January 25, 2010
Version 1.0

HITSP Retrieve Pseudonym Capability

HITSP/CAP138

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Capabilities Team

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
0.0.1	Populate Template	Capabilities Team	November 9, 2009
0.0.2	Review Copy	Selected Perspective, Domain and/or Tiger Team Reviewers	January 18, 2010
1.0	Released for Implementation	Selected Perspective, Domain and/or Tiger Team Reviewers	January 25, 2010

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

This Healthcare Information Technology Standards Panel (HITSP) document is divided into Requirements Analysis, External Capability Options, Design Specifications and Standards sections which may be used by analysts, architects and implementers. Analysts refer to this document to determine if the Capability satisfies their requirements. Architects and system implementers refer to this document as the architectural specifications for a system design, while software developers will use a Capability as the source of the design for interoperable information exchange. The Appendix lists requirements satisfied by this Capability.

All sections may be useful to analysts and architects. However as shown in Table 1-1, different readers may find specific sections of greater interest and utility. This table is provided as an aid to readers to assist them in identifying sections to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 1-1 Reader's Guide for Capability

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional security and privacy functions supported by the Capability
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	Lists regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	5.2 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues

1.1 CAPABILITY OVERVIEW

This Capability addresses interoperability requirements to support 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 Capability is to offer a pseudonymization framework for situations that require the use of specific data without disclosing the specific identity of 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. However, unlike anonymization, the alternative identifier key can be used to re-identify the individuals whose data was used.

1.2 SCOPE

A Capability enables business and policy requirements for a business need to be implemented through information exchanges specified in HITSP constructs. The objective of a Capability is to provide the bridge between the business, policy and implementation disciplines by defining a set of information exchanges at a level relevant to policy and business decisions and specifying the use of HITSP constructs sufficiently for implementation. A Capability supports stakeholder requirements and business processes and includes information content, infrastructure, security and privacy. The design of Capabilities leverages existing HITSP constructs and communication methodologies. As new constructs become available, the scope of this Capability may be extended.

1.3 COPYRIGHT PERMISSIONS

1.4 REFERENCE DOCUMENTS

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from HITSP Web Site.

Table 1-2 Reference Documents

Reference Documents	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
TN901 - Clinical Documents	TN901 is a reference document that provides the overall context for use of the HITSP Care Management and Health Records constructs
TN903 – Data Architecture	TN903 is a reference document that provides the overall context for use of the HITSP Data Architecture constructs
TN904 – Harmonization Framework and Exchange Architecture	TN904 is a reference document that provides the overall context for use of the HITSP Harmonization Framework and Exchange Architecture constructs

1.5 GUIDANCE FOR USE OF A CAPABILITY

NOTE: For questions related to details on HITSP Capabilities and HITSP System Roles, please refer to HITSP/TN904 Harmonization Framework and Exchange Architecture Technical Note.

To use a HITSP Capability, a HITSP Interoperability Specification or an implementation conformance statement must assign specific systems to one or more HITSP Capability System Roles and identify how the HITSP Capability Options are to be addressed. In order to assign systems to HITSP System Roles, the reader uses Table 2-3 Supported Information Exchanges to determine what systems can support the specific information exchanges required. For an example of how HITSP System Roles and systems are mapped, readers can consult a HITSP Interoperability Specification Table 3-3 Orchestration of

Capabilities by System. In the case of an Implementation Guide, systems can be assigned to HITSP System Roles using a similar methodology.

