

HITSP Security and Privacy Technical Note

HITSP/TN900



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Domain Technical Committee



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	July 20, 2007
1.0.1	Review Copy	Security and Privacy Technical Committee	October 5, 2007
1.1	Released for Implementation	Security and Privacy Technical Committee	October 15, 2007
1.1.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	August 20, 2008
1.2	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	August 27, 2008
1.2.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	June 30, 2009
1.3	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	July 8, 2009
1.3.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	January 18, 2010
1.4	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	January 25, 2010



TABLE OF CONTENTS

1.0	INTRODUCTION.....	6
1.1	Overview.....	6
1.1.1	HITSP Security and Privacy Policy	6
1.1.2	HITSP Security and Privacy Management Overview	7
1.2	Security and Privacy Relationship to Use Cases	7
1.3	Copyright Permissions.....	7
1.4	Terminology.....	7
1.5	HITSP References.....	8
2.0	SECURITY AND PRIVACY SCOPE.....	9
2.1	Security and Privacy Principles	9
2.2	Policy Groups	11
2.3	Guidance Standards.....	12
2.4	Relationship of Constructs to Security and Privacy Policies	12
2.5	Focus of Construct Development on Interoperability	13
3.0	ROADMAP AND GAPS OF THE HITSP SECURITY AND PRIVACY CONSTRUCTS	15
3.1	Selection of Security and Privacy Constructs.....	15
3.2	Roadmap for Security and Privacy Constructs.....	16
3.3	Limitations from Use Cases/Value Cases/Harmonization Requests	16
3.4	Requirements Outside the Current Scope	16
3.4.1	Gaps and Resolution Recommendations Specific to Security and Privacy Constructs.....	18
4.0	SECURITY AND PRIVACY CONSTRUCTS	20
4.1	HITSP Security and Privacy Construct Overview.....	20
4.2	Relationship Between Security and Privacy Principles and Constructs.....	20
4.3	Relationship Between NIST SP800-95 Web Services Attacks and Constructs.....	22
4.4	Overview of Construct Characteristics	23
4.5	Conceptual Relationship Between Constructs	30
4.5.1	Management of Consent Directives and Access Control.....	30
4.5.2	Nonrepudiation of Origin, and Document Integrity	31
4.5.3	Emergency Access.....	31
4.6	Description of Security and Privacy Constructs	32
4.6.1	HITSP/T17 Secured Communication Channel.....	32
4.6.2	HITSP/T15 Collect and Communicate Security Audit Trail	33
4.6.3	HITSP/SC109 Security Audit.....	33
4.6.4	HITSP/TP20 Access Control	34
4.6.5	HITSP/SC108 Access Control.....	34
4.6.6	HITSP/TP13 – Manage Sharing of Documents (with Document Integrity Option).....	35
4.6.7	HITSP/C19 - Entity Identity Assertion	35
4.6.8	HITSP/C26 - Nonrepudiation of Origin	36
4.6.9	HITSP/T16 - Consistent Time	37
4.6.10	HITSP/TP30 - Manage Consent Directives.....	37
4.6.11	HITSP/CAP143 - Manage Consumer Preference and Consents.....	38
4.6.12	HITSP/C25/C87/C88/C164/C165 – Anonymize	39
4.6.13	HITSP/T24 – Pseudonymize	39
4.6.14	HITSP/C44 - Secure Web Connection	40



5.0	SECURITY AND PRIVACY MANAGEMENT BACKGROUND	41
5.1	Privacy Background.....	41
5.2	Risk Management.....	43
5.2.1	Defining and Managing Risk	43
5.2.2	Developing a Risk Management Framework	44
5.3	Risk Assessment	44
5.3.1	Organizational (Strategic) vs. System (Tactical) Risk Assessments	44
5.4	Security Management.....	45
6.0	GLOSSARY	46
7.0	APPENDIX	47
7.1	Information Policy Management.....	47
8.0	CHANGE HISTORY	51
8.1	October 5, 2007	51
8.2	October 15, 2007	51
8.3	August 20, 2008	51
8.4	August 27, 2008	51
8.5	June 30, 2009.....	51
8.6	July 8, 2009	52
8.7	January 18, 2010.....	52
8.8	January 25, 2010.....	52



FIGURES AND TABLES

Figure 4-1 Dynamic Security and Privacy Constructs	31
Figure 7-1 Policy Concepts	48
Table 1-1 HITSP Reference Documents	8
Table 2-1 Guidance Standards	12
Table 3-1 HITSP Security and Privacy Constructs	15
Table 3-2 Out-of-Scope Requirements Assessment	17
Table 3-3 Construct Standards Gaps	18
Table 4-1 Relationship of Privacy Principles and HITSP Security and Privacy Constructs.....	21
Table 4-2 Relationship of Security Principles and HITSP Security and Privacy Constructs.....	21
Table 4-3 Relationship of Web Services Attacks and HITSP Security and Privacy Constructs.....	22
Table 4-4 Security and Privacy Construct Summary	23
Table 4-5 Reference Documents	30



1.0 INTRODUCTION

As an introduction to the Healthcare Information Technology Standards Panel (HITSP) Security and Privacy Technical Note, this section provides a high level overview of this specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Security and Privacy Scope.

1.1 OVERVIEW

The HITSP Security and Privacy Technical Note provides the context for use of the HITSP Security and Privacy constructs, based on the initial American Health Information Community (AHIC) Use Cases. It includes a design map of existing standards and specifications that will be used to meet the stated requirements of the Use Cases. It references the Requirements, Design and Standards Selection document which describes the process by which the Use Cases were analyzed, candidate standards were identified and the design developed. As additional Use Cases are provided to HITSP, the HITSP team will update this document based on any new Security and Privacy requirements. This document will also be updated to reflect changes to the design and relationships of the constructs.

1.1.1 HITSP SECURITY AND PRIVACY POLICY

The HITSP Security, Privacy & Infrastructure Domain Technical Committee (SPIDTC) designed the constructs described in this Technical Note to support a wide variety of security and privacy policies and technical frameworks. Consistent with the HITSP Technical Committee Terms of Reference, HITSP has not attempted to resolve privacy or security policy issues, risk management, healthcare application functionality, operating systems functionality, physical control specifications, or other low-level specifications. This approach is crucial because of the variety of requirements that the HITSP Security and Privacy constructs will be called on to address.

As discussed in Section 2.0, many federal and state laws and/or regulations define the security and privacy policy requirements for individually identifiable health information. In developing the constructs described in this document, core concepts from several of these federal and state laws and regulations were considered, although a comprehensive, exhaustive review of all existing security and privacy laws and regulations was not done. Those laws/or regulations and organizational policies stipulate the administrative, physical, and technical mechanisms needed to enforce jurisdictional and organizational health privacy policies. The constructs presented herein constitute a technical foundation that is applicable to the various policy options defined by these federal and state laws, or by other business and organizational requirements.

While there is no single Security and Privacy framework universally accepted in the U.S. or internationally, HITSP identified, discussed, and considered a number of Security and Privacy frameworks emerging in the U.S. and in other countries. In particular, policies from Canada, the European Union, Australia, and global policies such as the ones developed by the Organization for Economic Cooperation and Development (OECD) were reviewed. Work is underway through HITSP and other groups to develop material relevant to a common reference framework for both Security and Privacy, which includes the HITSP Security and Privacy matrices (see www.HITSP.org). Subsequently, "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information"¹ was published by HHS in December 2008.

¹ The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (PDF)
http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf



HITSP identified a group of existing and emerging standards that may be used in guiding the implementation of the constructs (see Table 2-1 Guidance Standards).

In the context of electronic health information exchange, the management of privacy policies must transition from a strictly administrative paper-based function to the enablement of the technical functions needed for electronic management of privacy. As the expression of privacy policies mature from paper-based formats to unstructured electronic formats, and to structured and computable formats that are interoperable, security mechanisms to enforce these policies will increasingly need to align with structured electronic formats for security and privacy rules.

1.1.2 HITSP SECURITY AND PRIVACY MANAGEMENT OVERVIEW

In defining the Security and Privacy constructs described in this document, HITSP used a set of core concepts regarding privacy of health information that were derived from overarching federal, state and international laws and regulations (see Section 5.15.1). The SPIDTC also recognized that to manage security and privacy, healthcare organizations and technology vendors perform security, privacy, and business risk assessments (see Section 5.0). As technology grows more complex, a risk management framework that consists of risk management and prioritization tools is needed to facilitate problem analysis and prioritization work throughout the risk management assessment lifecycle. However, HITSP does not specify methodologies or risk management frameworks for conducting strategic or system-focused risk assessments, but encourages organizations implementing HITSP Interoperability Specifications to conduct both types of analysis. In addition, HITSP recognizes that a complete security program includes tasks to provide ongoing management and assurance that security objectives are being met, but such tasks are typically implementation-specific and therefore out of scope for HITSP Security and Privacy constructs.

1.2 SECURITY AND PRIVACY RELATIONSHIP TO USE CASES

Security and Privacy Constructs have evolved and will continue to evolve as new Use Cases, Value Cases, or other Harmonization Requests are received by HITSP. The Harmonization Framework describes the hierarchy of HITSP Constructs, including Service Collaborations. Some Service Collaborations have a clear Security and Privacy focus, whereas others are focused on infrastructure, but include the appropriate underlying Security and Privacy considerations in the context of the healthcare workflow. The current set of Security and Privacy related Service Collaborations are discussed later in this document, and should be used in the context of the Interoperability Specification calling for it, as per any other HITSP construct. It should be noted however, that the Service Collaborations are designed with the intent of maximizing reuse in anticipation of future Harmonization Requests.

1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2010 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.

1.4 TERMINOLOGY

Throughout the HITSP SPIDTC documents, the term Individually Identifiable Health Information (IIHI) is used to depict health information considered to be identifiable to an individual. In this context, IIHI extends beyond the more focused and limited HIPAA term "Protected Health Information" (PHI), which is applicable to entities covered by HIPAA. The overall intent of HITSP is for standards to be applied to all health information and all entities that collect, access, maintain, use or disclose individually identifiable health information. The term "Personal Health Information" had the same meaning as IIHI.



1.5 HITSP REFERENCES

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 the www.hitsp.org Web Site.

Table 1-1 HITSP 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



2.0 SECURITY AND PRIVACY SCOPE

HITSP designed the constructs described in this Technical Note to support a wide variety of security and privacy policies and technical frameworks. Consistent with the HITSP Technical Committee Terms of Reference, HITSP has not attempted to resolve privacy or security policy issues, risk management, healthcare application functionality, operating systems functionality, physical control specifications, or other low-level specifications. This approach is crucial because of the variety of requirements that the HITSP Security and Privacy constructs will be called on to address.

The United States has an extensive body of federal and state laws and regulations that define the security and privacy requirements for collecting, creating, maintaining, using, disclosing and disposing individually identifiable health information. Among them, at the federal level are:

- American Recovery and Reinvestment Act (ARRA) of 2009, including Health Information Technology for Economic and Clinical Health (HITECH)
- HIPAA Privacy Regulations (45 CFR § 160 and 164 Part E)
- HIPAA Security Regulations (45 CFR § 160 and 164 Part C)
- Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR Part 2)
- Family Education Rights and Privacy Act (FERPA)
- Privacy Act of 1974
- [Right to Financial Privacy Act \(1978\)](#)
- [Privacy Protection Act of 1980](#)
- [Electronic Communications Privacy Act \(1986\)](#)
- [Communications Assistance for Law Enforcement Act of 1994](#)
- [Telecommunications Act of 1996](#)
- [Financial Modernization Act \(Gramm-Leach-Bliley Act\) \(2000\)](#)
- Emergency Supplemental Appropriations Act for Defense, the Global War on Terror and Tsunami Relief (Real ID Act) (2005)

At the state level, numerous state health information laws and regulations exist with different degrees of detail and granularity, some more stringent (thus, not preempted) by the overarching HIPAA Security and Privacy regulations.

These laws and regulations generally apply to the:

- Holder of the data
- User (requester) of the data
- Data itself
- Purpose of the use or disclosure of the data
- Timing of the use and disclosure of the data
- Methods and mechanisms used to collect, maintain, use and disclose data

Several of them also define and assign specific rights to consumers with respect to controls consumers can exercise over the collection, access, use and disclosure of their health information.

