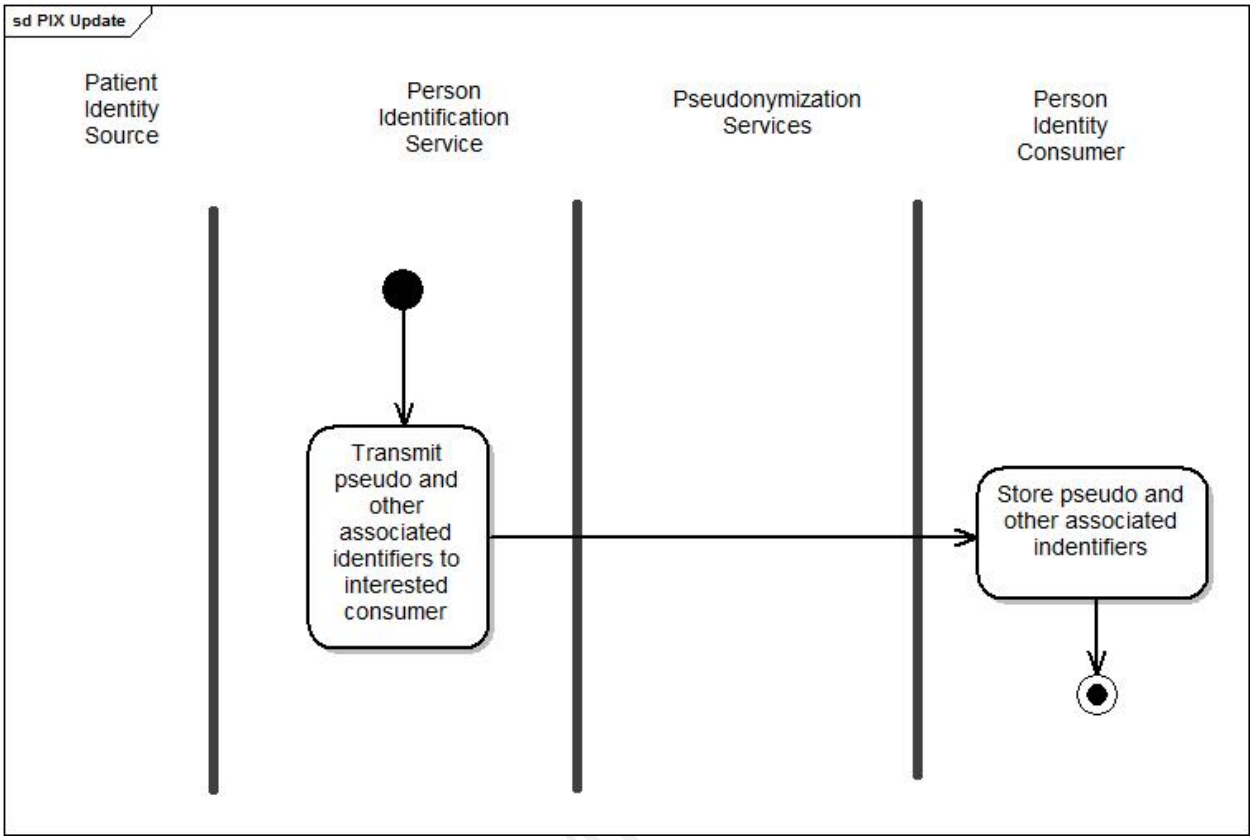
Figure 2.1.6.2-1 PIX Query



2.1.6.3 PIX UPDATE NOTIFICATION

Figure 2.1.6.3-1 below describes the inclusion of the Pseudonymization Services within the PIX Update Notification transaction. Additional details of the data flow may be found in HITSP/TP22 - Patient ID Cross-Referencing.

Figure 2.1.6.3-1 PIX Update



2.2 LIST OF HITSP CONSTRUCTS

The following list of constructs and their definitions are used by the Transaction specification.