The use of a HITSP Capability implies that these specific rules will be followed:

- For each HITSP Capability System Role listed in Table 2-2 Capability System Roles, the defined responsibilities of that HITSP Capability System Role are supported. Responsibilities for the HITSP Capability System Role are defined as support for the HITSP Construct interfaces listed in Section 4.3 Specified Interfaces by System Role. Support implies that the system assigned to the HITSP Capability System Role makes the associated HITSP construct interfaces available for use by other systems. For those HITSP construct interfaces in Section 4.3 that have associated content optionality, the HITSP Capability System Role must comply with the optionality condition listed in Table 4-6 Implementation Conditions.
- Responsibilities also include the constraints and assumptions associated with use of a Capability, as outlined in Table 4-3 Context. For those Capabilities with Section 3.2 options, the following additional rules apply:

1. Each topology option listed in Table 3-2 Topology Related Options should be supported by the implementation
1. Each content import option listed in Table 3-3 Content Import Options should be supported by the implementation
2. Each document content option listed in Table 3-4 Document Content Options should be supported by the implementation

2.0 REQUIREMENTS ANALYSIS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 2-1 Reader's Guide for Section 2.0

Document Section	Section Number	Intended Audience	Information Contained
Section 2.0 Requirements Analysis	2.1 Introduction	Policy Managers Policy Analysts Executive Leadership	Provides an overview of the requirements which this Capability addresses, and identifies the system roles supported by the Capability
	2.2 Requirements	Program Managers Policy Analysts Executive Leadership Architects Business Analysts	Defines the actual information exchanges supported by the Capability in terms of exchange actions and exchange content. It shows how these roles can be assigned at a higher level to real world systems, such as an Electronic Health Record

2.1 INTRODUCTION

Table 2-2 summarizes the system roles of the Capability. Section 2.2 identifies how these system roles participate in the set of information exchanges.

Table 2-2 Capability System Roles

System Role	System Role Definition
Pseudonymization Service	The service that responds to requests for pseudonyms
Request Patient Identity	The source that requests the pseudonym for the patient identity submitted

2.2 REQUIREMENTS

2.2.1 INFORMATION EXCHANGES

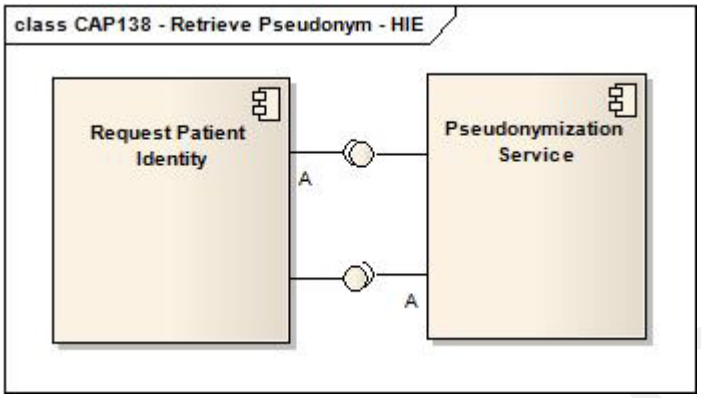
Table 2-3 defines each of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA) or Exchange Content (EC) used.

Table 2-3 Supported Information Exchanges

Information Exchange Identifier	Exchange Action	Exchange Content
A	Request & Response	Pseudo Identity

Figure 2-1 identifies how this Capability supports various system roles within multiple system architectures. For example, either an Electronic Health Record (EHR) system or a Health Information Exchange (HIE) might fill a document repository system role in an information exchange). In an implementation architecture, system roles may be combined locally (e.g., Hospital EHR System) and in others, the system roles may be provided by multiple-distributed trusted third parties (e.g., pharmacies within an HIE).

Figure 2-1 Information Exchanges Between System Roles



3.0 EXTERNAL CAPABILITY OPTIONS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 3-1 Reader's Guide for Section 3.0

Document Section	Section Number	Intended Audience	Information Contained
Section 3.0 External Capability Options	3.1 Security and Privacy	Policy Analysts Architects Business Analysts Developers	Describes the integrated and optional Security and Privacy functions supported by the Capability

This section is primarily for architects, engineers and analysts. It allows those who consider using this Capability to evaluate and/or constrain the options that are externally made available for the Capability implementers.

Interoperability among system roles defined by this Capability often requires the selection of consistent options.