2.1 SECURITY AND PRIVACY PRINCIPLES

In developing the HITSP Security and Privacy constructs, HITSP considered a set of overarching principles and concepts, derived from an analysis of major federal and common state laws and regulations. They included:



Privacy Principles

- Consumer consent requirements (including the concepts of consent and authorization, whether they are considered one and the same in some regulations, or treated differently in others)
 - Consumer's ability to provide directives on:
 - The collection, access, use and disclosure of his/her health information
 - What information is collected, accessed, used, disclosed
 - By whom
 - To whom
 - For what purpose(s)
 - When
 - For how long
 - Consumer's ability to modify or revoke directives
- Patient privacy rights, such as those identified in the HIPAA Privacy regulations, including the right to:
 - Receive a Notice of Privacy Practices
 - Access individually identifiable health information for review and/or copy
 - Request amendments to health information
 - Request privacy protections to health information including the right to request restrictions on the use and disclosure of health information and the right to request confidential communications from a covered entity
 - Request an accounting of certain disclosures that a covered entity has made of their protected health information (within the context of HIPAA)
 - File a complaint about privacy issues
- Privacy requirements:
 - Various degrees of sensitive health information
 - Minimum necessary
 - Accounting of disclosure
 - Procedures for ensuring confidential communications are being done (i.e., sending an electronic message with results to the patient at an alternative location)
 - Deidentification (anonymization) of information, when necessary
 - Verification requirements of the identity and authority of individual requesting health information prior to disclosure (if not known by the entity disclosing the information), including documentation of such identify and authority
 - Mitigation of harm, in the event of a use or disclosure done in violation of privacy requirements or organization's own policies and procedures

Security Principles

- Availability of health information – information is available when and where needed
- Confidentiality – information is not accessed, used, disclosed by non-authorized individuals or entities
- Integrity - Information content not alterable except under authorized circumstances
- Accountability – ensuring that those collecting, accessing, using or disclosing health information are accountable for their roles and responsibilities
- Identification – of users and subjects of health information, as appropriate and applicable
- Authentication – of users and subjects of health information, as appropriate and applicable
- Authorization – of those identified and authenticated, to allow them to perform the functions they are specifically authorized to perform with the health information they are collecting, accessing, using or disclosing
- Access Control - only authorized persons can access health information for authorized purposes



- Attribution/nonrepudiation - actions taken are reliably traceable
- Auditability – controls to identify, record and report and monitor health information events
- Secure communication – between entities exchanging health information
- Time recording – methods to control time of events in a consistent manner

Through an iterative process, these overarching concepts were identified and further refined in conjunction with the review of the first set of AHIC Use Cases. Further refinement of the existing constructs will continue, and new potential constructs will be identified and defined in the future, as new Use Cases are presented to HITSP.

2.2 POLICY GROUPS

Consistent with the HITSP Technical Committee Terms of Reference, the work of the Committee does not define or attempt to resolve security and privacy policy issues, risk management, healthcare application functionality, operating systems functionality, physical control specifications, or other low-level specifications. The HITSP Security and Privacy constructs were designed to support a wide range of federal, state, local, and institutional policies.

Work is being done elsewhere, and through other national and regional efforts to identify, define and address security and privacy related policy issues. These efforts include:

- The Health Information Technology Policy Committee
 - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1269&parentname=CommunityPage&parentid=2&mode=2&in_hi_userid=10741&cached=true
- Health Information Technology Standards Committee
 - http://healthit.hhs.gov/portal/server.pt?open=512&objID=1271&parentname=CommunityPage&parentid=3&mode=2&in_hi_userid=10741&cached=true
- National eHealth Collaborative
 - <http://www.nationalehealth.org/>
- The American Health Information Community's Confidentiality (AHIC), Security and privacy Workgroup
 - <http://www.hhs.gov/healthit/community/background/>
- The Health Information Security and Privacy Collaborative (HISPC)
 - http://healthit.ahrq.gov/portal/server.pt?open=514&objID=5562&mode=2&holderDisplayURL=http://prodportalb.ahrq.gov:7087/publishedcontent/publish/communities/a_e/ahrq_funded_projects/rti_public_page/main.html
 - <http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0>
- Certification Commission for Healthcare Information Technology (CCHIT), utilizing security and privacy standards in developing certification criteria
 - <http://www.cchit.org>
- Office for Civil Rights (OCR), HIPAA Privacy
 - <http://www.hhs.gov/ocr/hipaa/>
- Agency for Healthcare Research and Quality (AHRQ), Health Information Technology Program
 - <http://healthit.ahrq.gov/>
- Centers for Disease Control and Prevention (CDC), Public Health Information Network (PHIN)
 - <http://www.cdc.gov/phinf/>
- Centers for Disease Control and Prevention (CDC), BioSense
 - <http://www.cdc.gov/biosense/>
- Health Resources and Services Administration (HRSA)
 - <http://www.hrsa.gov/healthit/>



- Substance Abuse and Mental Health Services Administration (SAMHSA)
 - <http://www.samhsa.gov>
- Indian Health Services (IHS)
 - <http://www.ihs.gov/CIO/EHR/>
- U.S. Department of Defense (DoD)
 - <http://www.defenselink.mil>
- U.S. Department of Veterans Affairs (VA)
 - <http://www.va.gov>
- NCVHS – National Committee on Vital and Health Statistics (NCVHS)
 - <http://www.ncvhs.hhs.gov>
- National Governors Association's State Alliance for e-Health (NGA)
 - <http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnextoid=5066b5bd2b991110VgnVCM1000001a01010aRCRD>

The variability in health information security and privacy federal and state laws and regulations, and business policies and practices across the country, poses significant challenges to the development of a common set of security and privacy constructs. With this in mind, HITSP used an approach based on the identification of a core set of overarching policy concepts, and the establishment of a minimum common base set of requirements that could be applied to different health information exchange scenarios.

2.3 GUIDANCE STANDARDS

In looking at the various candidate standards for Security and Privacy Constructs, HITSP identified a group of standards that may be used in guiding the implementation of the constructs. These are listed in Table 2-1 below:

Table 2-1 Guidance Standards

Standard	Reference
ISO 27799:Health informatics: Security management in health using ISO 17799	www.iso.org
ASTM E1869: Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records	www.astm.org
ASTM E1986: Standard Guide for Information Access Privileges to Health Information	www.astm.org
ASTM E2086: Standard Guide for Internet and Intranet Healthcare Security	www.astm.org
ASTM E2085: Standard Guide on Security Framework for Healthcare Information	www.astm.org
WS-I: Security Challenges, Threats and Countermeasures Version 1.0	www.wsi.org
ISO 15408: Common Criteria Toolkit	www.commoncriteriaportal.org
ASTM E2595 PMI: Privilege Management Infrastructure	www.astm.org
ASTM E1985: Standard Guide for User Authentication and Authorization	www.astm.org
ASTM E1987: Standard Guide for Individual Rights Regarding Health Information	www.astm.org
NIST Special Publications (800 Series)	csrc.nist.gov
NIST Federal Information Processing Standards (FIPS) Publications	http://csrc.nist.gov/publications/PubsFIPS.html

2.4 RELATIONSHIP OF CONSTRUCTS TO SECURITY AND PRIVACY POLICIES

The Security and Privacy constructs include:

- Service Collaborations
- Transaction Packages
- Transactions
- Components



They describe the capabilities needed to support security and privacy policies. Specifically, security policies stipulate the administrative, physical, and technical mechanisms required to enforce jurisdictional and organizational health privacy policies.

In the context of electronic health information exchange, the management of privacy policies migrates from being strictly an administrative paper-based function (“out-of-band” capability) to enablement as technical functions (“in-band” capability). As the expression of privacy policies mature from paper-based formats to unstructured electronic formats, and finally to structured, interoperable and computable formats, our ability to enlist security mechanisms to enforce these policies will be proportional to our alignment of the structured electronic formats of security and privacy rules.

For example, a privacy policy may dictate that a consumer has the right to create and update a consent directive. The policy describes the directive as follows:

- A consumer as a security entity
- The consumer has rights assigned to a role (consenter)
- The consumer has permission to perform certain operations (create and update) on an object or resource (the consent directive)

In this case, the security policies of the entity controlling access to the consent directive resource can unambiguously enforce this privacy policy.

Another example is a policy for an emergency. The capability to alter access privileges to an appropriate level for failsafe/emergency access may include an override of a consumer’s consent directive, based on the security attributes of the entities involved.

2.5 FOCUS OF CONSTRUCT DEVELOPMENT ON INTEROPERABILITY

Consistent with the terms of reference of HITSP, the focus of its work is on the interoperability of health information exchanges. Requirements outside of HITSP scope are described in the next section. In order to achieve complete end-to-end Security and Privacy interoperability, HITSP acknowledges the need for the industry to have 1) harmonized security and privacy policies; 2) defined standards at the end-user level; and 3) point-to-point system interoperability. HITSP also acknowledges that a basic tenet of security and privacy protections is building and establishing trust, and that the following goals should be aimed when addressing security and privacy requirements:

- Assure that all health record instances are attributable to known and accountable entities (e.g., patients/consumers, providers, health plans)
- Assure that health records are only shared with known and trusted recipients, authenticated and authorized
- Assure that health record instance context is known and may be authenticated (validated) at any point in the health record lifecycle, including the subject of health record instance, the source/author(s) of health record instance, the entity/individual delivering the care to the patient, the action(s) performed/provided, the action date/time and duration, and the location where the actions took place
- Assure that health record instances have traceable continuity to their source
- Assure that health record instances are persistent, indelible and have traceable continuity to their source, ensuring nonrepudiation of record source/authorship
- Assure that when health record instances are amended, the original and all amended content are preserved
- Assure that if health record attributes are translated (code set to code set, language to language), original and translated content are preserved
- Assure that the accuracy of health record instances is known and may be validated, based on author attestation of accuracy and/or algorithmic measure



- Assure that the completeness of health record instances is known and may be validated, based on author attestation of completeness and/or algorithmic measure
- Assure that each health record instance lifecycle is preserved and traceable, including record origination, amendment, verification, access/use, translation, transmittal/disclosure, receipt, de-identification, aliasing, re-identification, archival, and others
- Assure trusted end-to-end flow and protection of health record instances, from point of record origination to each ultimate point of record access/use, potentially traversing multiple points of interchange
- Assure both forward (downstream) and backward (upstream) traceability of health record instances: source to each ultimate recipient bi-directionally

The Security and Privacy constructs developed by HITSP address the interoperability requirements of these goals in a manner that support varying types of policy decisions and end-user security and privacy conditions.



3.0 ROADMAP AND GAPS OF THE HITSP SECURITY AND PRIVACY CONSTRUCTS

HITSP is focused on standards harmonization – it is neither a product design organization, nor a network design organization. Clearly these other layers of design are important to the end result, but are outside the scope of what a HITSP Interoperability Specification addresses. Application design or network design may be relied upon to provide the basis of an Interoperability Specification. For example, there is no HITSP Interoperability Specification on the act of authenticating a user. User authentication is a functional requirement that is highly influenced by the local security-domain policy on acceptable authentication methods. The point where this becomes an interoperability problem is when two systems are communicating using a HITSP Interoperability Specification and the user identity must be conveyed. For this HITSP has provided a construct.

A roadmap with identified gaps is needed for a number of reasons. For example:

- There might be solutions available, but HITSP has not yet worked on a Use Case that needs that solution (prioritization)
- The problem might not be an interoperability problem (out of scope)
- The problem might not have standards developed yet (availability of the standard)
- Available standards are not applicable to the problem (applicability of the standard)
- The standards to solve the problem may have been determined inadequate (maturity of the standard)
- The standards to solve the problem might not have been implemented (maturity of the technology)

3.1 SELECTION OF SECURITY AND PRIVACY CONSTRUCTS

Based on the analysis of security and privacy requirements from the Use Cases provided to HITSP by AHIC, HITSP identified and developed the following set of constructs:

Table 3-1 HITSP Security and Privacy Constructs

Construct Name	HITSP Reference	Type of Construct	Definition
Access Control	HITSP/TP20	Transaction Package	To ensure that an entity can access protected resources if they are permitted to do so
Access Control	HITSP/SC108	Service Collaboration	Provides the mechanism for security authorizations which control the enforcement of security policies, including: role-based access control, entity based access control, context based access control, and the execution of consent directives
Anonymize	HITSP/C25	Component	To provide specific instructions for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery
Anonymize Public Health Case Reporting Data	HITSP/C87	Component	Provides the ability to anonymize patient identifiable information for Public Health Case Reporting. It provides specific instruction for anonymizing data that was created as part of routine clinical care delivery in preparation for repurposing the data
Anonymize Immunizations and Response Management Data	HITSP/C88	Component	Provides the ability to anonymize patient identifiable information for Immunization and Response Management. It provides specific instruction for anonymizing data that was created as part of routine clinical care delivery in preparation for repurposing the data
Collect and Communicate Security Audit Trail	HITSP/T15	Transaction	To define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis
Consistent Time	HITSP/T16	Transaction	To ensure that all the entity systems that are communicating within the network have synchronized system clocks



Construct Name	HITSP Reference	Type of Construct	Definition
Entity Identity Assertion	HITSP/C19	Component	To ensure that an entity is the person or application that claims the identity provided
Manage Consent Directives	HITSP/TP30	Transaction Package	To ensure that a consumer's consent directive relating to the collection, access, use, or disclosure of the consumer's IIHI are captured, managed and available to requesting actors, e.g., a Document Source deploying the consent directive in the course of collecting, publishing, and registering the IIHI
Manage Sharing of Documents	HITSP/TP13	Transaction Package	To ensure the integrity of a document that is exchanged or shared
Nonrepudiation of Origin	HITSP/C26	Component	To support Nonrepudiation of Origin provide proof of the integrity and origin of documents in a high-assurance manner
Pseudonymize	HITSP/T24	Transaction	To describe a framework for including pseudonymization services where the use of "dummy" or pseudo references to specific patients or providers is required
Secure Web Connection	HITSP/C44	Component	Provides the capability to access documents through a secure web browser
Secured Communication Channel	HITSP/T17	Transaction	To ensure the authenticity, the integrity, and the confidentiality of Transactions, and the mutual trust between communicating parties
Security Audit	HITSP/SC109	Service Collaboration	The mechanism to record security relevant events in support of policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed

An overview and detailed description of the Security and Privacy constructs, the relationships between the security and privacy principles and the constructs, as well as the conceptual relationships between the constructs, are provided in Section 4.0.