Table 2.2-1 List of HITSP Constructs

Construct Name	Technical Actors	Description	Event/Action Code	Content
HITSP/TP22 - Patient ID Cross-Referencing	Patient Identity Source Patient Identity Cross-Reference Manager Patient Identity Consumer	These Patient ID Cross-Referencing (PIX) and Patient Identity Feed Transactions are portions of Interoperability Specifications that deal with identifying and cross-referencing different patient attributes for the same patient	NA	See HITSP/TP22 for details

2.2.1 CONSTRUCT DEPENDENCIES

The following table shows a list of Components with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific construct:

Table 2.2.1-1 Construct Dependencies

Construct	Depends On (Name of Component that it depends on)	Dependency Type (Pre-condition, post-condition, general)	Purpose (Reason for this dependency)
No applicable dependencies			

2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

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

Table 2.2.2-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
QPD-3	HITSP/TP22 - Patient ID Cross-Referencing	For provider pseudonymization, the PIX Query message shall use the field QPD-3 Person Identifier to convey a single Person ID uniquely identifying the provider within a given Identification Domain.	Pre-condition	To allow PIX Query message to support provider pseudonymization.
PV1-7, PV1-8, PV1-9, PV1-17, PR1-12	HITSP/TP22 - Patient ID Cross-Referencing	For provider pseudonymization, the Patient Identity Feed shall include provider information in at least one of PV1-7, PV1-8, PV1-9, PV1-17, PR1-12 to be pseudonymized.	Pre-condition	To convey the provider identifiers that need to be pseudonymized.

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 Transaction specification:

Table 3.1-1 List of Standards

Standard	Description
Health Insurance Portability and Accountability Act (HIPAA) -- Administrative Simplification	A listing of national standards plus rules adopted by federal regulation for electronically communicating specified administrative and financial healthcare transactions, and protecting the security and privacy of healthcare information, as applied to the three types of defined covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct any of the specified healthcare transactions. See the Code of Federal Regulations, Title 45, Parts 160, et. seq. for more information.
Health Level Seven (HL7) Version 2.5[2]	The HL7 Version 2.5 Messaging Standard is an application protocol for electronic data exchange in healthcare. It and prior versions have widespread use in the U.S. and internationally. Both message formats and value sets / code tables (e.g., diagnosis type, gender, patient class, result status, specimen collection method, abnormal flags, observation result status codes interpretation, timestamp format) are contained in the standard. Of particular focus for HITSP Interoperability Specifications are message formats described in Chapters 2, 3, 5, and 7 including patient demographic (ADT) and lab result reporting. These are also used within composite standards from IHE for Patient Identity Cross-Referencing and Feed (PIX), Patient Demographics Query (PDQ), and Acknowledgements. Visit www.hl7.org for more information.
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0	The IHE IT Infrastructure Technical Framework defines specific implementations of established standards to achieve integration goals that promote appropriate sharing of health information to support optimal patient care. IHE Integration Profiles, offer a common language that healthcare professionals and vendors may use in communicating requirements for the integration of products. The current version of the ITI-TF, rev. 3.0 for Final Text, specifies the IHE transactions defined and implemented as of December 9, 2006. The latest version of the IHE Technical Framework is available at www.ihe.net.
International Organization for Standardization (ISO) Health Informatics -- Pseudonymization, Unpublished Technical Specification # 25237	Health Informatics – Pseudonymization. Approved as a Technical Specification March, 2007. Visit www.iso.org for more information.

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

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 table 2.1.1-1, and implement all of the required actors from table 2.1.2-1, 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 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.

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 MAY 11, 2007

This document is now Released for Implementation.

5.2 DECEMBER 5, 2007

5.2.1 GENERAL UPDATES

- Updated to new template
- Added support for provider data pseudonymization
- Generalized term ‘patient’ to ‘person’

5.2.2 SECTION 2.1

- Updated context to include Quality in addition to Public Health
- Updated the standard use case as a general person pseudonymization use case
- Added Quality Extension

5.2.3 SECTION 2.2.2

- Added constraints to the Patient Identity Feed and PIX Query for support of provider pseudonymization

5.3 DECEMBER 13, 2007

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