3.1 SECURITY AND PRIVACY

The application of Security and Privacy is highly influenced by the security and privacy policies. The HITSP Security and Privacy Technical Note (HITSP/TN900) provides a detailed discussion of the security and privacy constructs, including consideration and appropriate context for needed security and privacy related policy decisions. Security and privacy constructs are integrated comprehensively into the Service Collaborations. The actual constructs used and the way in which the constructs are used is dependent on the policies and physical setting. Conformance claims are against the security and privacy constructs that are chosen to enforce the policies.

4.0 DESIGN SPECIFICATION

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 4-1 Reader's Guide for Section 4.0

Document Section	Section Number	Intended Audience	Information Contained
Section 4.0 Design Specification	4.1 Requirements Mapped to Constructs	Program Managers Architects Business Analysts Developers	Maps the information exchanges developed in requirements to the actual HITSP construct used by the Capability to support the exchange
	4.2 Constraints and Assumptions	Business Analysts Developers	Lists the context that is necessary to use the Capability, including constraints, assumptions, pre-conditions, post-conditions and triggers
	4.3 Specified Interfaces by System Role	Business Analysts Developers	Identifies the constructs and their interfaces assigned to each system role. It also lists the implementation conditions for use

4.1 REQUIREMENTS MAPPED TO CONSTRUCTS

4.1.1 CONSTRUCTS

Table 4-2 defines the mapping of the Information Exchanges supported by this Capability in terms of the Exchange Action (EA), Exchange Content (EC) and any Constraints applied to the Information Exchange with specific initiating and/or responding system interfaces. This provides the traceability of constructs to the information exchanges identified in Section 2.2 above. Content modules and terminology components are not listed here because they are referenced by other constructs, but do not provide an interface. HITSP/TN903 discusses how content modules and terminology components are referenced by other constructs.

Table 4-2 Information Exchanges Mapped to Constructs

Information Exchange Identifier	Exchange Type	Construct Identifier	Description
A – Request and Response Patient Identification Management	Action	HITSP/SC110 – Patient Identification Management	Provides the ability to lookup and/or cross-reference patient identities
A – Request and Response Patient Identification Management	Content	HITSP/T24 – Pseudonymize	Used to provide access to use specific pseudonyms for patients

4.2 CONSTRAINTS AND ASSUMPTIONS

Table 4-3 specifies the context that must be provided in order to use the Capability, identifying any assumptions, pre-conditions, post-conditions, and triggers relevant for use of the Capability.

Table 4-3 Context

Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
Security/communications policies between institutions are established using established standards for trust management, risk assessment and cross-jurisdiction information exchange	Assumption
Re-identification of pseudonymized data as needed is authorized	Assumption
Security standard selection must be done in accordance with HIPAA and based upon the risk assessment for the selected architecture	Assumption
Data to be pseudonymized is not anonymized	Pre-condition

Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
Security and Privacy policies, procedures and practices are commonly implemented to support acceptable levels of consumer/patient privacy and security	Pre-condition
Legal and governance issues regarding data access authorizations, data ownership, and data use are in effect, secure communications are in place, and all policy, compliance, and authorization issues are addressed through automated or manual means	Pre-condition
If pseudonymization is used, all re-identification events for Pseudonymized quality data shall record the re-identification purpose from the list provided in section 5.3.1 of ISO TS25237 Health Informatics: Pseudonymization	Post-condition
Policy for re-linking is defined	Pre-condition
Patient level data requires pseudonymization by policy	Trigger

4.3 SPECIFIED INTERFACES BY SYSTEM ROLE

This section specifies the HITSP Capability interfaces in terms of the System Roles identified in Table 2-2 Capability's System Roles.

Table 4-4 below specifies interfaces for the first system role as defined in Table 2-2.

Table 4-4 Request Patient Identity System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Request Patient Identity	Initiating	Patient Identification Management (HITSP/SC110)	C138 [101]
Request Patient Identity	Initiating	Pseudonymization (HITSP/T24)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-5 specifies interfaces for responding system roles as defined in Table 2-2.