3.2 ROADMAP FOR SECURITY AND PRIVACY CONSTRUCTS

In the field of Security and Privacy, healthcare is not unlike many other industries and so a variety of standards is available. Other industries (e.g., automotive, commerce, banking, insurance, and manufacturing) have developed and deployed standards that solve requirements found in the Use Cases. The Web Services Interoperability profile (WS-I) uses the same methods specified for securing network communications. On the other hand, many requirements are not fully solved by available standards. This lack of standards may be because, for other industries, the specific problem has not been as important as other basic security problems. For example, there is a lack of standards to communicate the full access control policies and obligations in the fidelity that healthcare ultimately needs. In cases like this, HITSP will present the best solutions available, and encourage standards organizations to fill the gaps.

3.3 LIMITATIONS FROM USE CASES/VALUE CASES/HARMONIZATION REQUESTS

In addition to the maturity of standards or the implementation of the standards, other factors affected the identification and selection of the initial set of Security and Privacy constructs. Particularly, HITSP's scope was defined by Use Cases prioritized by the AHIC.

3.4 REQUIREMENTS OUTSIDE THE CURRENT SCOPE

The following table shows a set of requirements that have been discussed and the current assessment for these requirements. In many cases the requirements are driven by policy and therefore are outside the scope of HITSP.



Table 3-2 Out-of-Scope Requirements Assessment

Security/Privacy Concept	Disposition	Organization addressing issue	Reason for Disposition
Policy	Out of scope	HIE Policy	The ultimate policies that will guide the solution must be created and promulgated by the Health Information Exchange (HIE)
User Authentication	Out of scope	HIE Policy and Application	The method used to authenticate users is specific to the HIE policy and would be included as functional requirements on the applications
Document Encryption	Future requirement	N/A	Not required by the initial Use Cases (Anticipated requirement under ARRA)
Advanced Access Controls (e.g., Privacy Consents)	Future work	HL7, OASIS, ISO, etc.	<p>The standards are not yet available to support advanced privacy controls. The architecture presented by HITSP supports the insertion in the future of these advanced controls when available. Some standards efforts to monitor: HL7 CDA Confidentiality codes. There is a standard HL7 V.3 confidentiality code vocabulary that can be used to associate consent directive rules relating to privilege and access permission rights with document, message, record, and data element level metadata. We anticipate the development of an ontology based structured terminology that is able to convey any combination of consent directive rules at any level of artifact granularity and that will support run-time validation</p> <p>OASIS XACML provides for the expression of rules, and obligations which must be enforced as part of the access control decision. The OASIS XACML standard does not specify how to communicate or enforce the obligation. While XACML obligations start in the security system, enforcement may require communication to an application. The access control construct provides XACML as a way to encode obligations</p> <p>DRM (Digital rights management) has found acceptance in controlling content distribution and use in the music industry for managing intellectual property rights. DRM offers appeal for controlling consents since the consent is bound to the protected data and the consent policy can be changed even after the document has been given to a requester. Nevertheless, current approaches tend to be proprietary and have not yet found great penetration</p>
Delegation of Access	Out of scope	OASIS	AHIC Use Cases have not required delegation of access, including authorized third parties
Delegation of Consent Directives	Out of scope	N/A	The SPI TC is not making any policy decisions about whether a consent can delegate power of consent to a third party
Nonrepudiation of Receipt	Future requirement	OASIS, IHE	AHIC Use Cases have not required nonrepudiation of receipt. This control would provide the originator of a transaction with proof that the recipient did receive the transaction. This might be used in future Use Cases where transfer of control is critical
Digital Certificate Management	Future requirement		This is an area where there are strong standards, and for which the infrastructure necessary (a.k.a. PKI) is becoming more and more accessible to deploy and maintain. There is, however, limited penetration of PKI technologies in the United States, which in turn limits the specification of high assurance controls for electronic signature and nonrepudiation. Federal programs requiring PKI for all employees and contractors may lead the way but universal adoption appears to be still some time down the road. The support for PKI will come as Use Cases demonstrate how the value, portability and extensibility of this technology
Centralized Access Control Decisions	Future requirement	ISO, OASIS, HL7	ISO 22600 Privilege Management and Access Control Parts 1, 2 and 3 provide Access Control models. Generally the models are in place, however, the necessary maturity and profiling needed to translate foundational work into useable/implementable cross domain specifications has yet to be realized



Security/Privacy Concept	Disposition	Organization addressing issue	Reason for Disposition
Policy Bridging	Future requirement	ISO, OASIS	Until policy models and structured terminologies are standardized and semantically interoperable conveyance of policies is supported, policy bridging must be negotiated "out-of-band" by non-automated means. Once these standards are fully developed and widely adopted, automated policy bridging or "in-band" algorithmic negotiation will be possible
"In-band" Policy Management	Future requirement	ISO, OASIS, HL7	Currently, policy management is conducted "out-of-band". However, we anticipate the development of HL7 V.3 policy specifications that would support "in-band" policy messaging and negotiation We envision a maturity migration path that will enable HIE participants to share data despite being at various levels of maturity. One example is the use of specifications that support both "in-band" and "out-of-band" conveyance of privacy policies and consent directives, such as the HL7 V.3 Data Consent standard
Currency of Consent	Future requirement	HL7, IHE	What is lacking at this level of maturity is the ability to check the currency of the confidentiality codes upon use of the IIHI. This requires intermediation of HIE by a Consent Management Service that executes the applicable Consent Directive at the time of publication. This enables real time updating and revocation of a consumer's Consent to the extent that access to the IIHI is available only through publication by the Consent Manager

3.4.1 GAPS AND RESOLUTION RECOMMENDATIONS SPECIFIC TO SECURITY AND PRIVACY CONSTRUCTS

This section describes gaps in standards specific to the Security and Privacy Constructs. Recommended resolutions were developed through a series of steps including the Technical Committee's initial recommendations, cross team validation of the gap, provisional recommendations and peer review.

Table 3-3 Construct Standards Gaps

Construct	Identified Gaps	Recommended Resolution
HITSP/TP20 Access Control	Limited capabilities to communicate policy	OASIS is publishing three Cross Enterprise Security and Privacy Authorization (XSPA) profiles
HITSP/TP20 Access Control	NIST identified Levels of Assurance are not associated with a recognized vocabulary standard	Encourage SDOs to develop a standardized level of assurance vocabulary
Collect and Communicate Security Audit Trail	IETF has published the syslog-protocol to provide a more robust alternative to BSD syslog (RFC 3164). IHE is updating the ATNA profile accordingly	N/A
Secured Communications Channel	The TLS specification defines cipher suites that feature the SHA-1 hash algorithm, which is the hash used by the Document Integrity option to HITSP/TP13. Supplemental TLS specifications using stronger variants of the secure hash algorithm, specifically SHA-256 and SHA-384, are currently under development. The National Institute of Standards and Technology (NIST) plans to phase out SHA-1 in favor of the larger and stronger hash functions by 2010 for digital signature applications	Promote use of SHA-256 in future
Secured Communications Channel	The construct is constrained to not include Asynchronous point-to-point communication channels. In the current marketplace, there are secured networks connected to the end points needed for these current Use Cases that utilize Asynchronous communications. These are highly effective for high volume messaging networks where waiting for responses to a sent message can significantly delay network traffic. Suggest Asynchronous protocols be added to the roadmap for future consideration	Considered to be addressed in future releases



Construct	Identified Gaps	Recommended Resolution
Manage Consent Directives	There is a gap re: ease of use for changing a deployed consent directive; this currently requires the whole consent directive be revised and this action is usually done at the direction of the patient	Modification to XDS to make it easier to change a deployed consent directive. Gap still being researched
	Managing XDS Affinity Domains and multiple/ conflicting consents. Conflicts in policies may arise across XDS Affinity Domains (particularly in regional or a nationwide health information network environments), and within the same XDS Affinity Domain. There will be other mechanisms to resolve them, including human intervention (phone, other). An approach for detecting and resolving inconsistencies when capturing consent directives is provided in the Manage Consent Directive construct. While this approach is aligned with the one presented in HITSP/TP13, it has been identified as a gap area for further development	A provisional line in the interface interaction as optional communication back to consenter has been added, to allow for the identification of potential problems detected by the consenter
Manage Consent Directives	When a consumer updates/revokes a consent directive, the Consent Originator must find the subject IHI for updating the confidentiality codes previously applied. A mechanism for enabling IHI location by the Consent Originator is lacking	Although both IHI Documents and Consent Documents are managed using HITSP/TP13 'Technical Actors', they may be independently managed. This is why the Manage Consents Directives construct indicates that there are "Consent Repository" and "Consent Registry" actors to distinguish the type of interface. This will allow a policy where they are managed independently as well as a policy where they are the managed in the same location
	Enforcement of jurisdictional or organizational privacy policies needs a defined vocabulary and combinatorial grammar to define and apply policies	Although a gap exists, to the extent such a vocabulary is not available, within the current basic consent codes there can still be a system to provide enforcement via the jurisdictional/organizational privacy policies
	HL7 Permission Catalogue Updates	HL7 should analyze the AHIC Use Cases using the HL7 defined RBAC analysis methodology to uncover any potentially new HL7 permissions that need to be added to the HL7 permissions catalogue
	The Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Basic Patient Privacy Consents (BPPC) Content Profile (IHE-ITI-TF BPPC) standard supports only a pre-negotiated set of consent policies	This constraint is recognized as a gap. There is work ongoing in the standard development organizations (HL7, ISO, OASIS) to fill this gap. The construct will be adjusted as the standards fill the gaps
	Communication of Consent along with clinical data communicated by HITSP/T31 Document Reliable Interchange and HITSP/T33 Transfer of Documents on Media still requires use of registry repository	To define a way to include consent along with the clinical data



4.0 SECURITY AND PRIVACY CONSTRUCTS

4.1 HITSP SECURITY AND PRIVACY CONSTRUCT OVERVIEW

This section provides a high level description of the Security and Privacy constructs that are based on the security and privacy requirements extracted from the 2006 AHIC Use Cases - Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment. The remainder of this document discusses the HITSP constructs defined to meet those security and privacy requirements.

4.2 RELATIONSHIP BETWEEN SECURITY AND PRIVACY PRINCIPLES AND CONSTRUCTS

The following tables highlight the applicability of HITSP constructs to the various security and privacy principles described in previous sections. More specific discussion about the relationship between Security and Privacy constructs and principles is provided in each construct sub-sections below.



Table 4-1 Relationship of Privacy Principles and HITSP Security and Privacy Constructs²

Privacy Principles	Manage Sharing of Documents	Collect and Communicate Security Audit Trail	Consistent Time	Secured Comm. Channel	Entity ID Assertion	Access Control	Nonrepudiation of Origin	Manage Consent Directives	Anonymize	Pseudonymize
Consent Directives	✓	✓	✓	✓	✓	✓	✓	✓		
Review/Copy IIHI		✓	✓	✓	✓	✓				
Request to Amend IIHI	✓	✓	✓	✓	✓	✓				
Sensitive Health Information						✓				
Minimum Necessary						✓				
Account Disclosures		✓								
Confidentiality Communication with Patient				✓	✓					
Anonymization						✓			✓	✓
Verification of Identity					✓					
Mitigation of Harm				✓		✓				

Table 4-2 Relationship of Security Principles and HITSP Security and Privacy Constructs

Security Principles	Manage Sharing of Documents	Collect and Communicate Security Audit Trail	Consistent Time	Secured Comm. Channel	Entity ID Assertion	Access Control	Nonrepudiation of Origin	Manage Consent Directives	Anonymize	Pseudonymize
Availability	✓			✓	✓	✓		✓		
Confidentiality	✓			✓	✓	✓		✓	✓	✓
Integrity	✓	✓	✓	✓	✓	✓	✓			
Accountability		✓								

² There are interactions between two or more constructs that ensure the ability to meet security and privacy requirements. For example, in order to ensure entities are authenticate to assure that the entity is the person or application that claims the identity, HITSP/C19 Entity Identity Assertion and HITSP/C26 Nonrepudiation of Origin work together to support this requirement. Similarly, to guarantee or assure authenticity of data transmitted, these same two constructs, along with HITSP/TP13 Manage Sharing of Documents (with Document Integrity inserted as an option) work together to support this requirement.



Security Principles	Manage Sharing of Documents	Collect and Communicate Security Audit Trail	Consistent Time	Secured Comm. Channel	Entity ID Assertion	Access Control	Nonrepudiation of Origin	Manage Consent Directives	Anonymize	Pseudonymize
Identification					✓					
Authentication				✓	✓					
Authorization						✓				
Access Control						✓				
Nonrepudiation							✓			
Auditability		✓								
Secured Communications				✓						
Time Recording			✓							

4.3 RELATIONSHIP BETWEEN NIST SP800-95 WEB SERVICES ATTACKS AND CONSTRUCTS

Appendix A of the NIST SP800-95 lists several possible attacks on web services. HITSP Security and Privacy constructs help mitigate some of them, as show in the table below. Attacks in NIST SP800-95 that are not mitigated by HITSP constructs are not shown.

Table 4-3 Relationship of Web Services Attacks and HITSP Security and Privacy Constructs

NIST SP800-95 Category	Manage Sharing of Documents	Collect and Communicate Security Audit Trail	Consistent Time	Secured Comm. Channel	Entity ID Assertion	Access Control	Nonrepudiation of Origin	Manage Consent Directives	Anonymize	Pseudonymize
Reconnaissance Attacks				✓						
Registry Disclosure Attacks				✓						
Privilege Escalation Attacks				✓	✓	✓				
Attacks on Confidentiality	✓			✓	✓	✓		✓	✓	✓
Attacks on Integrity	✓	✓	✓	✓	✓	✓	✓			
Denial of Service Attacks		✓	✓	✓						
Command Injection		✓		✓		✓				



NIST SP800-95 Category	Manage Sharing of Documents	Collect and Communicate Security Audit Trail	Consistent Time	Secured Comm. Channel	Entity ID Assertion	Access Control	Nonrepudiation of Origin	Manage Consent Directives	Anonymize	Pseudonymize
Malicious Code Attacks		✓		✓		✓				

4.4 OVERVIEW OF CONSTRUCT CHARACTERISTICS

The HITSP Security and Privacy Constructs are the result of an assessment of the current practices for Security and Privacy standards implementation within the scope of the HITSP Interoperability Specifications. They are summarized in Table 4-4 Security and Privacy Construct Summary below.

Table 4-4 Security and Privacy Construct Summary

Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/T15-Collect and Communicate Security Audit Trail	To define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis	The transport protocol for audit record communication shall be BSD syslog, per the IHE ATNA specification, not RFC 3195 (This is due to the lack of commercially available implementations of RFC 3195) The "provisional format" for audit records defined in IHE ATNA shall not be used	Consistent Time construct is a pre-requisite for this Transaction Secure Nodes is a pre-condition to this Transaction A policy exists defining what is to be audited Audit record source is initialized to the audit policy Audit record repository is active and designated as the destination for recorded audit events Policy defining the protection of the log and audit exists and is being enforced Identities are managed	Audit record is created, communicated, stored, and analyzed Subsequent action initiated per policy, e.g., reports and other automated actions Audit record (Defined in ATNA section 3.20.7.1 of IHE-ITI-TF-2 V4.0) Security Audit Alarms (Defined in ISO 10164-7) Security Report (Defined in ASTM E2147)
HITSP/SC109-Security Audit	Describes the mechanism to record security relevant events and provides the mechanism to determine the record format to support analytical reports that are needed	Per underlying constructs	HITSP/T16 - Consistent Time is a pre-requisite HITSP/T15 - Collect and Communicate Security Audit Trail is a pre-requisite	Audit record is sent
HITSP/T16-Consistent Time	To ensure that all the entity systems that are communicating within the network have synchronized system clocks	Network communications	All pre-conditions associated with this Transaction are specified in Section 3.1 of ITI Technical Framework Version 5.0 Volume 2	Time appropriately synchronized between two or more technical actors All outputs associated with this Transaction are specified in Section 3.1 of ITI Technical Framework Version 5.0 Volume 2



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/T17-Secured Communication Channel	To ensure the authenticity, the integrity, and the confidentiality of Transactions, and the mutual trust between communicating parties	<p>Only communications requiring the attributes of transmission authenticity, confidentiality and integrity need utilize this construct for session-oriented, synchronous, point-to-point communication channels</p> <p>Those communications that require the attributes of authenticity, confidentiality and transmission integrity shall either be prohibited, or be designed and verified to prevent access to IIHI if they are not communicated through connections that provide session- oriented, synchronous, point-to-point communication channels</p>	<p>There is a mutually agreed to set of policies and procedures for establishment of mutually acceptable identity credentials</p> <p>Existence of active and network accessible nodes</p> <p>Consistent Time</p>	<p>A trusted association will be established between the two nodes</p> <p>This association will be used for all further secure Transactions between the IHE actors in two nodes.</p> <p>Require node to record an audit event to indicate attempted connections from nodes that are not mutually authenticated. (See Collect and Communicate Security Audit Trail Construct)</p>
HITSP/C19-Entity Identity Assertion	To ensure that an entity is the person or application that claims the identity provided	Construct is constrained to HITSP Transactions that require that a user identity is conveyed	<p>Entities must have been identified and provisioned (credentials issued, privileges assigned) in accordance with the Entity Identity Assertion construct</p> <p>Audit services are initialized as outlined in the Collect and Communicate Security Audit Trail Transaction</p> <p>Secure channels are initialized in accordance with Secured Communications Channel Transaction</p> <p>All actors are synchronized to a consistent time base by the Consistent Time Transaction</p>	<p>User has authenticated</p> <p>An error condition occurs. This can include errors in the verification step – malformed assertion; assertion from a distrusted identity provider; assertion from individual without enough information to perform verification; or identity provider is unknown</p> <p>User identity assertion is verified</p> <p>The results of the authentication are made available to the Authentication Provider</p> <p>A security audit event is generated (See Collect and Communicate Security Audit Trail Transaction)</p> <p>Authentication information that was verified is available (Standards for minimum core set of required data – use specific)</p>



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/TP20-Access Control	To ensure that an entity can access protected resources if they are permitted to do so	Entities must be members of defined information domains under the authorization control of a defined set of policies	<p>Entities must have been identified and provisioned (credentials issued, privileges granted, etc.) in accordance with Entity Identity Assertion construct</p> <p>Privacy policies are identified and provisioned (consents, user preferences, etc.) in accordance with policy</p> <p>Pre-existing security and privacy policies are provisioned to access control services</p> <p>The capabilities and location of requested information/document repository services are known</p> <p>Secure channels are established as required by policy in accordance with the Secured Communication Channel construct</p> <p>Audit services are initialized in accordance with the Collect and Communicate Security Audit Trail construct</p> <p>Entities have asserted membership in an information domain by successful and unique authentication consistent with the Entity Identity Assertion construct</p> <p>Requests for updates/append to data by patients have been received and approved</p>	<p>Access is authorized/denied</p> <p>Clean up state for credentials issued that are no longer required</p> <p>Fulfill any requirements and obligations on enterprise systems (e.g., audit)</p>
HITSP/SC108-Access Control	Provides the mechanism for security authorizations which control the enforcement of security policies	Uses HITSP/TP20- Access Control HITSP/TP30-Manage Consent Directives	<p>Uses HITSP/C17 Secure Communications Channel as a pre-condition (a secure communications channel shall exist)</p> <p>Uses HITSP/C19 Entity Identity Assertion as a pre-condition (entity identity assertions have been asserted)</p>	Per underlying constructs



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/TP30-Manage Consent Directives	To ensure that individually identifiable health information is only collected, accessed, used or disclosed with a consumer's consent	Constrained to support an IHE XDS document-centric architecture as described in HITSP/TP13 Manage Sharing of Documents	Consistent Time construct is a pre-requisite for this Transaction Secure Nodes is a precondition to this Transaction A policy defining what is to be audited exists Audit record source is initialized to the audit policy Audit record repository is active and designated as the destination for recorded audit events Policy defining the protection of the log and audit exists and is being enforced Identities are managed (by a HITSP construct, or through an out of band agreement, or local administration) Consenter must have an account with a Consent Originator (for Capture Consent Directive Transaction) All pre-conditions that are specified in the IHE BPPC specification	Consent Directive is captured/updated (Capture Consent Directives Transaction) Consent Directives are evaluated to obtain confidentiality codes which are subsequently associated with IHI as Metadata (Request Consent Directive Transaction) A record of new/updated consent directives is available (Capture Consent Directives Transaction) A security audit event is generated Consent Directive Location is provided (or denied) (Request Consent Directive Transaction) Consent Directive is provided (or denied) (Request Consent Directive Transaction)
HITSP/CAP143- Manage Consumer Preference and Consents	To enable the sending, receiving, and storage of consumer preferences and consents for use by EHR and HIE systems privacy policy enforcement	Uses HITSP/SC112 – Healthcare Document Management Service Collaboration, HITSP/TP30 – Manage Consent Directives, and s HITSP/C62 – Unstructured Document	As a precondition, this capability assumes legal and governance issues regarding data access authorizations, data ownership, and data use are in effect	Consumer preferences and consents are captured, stored, and provided to EHR and HIT systems



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/TP13-Manage Sharing of Documents	To ensure the integrity of a document that is exchanged or shared (when used with Document Integrity Option)	The Document Consumer interface must validate the SHA-1 hash	Secure Nodes is a pre-condition to this Transaction	<p>Document Integrity has been maintained</p> <p>The document consumer has validated the SHA-1 hash. Currently this is not a requirement of HITSP/TP13</p> <p>For SHA-1 hash validations which return a "no match", the document shall be considered invalid by the supporting application</p> <p>For SHA-1 hash validations which return a "match", the document shall be considered valid by the supporting application</p> <p>For failure to validate the hash value, the document shall be considered invalid by the supporting application</p> <p>Require application to record an audit event to indicate "no match" outcomes (See Collect and Communicate Security Audit Trail)</p>



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/C26-Nonrepudiation of Origin	To support nonrepudiation of origin	Persistent document contained in Electronic Health Records per HITSP/TP13-Manage Sharing of Documents Environment where Policies have defined the Public Key-management Infrastructure (PKI) from which digital signing certificates are obtained	Existence of policy requiring Nonrepudiation Existence of policy to guide the creation of digital certificates as proof of identity and authority Possession of digital certificate for signing Existence of a PKI identity management framework Policy-determined vocabulary for the intent or authority for use of a digital signature Consistent Time construct is a pre-requisite for this Transaction Secure Nodes is a pre-condition to this Transaction A policy defining what is to be audited exists Audit record source is initialized to the audit policy Audit record repository is active and designated as the destination for recorded audit events Policy defining the protection of the log and audit exists and is being enforced Identities are managed	Existence of digital signature for the subject document Verified identity and intent/authority of the signer (currently assigned to the construct that requires nonrepudiation) Digitally signed documents
HITSP/C87-Anonymize Public Health Case Reporting Data	Provides guidance for anonymization of data to be reported to public health and should be implemented with consideration of risk assessment results in the intended operating environment.	N/A	N/A	N/A
HITSP/C88-Anonymize Immunizations and Response Management Data	Provides guidance for anonymization of immunization data and should be implemented with consideration of risk assessment results in the intended operating environment.	N/A	N/A	N/A
HITSP/C25-Anonymize	Provides guidance for anonymization of Biosurveillance and Quality data and should be implemented with consideration of risk assessment results in the intended operating environment.	N/A	N/A	N/A



Construct	Description	Constraints	Pre-conditions	Post-conditions/ Required Outcomes
HITSP/T24-Pseudonymize	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	<p>Patient Identity Consumers may not receive real identifiers. They may receive only pseudo-identifiers, for patient records outside their own domain</p> <p>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 interface to a PIX interface in one of the following groupings:</p> <p>PDQ Patient Demographics Supplier with PIX Patient Identifier Cross-Reference Manager</p> <p>PDQ Patient Demographics Supplier with PIX Patient Identifier Cross-Reference Consumer</p> <p>PDQ Patient Demographics Consumer with PIX Patient Identifier Cross-Reference Consumer</p> <p>Implementation considerations for each of these groupings are discussed in IHE IT Infrastructure Technical Framework, Volume 3 [IHE ITI-TF-2 V4.0] Appendix M, "Using Patient Demographics Query in a Multi-Domain Environment"</p>	<p>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</p> <p>Patient Identifier Cross-Reference Manager will have established a relationship of trust with the Pseudonymization Services</p> <p>The Patient Identity Source will be known both to the Patient Identifier Cross-Reference (PIX) Manager and to the Pseudonymization Services</p>	An alternative identifier that permits a patient to be referenced by a key that suppresses his/her actual identification information is supplied
HITSP/C44-Secure Web Connection	Provides the capability to access documents through a Secure Web Browser	N/A	N/A	This construct should only be used in well-defined circumstances where the user doesn't possess a digital certificate for identification and is not expected to have one



4.5 CONCEPTUAL RELATIONSHIP BETWEEN CONSTRUCTS

The following table is provided to illustrate the conceptual relationship between the key Security and Privacy Capabilities which have been identified. The table groups the constructs to show the relationships and interdependencies between the constructs and their key functions. It shows that Collect and Communicate Security Audit Trail Transaction, and Consistent Time Transaction, Secured Communication Channel Transaction, Entity Identity Assertion Component, Access Control Transaction Package, and Manage Consent Directives Transaction Package are key functions that are necessary to support security and privacy. They are pre-requisite conditions of all the events that are supported.