Table 4-5 Pseudonymization Service System Role Mapped to HITSP Construct Interfaces

Construct Interface	Interface Type	T/TP/SC or Content	T/SC/Content Optionality
Person Identification Service	Responding	Patient Identification Management (HITSP/SC110)	C138 [101]
Person Identification Service	Responding	Pseudonymization (HITSP/T24)	R

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

Table 4-6 specifies optionality conditions referenced in Table 4-4 through Table 4-5 above.

Table 4-6 Implementation Conditions

Condition ID	Condition Description
C138 [101]	Implementations of this Capability SHALL support the HITSP/T24 Pseudonymize option

5.0 STANDARDS

The following table is provided as an aid to readers to assist them in identifying the parts of this section to focus on. Readers are encouraged to review all sections of this document to further their understanding of HITSP's work.

Table 5-1 Reader's Guide for Section 5.0

Document Section	Section Number	Intended Audience	Information Contained
Section 5.0 Standards	5.1 Standards Used	Program Managers Policy Analysts Architects Business Analysts Developers	List regulatory guidance, selected standards and informative references used by the Capability and all its supporting constructs
	5.2 Standards Gaps and Overlaps	Program Managers Policy Analysts Architects Business Analysts Developers	Identifies gaps or overlaps in standards to implement the Capability including a plan to resolve issues

5.1 STANDARDS USED

5.1.1 REGULATORY GUIDANCE

Table 5-2 lists any regulatory guidance that determines or constrains use of standards.

Table 5-2 Regulatory Guidance

Regulation	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. For more information see the Code of Federal Regulations, Title 45, Parts 160, et. Seq.

5.1.2 SELECTED STANDARDS

Table 5-3 lists the standards selected as relevant to this Capability.

Table 5-3 Selected Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later	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, specifies the IHE transactions defined and implemented as of August 22, 2007. The latest version of the IHE Technical Framework is available at www.ihe.net
International Organization for Standardization (ISO) Health Informatics -- Pseudonymisation, Unpublished Technical Specification # 25237	Health Informatics – Pseudonymization. Approved as a Technical Specification March, 2007. Visit www.iso.org for more information

5.1.3 INFORMATIVE REFERENCE STANDARDS

Table 5-4 includes reference standards that inform the overall semantic interoperability.

Table 5-4 Informative Reference Standards

Standard	Description
Health Level Seven (HL7) Version 2.5[1]	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, Volume 2 Transactions, Appendix M Using Patient Demographics Query in a Multi-Domain Environment	Appendix M - Using Patient Data Query (PDQ) in a Multi-Domain Environment, provides an architectural discussion of how Query Parameter Definition, QPD-8 is processed

5.2 STANDARDS GAPS AND OVERLAPS

Table 5-5 identifies the information exchange requirements and known standards gaps, along with the recommended resolutions to the gaps.

Table 5-5 Information Exchange Requirements (IER) and Associated Standards Gaps

IER Gap Description	Responsible HITSP TC	Design Approach	Required Standards Now Unavailable for Constructs	SDO Working on Unavailable Standards	Expected Availability
None					

Table 5-6 lists any standards overlaps and describes plans to resolve each of the overlaps.

Table 5-6 Information Exchange Requirements (IER) and Associated Standards Overlaps

IER Number	Summary Description	Standard Overlap	Recommended Resolution
None			

[1] 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.

6.0 APPENDIX

This section may include additional materials referenced throughout this document, such as requirements analysis tables and figures. If the Capability is yet to be implemented, it may contain the candidate standards for Tier 2 evaluations.

- HITSP/IS02 Biosurveillance
- HITSP/IS06 Quality
- HITSP/IS10 Immunizations and Response Management
- HITSP/IS11 Public Health Case Reporting
- HITSP/IS92 Newborn Screening

7.0 DOCUMENT UPDATES

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

7.1 NOVEMBER 9, 2009

No changes. This is the first published version of the document.

7.2 JANUARY 18, 2010

Updated to HITSP Capability Template Version 2.3.

7.3 JANUARY 25, 2010

Upon approval by the HITSP Panel on January 25, 2010, this document is now Released for Implementation.