Table 4-5 Reference Documents

Use	Construct
Core – always required	HITSP/T15-Collect and Communicate Security Audit Trail
	HITSP/T16-Consistent Time
	HITSP/T17-Secured Communications Channel
	HITSP/C19-Entity Identity Assertion
	HITSP/TP20-Access Control
	HITSP/TP30-Manage Consent Directives
Context Dependent – optional	HITSP/C26-Nonrepudiation of Origin
	HITSP/TP13-Manage Sharing of Documents
	HITSP/C25-Anonymize
	HITSP/C87-Anonymize Public Health Case Reporting Data
	HITSP/C88-Anonymize Immunizations and Response Management Data
	HITSP/T24-Pseudonymize

Refer to the construct specifications for the selected standards and corresponding implementation guidance.

4.5.1 MANAGEMENT OF CONSENT DIRECTIVES AND ACCESS CONTROL

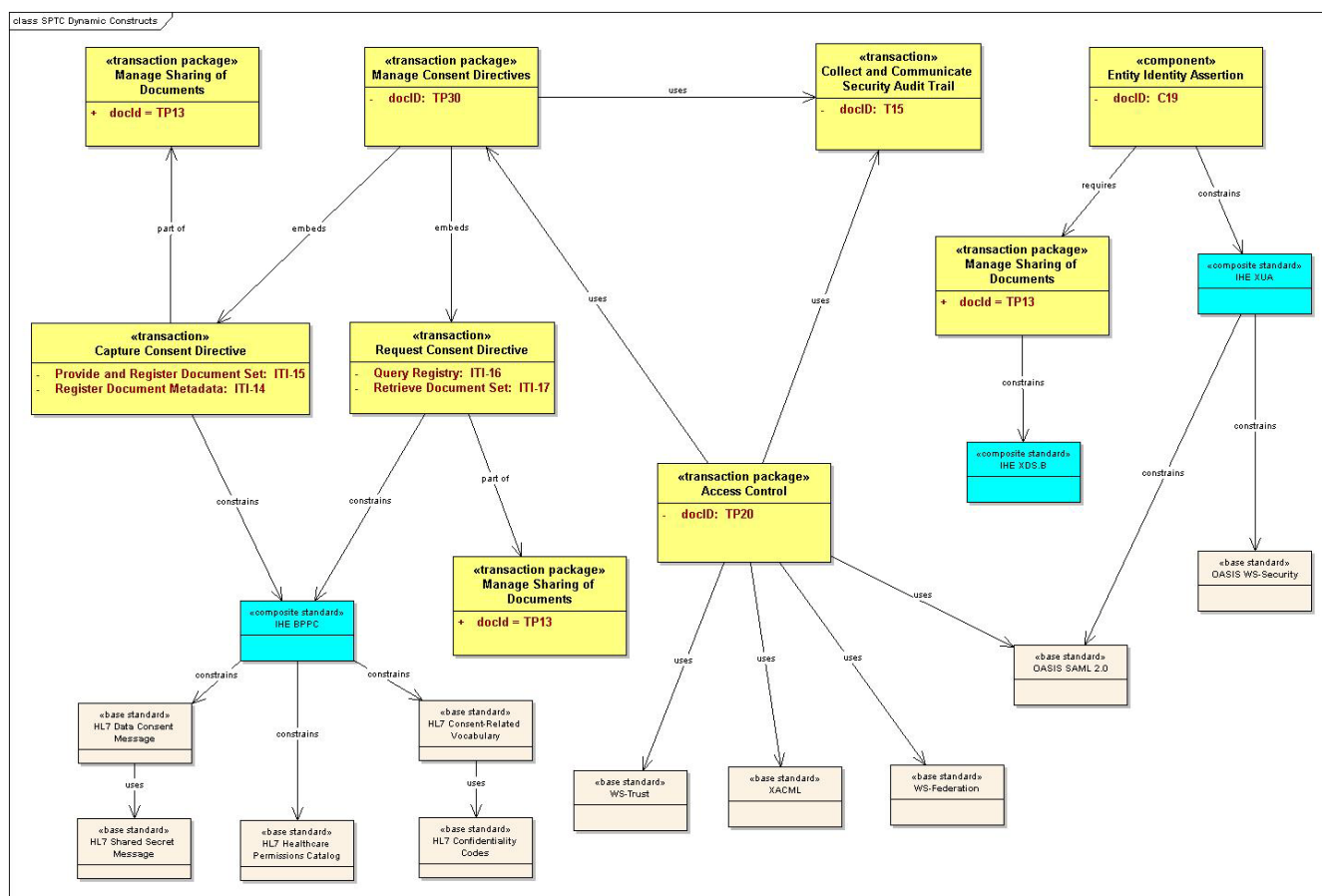
The HITSP/TP30 Manage Consent Directives construct is to be considered a precondition to HITSP/TP20 Access Control. HITSP/TP30 specifies patient specific policy decisions for object access control, versus organizational level access control.

Privacy policy provides access control information as a type of enforceable security policy that can be enforced by the Access Control Transaction Package. Accordingly, privacy policy management is conceptually no different from any other type of policy (from the security system point of view). Once the privacy policy is formulated, it needs to be provisioned and managed as part of the overall security policy.

Figure 4-1 below represents the relationship of the constructs for the use and disclosure of individually identifiable health information within the context of the AHIC Use Cases.



Figure 4-1 Dynamic Security and Privacy Constructs



4.5.2 NONREPUDIATION OF ORIGIN, AND DOCUMENT INTEGRITY

Local implementation policy as determined by risk assessment, including assessment of jurisdictional and regulatory requirements, will determine which assurance level of Nonrepudiation of origin is needed. For instance, in document-based transmissions, a low level is offered by the basic use of HITSP/TP13 Manage Sharing of Documents construct. A medium level of assurance is offered by use of the HITSP/TP13 construct option called "Document Integrity"; a higher level of assurance is offered by the use of the HITSP/C26 Nonrepudiation of Origin. HITSP/C26 requires the existence of a Public Key Infrastructure.

4.5.3 EMERGENCY ACCESS

The following is a description of an instance of a break-glass scenario which may be used in the absence of automated policy controls. Support for this scenario is not required, and is provided informatively.

In emergency or life-threatening conditions, strict security controls may interfere with the provision of needed healthcare services. For example, the user may be unable to use the health information system because of insufficient privilege. In such contexts, bypass or "emergency" access may be required.

In an emergency situation, immediate access to system information regarding the victim is paramount to the provision of care. While "Good Samaritan"³ laws ensure that medical care provided by even non-

³ Good Samaritan Act - To trigger the protection of such an act, two conditions must be satisfied: it must be a volunteer act, and the actions must be a good faith effort to help. In the medical sense, a Good Samaritan is a



medical personnel is a protected activity, this is not extended to include all access to health information systems.

Declaration of an “emergency” allows specific pre-authorized individuals to gain access to records containing protected health information when timely access is needed to prevent harm or risk to life. Emergency access includes situations for which a caregiver would not normally have need-to-know access to a record, or parts of a record or system functions covered by “least privilege” restrictions:

- Persons declaring an emergency must be properly authenticated; anonymous access to protected health information is not provided under this construct
- User authorizations and patient consents (to the extent required by policy or law) must be verified by the access control system
- Declaration of an emergency includes obligations that subject the user to additional monitoring and reporting (audit) of activities for later review

There are no established standards for emergency access. Specific policies that vary from one information domain to another may indicate implementation.

4.6 DESCRIPTION OF SECURITY AND PRIVACY CONSTRUCTS

The sections below provide the high level descriptions of the Security and Privacy Constructs. For detailed implementation details, refer to the Construct Specifications available from www.hitsp.org.

4.6.1 HITSP/T17 SECURED COMMUNICATION CHANNEL

The Secured Communication Channel Transaction provides the mechanisms to ensure the authenticity, integrity, and confidentiality of transactions, and the mutual trust between communicating parties. Its objectives include providing:

- Mutual node authentication to assure each node of the others’ identity
- Transmission integrity to guard against improper information modification or destruction while in transit
- Transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes

This Secured Communication Channel Transaction supports both application and machine credentials, and user machines (user nodes). A practical example of this Transaction is a secured communication channel between a Personal Health Record (PHR) system and an Electronic Health Record (EHR) system, or an EHR system to a laboratory.

4.6.1.1 CONSTRUCT REQUIREMENTS

The following are the requirements for this Transaction:

- Session used to transmit data has mutual authentication
- Data are transmitted with confidentiality and transmission integrity

4.6.1.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct includes Mutual Node Authentication, session transmission, confidentiality and transmission integrity, trusted path, and session authenticity. At the end of the Transaction, the following conditions or outputs are provided:

medical care professional who volunteers to help someone in need of emergency medical care. The act must be done without there being any duty to care for the patient and without any expectation of compensation.



- A Secured Communication Channel providing transmission confidentiality, integrity, and session authenticity is established between the two nodes. This Secured Communication Channel will be used for all future secure transactions between the two nodes
- Require node to record an audit event to indicate attempted connections from nodes that are not mutually authenticated

4.6.1.3 EXPECTED USE

The construct should be used in a scenario that requires establishment of a channel of communication between two nodes, entities, or systems.

4.6.2 HITSP/T15 COLLECT AND COMMUNICATE SECURITY AUDIT TRAIL

The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. The construct describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.

This Transaction is only relevant to security conformance, enforcement, and risk mitigation as a required element in the HIPAA Security Rule. It is distinct from a disclosure log, as defined by the HIPAA Privacy Rule. Audit record data may be applicable to help with the requirements for a disclosure log or transmittal to a PHR.

4.6.2.1 CONSTRUCT REQUIREMENTS

The following are the requirements derived from the AHIC Use Cases for this Transaction:

- Data to be audited are identified, collected, formatted and reported
- Automated responses (alerts, alarms or reports) are provided for audited data

4.6.2.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct includes time, auditable events, record content, monitoring analysis reporting (includes anomaly detection and analysis) and reduction, audit protection, alerts and alarms, and support for accounting of disclosures. At the end of the Transaction, the following conditions or outputs are provided:

- Audit record is created, communicated, stored, and analyzed
- Subsequent action initiated per policy (e.g., reports and other automated actions)
- Audit record
- Security audit alarms
- Security report

The construct should be used in any scenario that requires the generation of an auditing record.

4.6.3 HITSP/SC109 SECURITY AUDIT

The Security Audit Service Collaboration describes the mechanism to record security relevant events in support of policy, regulation, or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed. This Service Collaboration:

- Uses HITSP/T15 Collect and Communicate Security Audit Trail
- Uses HITSP/T16 Consistent Time



4.6.4 HITSP/TP20 ACCESS CONTROL

The Access Control Transaction Package is principally concerned with the three Components of: privacy policies, security policies and enforcement of the resulting merged set of policies that are used to determine if access to system resources and functions are to be authorized.

4.6.4.1 CONSTRUCT REQUIREMENTS

The following are the requirements derived from the AHIC Use Cases for this Transaction Package:

- Access Control is managed (created, modified, deleted, suspended, or restored, and provisioned based on defined rules and attributes)
- Data access policy is enforced
- Data access policy bypass is enforced (Emergency access)
- User data are located by an entity with the ability (privileges) to search across systems
- Protected data are accessed based on access control decisions information attributes for data access
- Protected data are modified, updated or corrected only by identified users and authorized users
- Select protected data are blocked from users otherwise authorized to access the information resource
- Requests for changes to protected data are made by users to providers/sources of data
- Obligations may be placed upon providing systems prior to granting data access. Obligations may also be placed upon users receiving data that must be honored as a condition or restriction on use
- Protected data – Any data or information of any type requiring the evaluation and enforcement of access control decisions prior to granting user access

4.6.4.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct includes:

- Audit events are recorded and alerts communicated
- Request is fulfilled
- Forward obligations on users and user Enterprise ACS

4.6.4.3 EXPECTED USE

This construct should be used in any scenario that requires access rights to be granted to a user in order to access IIHI, or any scenario that requires policy management.

4.6.5 HITSP/SC108 ACCESS CONTROL

The Access Control Service Collaboration provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR)). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents. This Service Collaboration:

- Uses HITSP/T17 and HITSP/C19 as pre-conditions
- Uses HITSP/TP20
- Uses HITSP/TP30



4.6.6 HITSP/TP13 – MANAGE SHARING OF DOCUMENTS (WITH DOCUMENT INTEGRITY OPTION)

Document Integrity provides the mechanism to ensure the integrity of a document that is exchanged or shared. An example of this is the ability to provide assurance that a document at rest is the same when it is retrieved as it was when it was stored. Document integrity does not include clinical integrity, accuracy or quality of the content, which are outside the scope of this Transaction.

The Document Integrity construct is implemented via an attribute in the metadata that is used by the IHE XDS Profile (Cross Enterprise Document Sharing). The specific implementation of XDS used by HITSP is described as a contextual constraint in HITSP/TP13 Manage Sharing of Documents. Currently, in the context of the existing Use Cases and Interoperability Specifications, document handling is always in the context of XDS, which therefore limits the scope to the document at rest. Documents in transit are covered by the Secured Communication Channel Transaction. The Secured Communication Channel Transaction also is implemented while protecting documents in transit.

4.6.6.1 CONSTRUCT REQUIREMENTS

The following are the requirements derived from the AHIC Use Cases for Document Integrity:

- Data needs to be checked for integrity of contents when it is transmitted from one entity to another (specifically applicable to the Biosurveillance and Electronic Health Records-Laboratory Results Reporting Use Cases)
- Data needs to be secured to ensure that it is not altered in violation of any existing policies (specifically applicable to the Biosurveillance and Electronic Health Records-Laboratory Results Reporting Use Cases)

4.6.6.2 CONSTRUCT FUNCTIONALITY

The key functionality supported is assurance that a document has not been altered while at rest, in violation of policy. The optional use of this contextual constraint in HITSP/TP13 provides the following conditions, outputs or assurances:

- Document integrity has been maintained
- The document consumer has validated the SHA-1 hash
- For SHA-1 hash validations which return a “no match”, the document shall be considered invalid by the supporting application
- For SHA-1 hash validations which return a “match”, the document shall be considered valid by the supporting application
- For failure to validate the hash value, the document shall be considered invalid by the supporting application
- Require an application to record an audit event to indicate “no match” outcomes

4.6.6.3 EXPECTED USE

The use of document integrity is expected whenever the use of documents requires that the integrity of the document be monitored and assured.

4.6.7 HITSP/C19 - ENTITY IDENTITY ASSERTION

The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a PHR system. The scope of this Component is meant to cover all scenarios in which HITSP Transactions cross enterprise boundaries, as well as transactions that may occur within an enterprise. For all HITSP Transactions, the assertion mechanism is the same whether the Use Case scenarios are within an enterprise or cross-enterprise. However, the scope of the Component



is limited to how to correctly authenticate the identity of the user for a HITSP Transaction to a service provider.

Note: The concept of “entity identity” in this construct identifies actors for access control purposes. This is not the same as “patient identity” that identifies patient's data.

4.6.7.1 CONSTRUCT REQUIREMENTS

The following is the requirement for this Component:

- Entities are authenticated to assure that the entity is the person or application that claims the identity

4.6.7.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct is the identification and authentication of entities accessing the protected resources. At the end of the Component, the following conditions or outputs are provided:

- Entity has authenticated
- An error condition occurs. This can include errors in the verification step – malformed assertion; assertion from a distrusted identity provider; assertion from individual without enough information to perform verification; or identity provider is unknown
- Entity identity assertion is verified
- The results of the authentication are made available to the Authentication Provider
- A security audit event is generated
- Authentication information that was verified is available

4.6.7.3 EXPECTED USE

The Entity Identity Assertion Component is used to satisfy the requirements defined above. In addition, the Entity Identity Assertion Component is meant to apply to the following scenarios as defined in the HITSP Interoperability Specifications for Biosurveillance, Electronic Health Records-Laboratory Results Reporting, and Consumer Sharing of Health Information via Networks:

- Entities are authenticated to assure that the entity is the person or application that claims the identity
- User using a Document Registry or Document Repository where the Service Provider wants a user identity for additional detail in their audit log – applicable to Biosurveillance
- User using a Document Registry or Document Repository where the Service Provider wants to be assured that the user has been authenticated to a specific assurance level – applicable to Biosurveillance and Electronic Health Records-Laboratory Results Reporting
- User using a Document Registry or Document Repository where the Service Provider wants to impose additional access controls – applicable to Electronic Health Records-Laboratory Results Reporting and Consumer Access to Health Information Networks
- User using a Document Registry or Document Repository is the patient. They are using an authorized PHR service which is handling the Document Consumer responsibilities. The Service Provider wants to restrict the information returned to those that have been released for patient consumption (for example a lab result that regulations require the provider to discuss in person before releasing the information) – applicable to Electronic Health Records-Laboratory Results Reporting and Consumer Access to Health Information Networks

4.6.8 HITSP/C26 - NONREPUDIATION OF ORIGIN

The Nonrepudiation of Origin Component provides the mechanisms to support nonrepudiation of origin, which refers to the proof of the integrity and origin of data both in an unforgeable relationship which can



be verified by any party. (ref. ASTM E2084). This Component does not provide Nonrepudiation of Receipt.

4.6.8.1 CONSTRUCT REQUIREMENTS

The following is the requirement for this Component:

- Authenticity of data transmitted is guaranteed or assured

4.6.8.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct is guaranteed or assured authenticity of the integrity and origin of data. At the end of the Component, the following conditions or outputs are provided:

- Existence of signed document
- Verified integrity of the document and its associated attributes
- Verified identity and intent/authority of the signer
- Nonrepudiated document

4.6.8.3 EXPECTED USE

The construct should be used in any scenario where a document is being transmitted between two technical actors and proof of origin (but not receipt) is required.

4.6.9 HITSP/T16 - CONSISTENT TIME

The Consistent Time Transaction provides a mechanism to ensure that all the entity systems that are communicating within the network have synchronized system clocks.

4.6.9.1 CONSTRUCT REQUIREMENTS

The following are the requirements for this Transaction:

- Clock synchronization source is determined
- EHR and PHR time clocks are synchronized to a predetermined source to ensure both are consistent

4.6.9.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct is the synchronization of clocks to a predetermined source. At the end of the Transaction, the following conditions or outputs are provided:

- Time appropriately synchronized between the two or more technical actors
- All outputs associated with this Transaction are specified in Section 3.1 of the IHE ITI Technical Framework

4.6.9.3 EXPECTED USE

The construct should be used in any scenario that is dependent on time synchronization in order to complete a transaction.

4.6.10 HITSP/TP30 - MANAGE CONSENT DIRECTIVES

The Manage Consent Directives Transaction Package provides a mechanism to ensure that individually identifiable health information is only collected, accessed used or disclosed in accordance with a consumer's consent.



4.6.10.1 CONSTRUCT REQUIREMENTS

The following are the requirements for this Transaction Package:

- Consent is captured and managed so that all Consent Directives specified in the consent are recognized and enforced

4.6.10.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct is the management of consent. At the end of the Transaction Package, the following conditions or outputs are provided:

- Consent Directives captured on paper and then scanned for electronic capture or entered electronically as structured or coded data
- Consent Directives are transformed into confidentiality codes and associated with IIHI as Metadata
- Consent Directives or their associated confidentiality codes are transformed into XACML Policies by a Security Access Control Service

The Manage Consent Directives Transaction Package utilizes the document content profile defined in the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Basic Patient Privacy Consents (BPPC) Content Profile (IHE-ITI-TF BPPC). The BPPC content allows for the capturing of the patient acknowledgement to simple privacy domain policy. This BPPC content is managed using the HITSP/TP13 construct. The BPPC content supports only a set of pre-negotiated consent policies. This constraint is recognized as a gap in an earlier section of this document.

4.6.10.3 EXPECTED USE

The construct should be used in any scenario that is dependent on the capture and management of a consumer's consent.

4.6.11 HITSP/CAP143 - MANAGE CONSUMER PREFERENCE AND CONSENTS

The Manage Consumer Preference And Consents Capability addresses management of consumer preferences and consents as an acknowledgement of a privacy policy. This Capability is used to capture a patient or consumer agreement to one or more privacy policies; where examples of a privacy policy may represent a consent, dissent, authorization for data use, authorization for organizational access, or authorization for a specific clinical trial. This Capability also supports the recording of changes to prior privacy policies, to reflect changes in consumer preferences, such as when a patient changes their level of participation or requests that data no-longer be made available because they have left the region. This Capability:

- Uses HITSP/SC112 – Healthcare Document Management
- Uses HITSP/TP30 – Manage Consent Directives
- Uses HITSP/C62 – Unstructured Document

4.6.11.1 CAPABILITY REQUIREMENTS

As a precondition, this Capability assumes legal and governance issues regarding data access authorizations, data ownership, and data use are in effect.

4.6.11.2 CAPABILITY FUNCTIONALITY

This Capability enables the sending, receiving, and storage of consumer preferences and consents for use by EHR and HIE systems privacy policy enforcement.



4.6.11.3 EXPECTED USE

The Capability should be used in any scenario that depends on the acquisition, maintenance, and provision of consumer preferences and consents as an element of privacy policy enforcement.

4.6.12 HITSP/C25/C87/C88/C164/C165 – ANONYMIZE

The HITSP Anonymization Component constructs provide guidance for anonymization and should be implemented with consideration of risk assessment results in the intended operating environment. 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. At time of this publication, there are 5 Anonymize constructs currently developed by HITSP:

1. HITSP/C25 - Anonymize Biosurveillance and Quality Data
2. HITSP/C87 - Anonymize Public Health Case Reporting Data
3. HITSP/C88 - Anonymize Immunizations and Response Management Data
4. HITSP/C164 - Anonymize Long Term Care
5. HITSP/C165 - Anonymize Long Term and Post Acute Care Assessment Data

Each provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. Each construct is intended specifically for the context for which they are defined, and should not be reused for any other purpose.

Note: The concept of “patient identity” in this construct is data that identifies patient’s data. This is not the same as “entity identity” that identifies actors in access control constructs.

4.6.12.1 CONSTRUCT REQUIREMENTS

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.

4.6.12.2 CONSTRUCT FUNCTIONALITY

The key functionality supported by this construct is the removal and aggregation requirements for data variables submitted to a Public Health Information System.

4.6.12.3 EXPECTED USE

The construct should be used in any scenario where it is necessary to anonymize patient identifiable information.

4.6.13 HITSP/T24 – PSEUDONYMIZE

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 construct is currently limited to patient-centric transactions where the primary subject of the pseudonymization request is a patient.

Note: The concept of “patient identity” in this construct is data that identifies patient’s data. This is not the same as “entity identity” that identifies actors in access control constructs.

4.6.13.1 CONSTRUCT REQUIREMENTS

The following is the requirement for this Component:

- The purpose of this Transaction is to describe a framework for including Pseudonym Service in Use Cases that require the use of “dummy” or pseudo references to specific patients.



- Pseudo-identifiers are intended to allow accessibility to longitudinal clinical information, while safeguarding any information that may compromise the privacy of the individual patient.

4.6.13.2 CONSTRUCT FUNCTIONALITY

The construct is 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.

4.6.13.3 EXPECTED USE

The construct should be used in any scenario where it is necessary to have an alternative identifier, which permits a patient to be referred to by a key that suppresses his/her actual identification information.

4.6.14 HITSP/C44 - SECURE WEB CONNECTION

This Component provides the capability to access documents through a secure web browser.

4.6.14.1 CONSTRUCT REQUIREMENTS

The context for the HITSP Secure Web Connection Component is the premise that a system needs to establish a secure communication session with another system across a potentially insecure network. Before exchanging any messages, the sending system must verify the identity of the other system, and the two systems must agree on cryptographic protocols to both initiate the session and to encrypt data during the session to prevent eavesdropping, and to exchange information in a manner that prevents tampering and message forgery.

4.6.14.2 CONSTRUCT FUNCTIONALITY

Hypertext Transfer Protocol Secure (HTTPS) is a Uniform Resource Identifier (URI) scheme which is syntactically identical to the http: scheme normally used for accessing resources using Hypertext Transfer Protocol (HTTP). Using an https: Uniform Resource Locator (URL) indicates that HTTP is to be used, but with a different default port and an additional encryption/authentication layer between HTTP and the Transmission Control Protocol (TCP).

4.6.14.3 EXPECTED USE

The construct should only be used in well-defined circumstances where the user doesn't possess a digital certificate for identification and is not expected to have one.



5.0 SECURITY AND PRIVACY MANAGEMENT BACKGROUND

In defining the Security and Privacy constructs described in this document, HITSP used a set of core concepts regarding privacy of health information that were derived from overarching federal, state and international laws and regulations. The HITSP Security and Privacy, Infrastructure Domain Technical Committee also recognized that to manage security and privacy, healthcare organizations and technology vendors perform security, privacy, and business risk assessments. As technology grows more complex, a risk management framework that consists of risk management and prioritization tools is needed to facilitate problem analysis and prioritization work throughout the risk management assessment lifecycle. However, HITSP does not specify specific methodologies or risk management frameworks for conducting strategic or system focused risk assessments, but encourages organizations implementing HITSP Interoperability Specifications to conduct both types of analysis. Further information on the development of security and privacy protections is provided in HITSP/TP20 Access Control.

5.1 PRIVACY BACKGROUND

As noted in previous sections, HITSP used a set of core concepts regarding privacy of health information that were derived from overarching federal, state and international laws and regulations. Key among them were guidelines on the protection of privacy and trans-border flows of personal data developed by the Organization for Economic Cooperation and Development (OECD) to harmonize national privacy laws within and across their member countries. The OECD guidelines have served as a basis for data protection laws in the United States, European, Canada, Japan, Australia, and elsewhere.

As a point of reference, the eight OECD privacy principles are listed next with concordance requirement descriptions from the European Union Directive on Data Protection (“EU Directive”) and the Health Insurance Portability and Accountability Act (“HIPAA”) in the United States. Together, these principles and laws provide a useful framework for developing general data protection requirements for health information systems.

Collection Limitation – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the individual. Article 10 of the EU Directive similarly requires the data collector to advise the individual of the data collector’s identity, the purposes for which the data are intended, and any information such as the recipients of the data. In the United States, the HIPAA Privacy Rule requires healthcare entities covered under HIPAA (“Covered Entities”) to notify individuals of their privacy practices upon enrollment and at least every three years thereafter so the individuals are aware of how any personal information they provide will be used and disclosed (45 C.F.R. §164.520).

Data Quality – Personal data should be relevant to the purposes for which they are collected and should be accurate, complete, and up-to-date. Articles 6(1)(c) of the EU Directive also require that personal data be kept accurate and, where necessary, kept up to date, and that inaccurate and incomplete data should be erased or rectified. The HIPAA Security Rule requires Covered Entities to implement policies and procedures to protect electronic protected health information (“EPHI”) from improper alteration or destruction (§164.312(c)(1)).

Purpose Specification - The purposes for which data are collected should be specified no later than the time of collection. Subsequent use of this personal data should be limited to those purposes or other purposed that are subsequently authorized. Article 6(1)(a) and (b) of the EU Directive require that personal data be collected only for specified, explicit, and legitimate purposes and not further processed in a way incompatible with these purposes. The HIPAA Privacy Rule provides that Covered Entities must obtain the individual’s written authorization for any use or disclosure of protected health information (PHI) that is not for treatment, payment or healthcare operations or otherwise permitted or required by the Privacy Rule (§164.508).



Use Limitation - Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified by the individual, except as subsequently permitted by the individual or by the authority of law. Article 7 of the EU Directive provides that data collectors may only process personal information with the individual's unambiguous consent, to perform a contractual or legal obligation, to protect the interests of the individual or the public, or are necessary for the legitimate interests of the data processor, but do not violate the rights of the individual. The HIPAA Privacy Rule specifically limits the circumstances under which Covered Entities in the United States may use and disclose protected health information (PHI) without written patient consent. It also requires these entities to make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request (§164.502(b)).

Security Safeguards - Personal data should be protected with reasonable security safeguards against such risk as loss or unauthorized access, destruction, use, modification, or disclosure of data. Article 17 of the EU Directive similarly requires data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. The HIPAA Security Rule outlines a number of required administrative, procedural, and technical safeguards necessary to protect electronic protected health information (EPHI) from any intentional or unintentional use or disclosure that is in violation of the Privacy Rule. Required technical safeguards include access controls, auditing, encryption and decryption, authentication procedures, transmission security, and audit controls.

Openness – There should be readily available means to establish the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller. Article 11 of the EU Directive requires data controllers, upon obtaining personal data about an individual from someone other than the individual, to notify the individual of the identity of the data controller, the purposes of the processing, and any further information such as the categories of data concerned, the intended recipients, and the existence of a right of access to and the right to rectify data concerning the individual. The HIPAA Privacy Rule obligates Covered Entities to provide individuals with notice of their privacy practices and any amendments thereto, describing the ways in which it may use and disclose personal information collected from the individual. The Covered Entity must make a good faith effort to obtain the individual's acknowledgment of this notification and subsequent amendments, before collecting, using, or disclosing the individual's personal information (§164.520).

Individual Participation – An individual should:

- (a) Be able to confirm whether the data collector has personal data relating to him or her;
- (b) Have the right to receive the data within a reasonable time and in an intelligible form; and
- (c) Have an opportunity to challenge the data and, if the challenge is successful, have the data erased, rectified, completed, or amended

Article 12 of the EU Directive entitles an individual to obtain from the data controller:

- (a) Confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and
- (b) The rectification, erasure, or blocking of data that is incomplete or inaccurate

The HIPAA Privacy Rule provides individuals with the right to access personal information contained in a designated record set and to request that the Covered Entity amend any information that is inaccurate or incomplete (§164.514(d)(2)).

Accountability - A data controller should be accountable for complying with measures that give effect to the foregoing principles. Articles 22 and 23 of the EU Directive require Member States to provide individuals with a judicial remedy for violations of national privacy laws and the right to obtain



compensation for damage suffered. In the United States, the HIPAA Privacy Rule requires Covered Entities to account for past disclosures of PHI upon the request of an individual (§164.528), while the Security Rule requires such entities to implement technical mechanisms to record and examine activity in information systems that contain or use EPHI (§164.312(b)).

5.2 RISK MANAGEMENT

Healthcare organizations and technology vendors are performing security risk assessments, privacy risk assessments, business risk assessments, etc. to ensure installed healthcare technology will have a positive impact on healthcare delivery. Some of these assessments are mandatory for healthcare delivery organizations under the HIPAA Security and Privacy Rules. However, key decision makers often have difficulty understanding the business or healthcare delivery relevance of the risks identified, discussions such as how much risk is acceptable, what types of risk may arise from new technologies, and how much to spend on mitigating risk. As a result, risk may not be properly considered when determining technology strategy and may not be continually assessed on an ongoing basis.

As healthcare technology grows more complex, the need for a unified approach to managing the risks inherent in new technologies grows with it. These risks include many different types of risks including: IT security, privacy, safety, corporate risks and human error factors. A holistic analysis is necessary to weigh the cost of preventative measures.

Risk management is about more than keeping hackers from stealing personal health information. It is critical to address such issues as:

- Protecting confidentiality of personal information
- Legal compliance
- Safe provision of healthcare services
- Patient safety
- Avoiding medical errors
- The cost and benefit of protective measures

Diligent healthcare organizations, as well as technology vendors, have been working since the inception of healthcare technology to assess their own risk levels, as best they can, by performing threat risk assessments, privacy impact assessments, business impact analyses, and security posture assessments, ad infinitum. Even when mandated by regulations, risk assessments are still often incomplete or their results and recommendations are not acted upon. Key decision makers may have difficulty understanding the relevance of the risks identified, which might subsequently be overlooked when determining technology strategy. As a result, discussions such as how much risk is acceptable, what types of risk may arise from new technologies, and how much to spend on mitigating risk are often overlooked or misunderstood. Furthermore, security, privacy or other technologies may be invested in as a result of popular demand rather than cohesive vision.

5.2.1 DEFINING AND MANAGING RISK

Risk is defined as the combination of the probability of an event and its consequences⁴. The majority of risks reported, mention negative impacts; however it is important to note that risk analysis can expose opportunities to reduce wait times, provide patients with access to their health data, and reduce medication conflicts through automated checks against a database. The risk level can be measured as a combination of the likelihood and impact of an anticipated event. While traditional healthcare risks have always necessitated management such as errors in prescribing, errors in treatment or patients falling or wandering off, new sources of risk associated with information technology have been introduced. These include IT security and privacy, safety and availability of information when needed, corporate

⁴ ISO/IEC Guide 73:2002 definition 3.1.1 Risk management – Vocabulary – Guidelines for use in standards.



management of technology systems, and even human factor risks such as fatigue and difficult to read application interfaces.

Risk Management is defined as the systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk⁵. It is a combination of all the processes involved in realizing existing as well as newly identified opportunities in a manner consistent with public interest, human safety and the law while managing adverse effects caused by the complexity of healthcare systems. It involves identifying, assessing and judging risks, assigning ownership, taking action to mitigate or anticipate them, and monitoring and reviewing progress. The outcome is a holistic analysis that weighs the cost of protective measures and establishes a continuous process to manage them.

Effective risk management enables senior management, middle management, and technical and operational staff to:

- Improve business performance by informing and improving decision making and planning
- Promote a more innovative, less risk adverse culture in which the taking of calculated risks in pursuit of opportunities is encouraged
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance
- Assist in meeting healthcare requirements and objectives
- Facilitate partnerships with other healthcare organizations to address the issues inherent in interoperable systems and data sharing
- Benefit patients who are often shared among unrelated healthcare providers both in terms of the handling of their information as well as improving the safety of healthcare services

5.2.2 DEVELOPING A RISK MANAGEMENT FRAMEWORK

A risk management framework consists of risk management and prioritization tools that facilitate problem analysis and prioritization work throughout the risk management assessment lifecycle.

As with all assessment exercises, once a risk management framework is agreed upon, the real work must begin. Healthcare IT exists in an environment which is constantly identifying new issues and risks on a continuous basis primarily in but not limited to the security domain. An ad-hoc approach to addressing these is dangerous and creates many new risks, such as technology conflicts, obsolescence, and inadequate focus on prioritizing solutions according to greatest value. A prime example of this phenomenon is leveraging biometric technology for uses which expose novel privacy risks, and which are inappropriate for the environment. Instead, there must be a corporate-wide commitment to applying the risk management framework on a continuous basis. This is the proven method of benefiting from risk management activities.

5.3 RISK ASSESSMENT

5.3.1 ORGANIZATIONAL (STRATEGIC) VS. SYSTEM (TACTICAL) RISK ASSESSMENTS

Organizational or Strategic risk assessments are usually tailored towards specific compliance requirements such as the HIPAA Security Rule (which is a requirement for Covered Entities), or against baseline framework standards such as ISO 17799. Well documented techniques and methodologies exist for conducting organizational risk assessments, which draw from relevant best practices and industry specific guidelines or requirements, such as the OCTAVE[®] Catalogue of Practices and Special Publications from NIST. The outcomes of organizational risk assessments usually include long-term organizational protection strategies in addition to critical-asset focused high level mitigation plans. Organizational risk assessments are therefore suitable for helping key decision makers define and roadmap long term security strategies, which may include the identification of requirements to adopt new

⁵ ISO 14971:2000, Application of Risk Management to Medical Devices definition 2.18.



technologies with a view to progressing along an overall security strategy. This approach helps organizations avoid investing in protective technology without truly understanding the impact on the overall security posture of the organization.

System-based risk assessments usually include detailed, in-depth analysis of all aspects of the information system under review, including relevant areas of the system development life cycle and appropriate security best practices for information systems. System specific risk assessments are often geared towards specific compliance requirements (e.g., Government System Certification and Accreditation) and are designed to help organizations understand the risks associated with implementation of a specific system or technology. Conducting an in-depth system based risk assessment will help organizations understand any additional risk they may inherit as a result of implementing the technology, and allow them the opportunity to implement configuration changes or additional mitigation measured to reduce the risk to an acceptable level prior to deployment.

HITSP does not recommend specific methodologies for conducting organizational or system focused risk assessments, but encourages organizations implementing HITSP Interoperability Specifications to conduct both types of analysis in order to:

- Understand the organizational impact and associated requirements in support of an overall risk management strategy
- Identify and reduce residual risk to an acceptable level when implementing specific technologies

5.4 SECURITY MANAGEMENT

As part of a complete security program, it is necessary to perform certain tasks to provide ongoing management and assurance that security objectives are being met. Security management is typically implementation-specific and therefore out of scope for the HITSP Security and Privacy Constructs.

The ISO 17799 and 27799 standards, used together, provide excellent guidance on establishing and running a comprehensive security management program for healthcare IT. This includes:

- Risk assessment and treatment
- Security policy
- Organization of information security – internal and external
- Asset management
- Human resource security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance – legal, policies, and audits

In addition, the ISO 15408 (Common Criteria) standard, part 3, provides a method to identify security assurance requirements for specific target environments. This includes:

- Evaluation of the criteria used to develop security requirements
- Evaluation of security targets
- Development
- Documentation
- Life-cycle support
- Testing
- Vulnerability assessments
- Composition/aggregation of components



6.0 GLOSSARY

The HITSP Glossary available from www.hitsp.org provides a glossary of Security and Privacy terms used within the Security and Privacy Technical Note and construct specifications.

RELEASED FOR IMPLEMENTATION



7.0 APPENDIX

7.1 INFORMATION POLICY MANAGEMENT

The ontology, illustrated below, begins at the most generic level of policy and proceeds to specify the components necessary for managing and controlling access to health information⁶.

- Information Policy Management is the means by which an information domain shares information internally or externally in accordance with policies to which one or more relevant domain authorities require compliance
- An information domain is a conceptual construct that consists of a set of information and entities with an interest in, or “right” to, the information
- Information policies dictate and protect those rights
- Security policies specifically safeguard the information (a valued resource) and enforce information rights
- Information rights policies institute the rights of entities to information, and dictate how those rights may be exercised

Figure 7-1 depicts the relationships between the privacy concepts.

⁶ This discussion follows the ISO 22600 Health Informatics – Privilege Management and Access Control and the current working draft of that standard.



The diagram illustrates the Consent Concepts model, showing the relationships between various policy and consent-related classes. The classes are organized into several groups:

- Policy Classes:**
 - InformationPolicy** (Base Class):
 - Security Policy
 - Privacy Policy
 - Information Rights Policy
 - Policy** (Base Class):
 - Identifiers: II [1..*]
 - Name: ST
 - Authority Name: ST
 - Domain ID: OID [1..*]
 - Domain Name: ST [1..*]
 - Organizational Security Policy** (Specialization of InformationPolicy):
 - Required by organization: 1..*
 - Jurisdictional Security Policy** (Specialization of InformationPolicy):
 - Named Jurisdiction: char
 - Organizational Privacy Policy** (Specialization of InformationPolicy):
 - Named Organization: char
 - Organization ID: OID
 - Privacy Rule 1
 - Privacy Rule 2
 - Privacy Rule 3
 - Jurisdictional Privacy Policy** (Specialization of InformationPolicy):
 - Named Jurisdiction: char
 - Authority ID: OID
 - Privacy Rule 1
 - Privacy Rule 2
- Consent Classes:**
 - Consent Directive Set**:
 - Identifier: set(II)
 - Address: set(URI)
 - Effective Time: INV<TS>
 - Consent Directive**:
 - Identifier: II
 - Effective Time: INV<TS>
 - Consent Author**:
 - Consent Author Type: code
 - Consent Author ID: II [1..*]
 - Consent Author Name: ST [0..*]
 - Policy Location**:
 - Identifier: II
 - Consent Directive Location: OID
 - Consent Directive Location Name: ST [0..*]
- Access Control and IIHI Classes:**
 - Access Control Policy**:
 - Enforce Obligation: void
 - Enforce Permitted Operation: void
 - Privilege Management Policy**:
 - Authenticate PHI User: void
 - Authorize PHI User: void
 - Confidentiality Policy Set**:
 - Confidentiality Policy
 - Confidentiality Policy**:
 - Identifier: II
 - Address: URI
 - Effective Time: INT<TS>
 - IIHI Principal**:
 - Identifier: II [1..*]
 - Name: ST
 - IIHI Access Permission**:
 - IIHI Access Permission: code
 - IIHI Resource**:
 - IIHI Type: code
 - Name: ST [0..*]
 - Identifier: II [1..*]
 - IIHI Access Constraint**:
 - Constraint Type: char
 - Identifier: II [1..*]
 - Name: ST [0..*]

The diagram shows various relationships between these classes, including inheritance, association, and specialization, with many labeled with 'enforces' or 'adheres to'.

Using a domain information rights policy, an entity with an ownership right, or control of information, may grant another entity the right to access that information for some specified use and under certain conditions. The right to access information is made through the issuance of a license. The license may stipulate:

- 

- The entities or roles that are authorized under the license
- The rights or operations that may be performed with the information
- The conditions for exercising the right, such as:
 - The purpose for which the information will be used
 - The medium, mechanism, or location by which the information may be accessed
 - The time interval during which, or frequency with which, a right may be exercised
- Any obligations that are required by the licensee, such as:
 - The payment for the license
 - Auditing of the exercise of the license
 - The assurance of compliance with the license
 - Limitations on the use of the information beyond those granted by the license

An entity may delegate the right to grant a license to another entity, such as a legal representative. The entity may then delegate the issuance of such licenses to a third party license issuer. The domain's information rights policy is enforced by a domain's information security policy, which controls access to permitted operations on the information by authorized entities, in accordance with the information rights policy.

Where the domain includes personal information, information rights policies will likely include compliance with jurisdictional and/or organizational *privacy* policies. Privacy policies are specialized information rights policies that enable the collection, access, use, and disclosure of information about the subject. The privacy policies are constrained by superseding interests, such as national security, or an entity who is the subject of the personal information.

A jurisdictional privacy policy may be comprised of a number of different policies such as non-conflicting jurisdictional privacy policies, cross-jurisdictional privacy policies, and HIPAA and other federal privacy laws. Examples are an EU member nation's privacy policy and the EU Privacy Policy, 42 CFR Part 2 for Substance Abuse Program information, Title 38 Section 7723 for Veterans' Administration, or 42 CFR 431.301 for the use of Medicaid Applicant and Recipient information.

A privacy policy that follows an "opt-in" model gives the entity, or their delegate, the right to explicitly grant a license for a specific use of their information to another principal. A privacy policy that follows an "opt-out" model gives the entity, or their delegate, the right to explicitly withhold a license to that information for a specific use.

An entity that is the subject of information may exercise privacy rights by granting or withholding consent, in accordance with overarching jurisdictional and organizational privacy policies. The entity would assert a specialized license in personal information or a "consent directive". An example is a consumer's privacy right to opt-out of personal information sharing financial information⁷.

With respect to individually identifiable health information, an entity's consent directive is an individually identifiable health privacy policy to control collection, access, use and disclosure of personal health information, constrained by the overarching jurisdictional and organizational privacy policies that are in effect, e.g., public health.

An entity who is a healthcare consumer may author multiple consent directives in accordance with multiple organizations, and within multiple jurisdictions. The consent directives may be recorded in

⁷ In November, 1999, President Clinton signed the Financial Services Modernization Act, more commonly known as Gramm-Leach-Bliley or GLB, after the Congressional sponsors of the Act. The main purpose was to overhaul the financial services industry. But privacy provisions were added to GLB near the conclusion of Congressional proceedings giving consumers new rights to notice and consent regarding the information-sharing practices of financial institutions. Title V of GLB gives consumers a right to opt-out, that is, to prevent sharing or other disclosures of personal information to third-party non-affiliates.



multiple consent repositories within a personal health record, and in multiple provider electronic health record systems. Together, these form the *consent directive set* for the healthcare consumer. The consent directives may be indexed by multiple consent directive registries, which may be stored within a healthcare consumer identity registry or as part of a health record index, and may be accessible by health information exchange record locator services.

Of note are the differences between information rights policies at the jurisdictional or organizational levels, and personal information rights policies that are asserted by entities. Jurisdictional and organizational information rights policies should, in theory, result in a consistent and somewhat stable overarching set of rules within some governance space (*rights governance level*). In contrast, personal information rights policies are by nature manifold, changeable, and likely inconsistent. The differences between the levels impact information exchange requirements. Both levels require capture, management, communications and negotiation, and should be enabled by automated and interoperable mechanisms. However, entities asserting rights need the ability to change multiple factors relating to their assertions easily and in real time, and to manage inconsistencies among assertions between different jurisdictions or organizations.

Interoperability within and among complex health information systems also requires the ability to convey and enforce jurisdictional, organizational, and personal privacy policies (consent directives) by binding these to applicable confidentiality policies. Confidentiality policies are additional specialized security policies that enforce jurisdictional, organizational, and personal privacy policies to meet non-privacy related information rights policies. The applicable security policies may be comprised of non-conflicting jurisdictional security policies between and across jurisdictions, and organizational security policies.

Any type of healthcare consumer consent directive that may be specified in accordance to an organization's privacy policy, may also have include one or more confidentiality policies necessary to enforce the consent directive.

The required confidentiality policies specify:

- The privilege management policies necessary to enforce consent directive authorizations
- The access control policies necessary to enforce the consent directive access permissions
- Any associated constraints on those permissions in the form of conditions on the permission or obligations on the privileged principal

Privilege management and access control are discussed further in the Manage Access Control Construct.

There exists an exhaustive set of confidentiality policies required to enforce the consumer's set of consent directives. When sharing the consumer's individually identifiable health information outside of an organization or jurisdiction, conflicting confidentiality policies may require policy bridging. This may be conducted via in-band and out-of-band negotiation mechanisms. For example, one jurisdiction or organization may refuse to share individually identifiable health information with another that has less restrictive protections, unless the receiving party agrees to enforce at least some of the sending party's confidentiality policy.

Until policy models and structured terminologies are standardized and the semantically interoperable conveyance of policies is supported, policy bridging must be negotiated out-of-band by non-automated means. Once standards are fully developed and widely adopted, automated policy bridging or in-band algorithmic negotiation will be possible.

As a final note on Security and privacy Policy Management, the capability to electronically enforce consent directive obligations on entities downstream from the initially authorized recipient entity is of particular interest for future work. Within U.S. healthcare, there is an expectation that HIPAA compliant covered parties will enforce certain obligations on downstream business associates via out-of-band contractual mechanisms. While the actual enforcement of out-of-band mechanisms is difficult to ascertain, the cost is higher when compared to in-band approaches that might be used.



8.0 CHANGE HISTORY

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

8.1 OCTOBER 5, 2007

The changes in this cycle address the following comments received during the Public Comment and Inspection Testing period (July 23, 2006 - August 17, 2007):

- 272, 517, 561, 562, 563, 566, 586, 587, 641, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 743, 887, 890, 899, 922, 984, 985, 1197, 1210, 1211, 1212, 1213, 1229, 1231, 1254, 1255, 1256, 1257, 1263

8.2 OCTOBER 15, 2007

Upon approval by the HITSP Panel on October 15, 2007, this document has been moved to Version 1.1. This document is now Released for Implementation.

8.3 AUGUST 20, 2008

Removed Glossary. The overall HITSP glossary, applying to all documents, will be used henceforth.

Minor editorial corrections.

8.4 AUGUST 27, 2008

Upon approval by the HITSP Panel on August 27, 2008, this document is now Released for Implementation.

8.5 JUNE 30, 2009

Editorial updates for the following:

- ARRA added to list of sources.
- Removed sections that are described in more detail in the security and privacy constructs.
- Updated formatting and links of references to standards in Table 2-1 Guidance Standards
- Added Security and Privacy Service Collaborations to list of constructs in Table 3-1 HITSP Security and Privacy Constructs
- Amended descriptions of out-of-scope requirements in Table 3-2 Out-of-Scope Requirements Assessment
- Added gaps to point to XSPA AND NIST levels of assurance in Table 3-3 Construct Standards Gaps
- Added columns for Anonymize and Pseudonymize in Table 4-1 Relationship of Privacy Principles and HITSP Security and Privacy Constructs
- Added Privacy and Security service collaborations to Table 4-4 Security and Privacy Construct Summary
- Removed Figure 4.4-1 Core Security and Privacy Constructs diagram
- Updated figures to reflect current updates to underlying constructs,
- Removed appendix descriptions of the application of security and privacy constructs to the HITSP/IS01, HITSP/IS02, and HITSP/IS03 specifications. These specifications have since been published with the appropriate security and privacy requirements as previously noted.
- Added discussion on HITSP/T31 and HITSP/T33, and their relationship to HITSP/TP13.
- Clarified construct relationships
- Added descriptions for the Anonymize, Pseudonymize, and Secure Web Connection constructs
- Added descriptions for the Access Control and Security Audit Service Collaborations



- Added a current list of Security, Privacy and Infrastructure Constructs

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

8.6 JULY 8, 2009

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

8.7 JANUARY 18, 2010

- Differentiate “entity identity” and “patient identity”
- Integrate NIST SP800-95 threats as part of risk mitigation description (Table 4-3)
- Describe Consent Management Capability (HITSP/CAP143)
- Included additional Anonymize constructs (HITSP/C164, HITSP/C165)

8.8 JANUARY 25, 2010

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

