

HITSP Security and Privacy Requirements, Design and Standards Selection for Biosurveillance, EHR-Lab, and Consumer Empowerment Use Cases

HITSP/RDSS51



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security and Privacy Technical Committee



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	April 13, 2007

REVIEW COPY



TABLE OF CONTENTS

1.0	INTRODUCTION.....	4
1.1	Purpose	4
1.2	Audience.....	4
1.3	How to Use this Requirements, Design and Standards Selection Document.....	4
1.3.1	Conventions, Acronyms and Resources/References.....	5
1.4	Copyright Permissions.....	5
2.0	REQUIREMENTS ANALYSIS	6
2.1	Use Case Synopsis	6
2.2	Use Case Requirements	7
2.2.1	Mapping of Use Case Requirements to Business Requirements	8
2.2.2	Data and Information Requirements Matrix.....	23
2.2.3	Identification of Business Actors, Interactions, and Scenarios.....	23
2.2.4	High-Level UML Interaction (Business Sequence) Diagram.....	26
3.0	DESIGN.....	31
3.1	Scope of Design	31
3.1.1	Assumptions	31
3.1.2	Constraints	32
3.1.3	Pre-Conditions	32
3.1.4	Post-Conditions	32
3.1.5	Process Triggers	33
3.2	Design.....	33
3.2.1	Mapping of Business Actors to Technical Actors	33
3.2.2	Technical Design	39
3.2.3	List of Transactions	40
3.2.4	Data Detail.....	44
3.2.5	Planned HITSP Constructs.....	45
4.0	CANDIDATE STANDARDS.....	52
4.1	Table of Candidate Standards.....	52
4.2	Gaps Where There Are No Standards	61
4.3	Standard Overlaps.....	61
5.0	NEXT STEPS	63
6.0	APPENDIX	64
6.1	Description of Candidate Standards.....	64
6.2	Security and Privacy Technical Committee Members.....	124



FIGURES AND TABLES

Figure 2.2.4-1 Security and Privacy Key Capabilities/Potential Constructs	29
Table 2.2.1-1 Mapping of Use Case Requirements to Business Requirements	9
Table 2.2.2-1 Data Element and Information Requirements	23
Table 2.2.3-1 Business Actors	24
Table 2.2.4-1 Key Capabilities/Potential Constructs.....	27
Table 2.2.4-2 Logical Relationships Between Key Capabilities.....	30
Table 3.1.1-1 Assumptions	32
Table 3.1.2-1 Constraints.....	32
Table 3.1.3-1 Pre-conditions.....	32
Table 3.1.4-1 Post-conditions	33
Table 3.1.5-1 Process Triggers.....	33
Table 3.2.1-1 Mapping of Business Actor(s) to Technical Actor(s).....	34
Table 3.2.3-1 Event/Action Codes and Related Transactions	40
Table 3.2.4-1 Data Element Constraints	44
Table 3.2.5.1-1 New HITSP Constructs.....	45
Table 3.2.5.2-1 Existing HITSP Constructs	49
Table 4.1-1 Legend for Table 4.1-2: Mapping of Key Capability/Potential Construct Numbers to Names.....	53
Table 4.1-2 Candidate Standards Linked to Requirements.....	53
Table 4.2-1 Use Case Events and Associated Gaps.....	61
Table 4.3-1 Standard Overlaps	62
Table 6.1-1 Description of Candidate Standards	64
Table 6.2-1 Security and Privacy Technical Committee Members.....	124



1.0 INTRODUCTION

As an introduction to the HITSP Security and Privacy Requirements, Design and Standards Selection, this section describes the purpose of the document, the intended audience for the technical content of the document, and how to use this document. It acknowledges the copyright protections that pertain, provides Internet links to the HITSP Acronyms List and an explanation of the conventions we use to convey the full descriptions and usage of standards. If you are already familiar with this information, proceed to Section 2.0 Requirements Analysis.

1.1 PURPOSE

The Requirements, Design and Standards Selection document is used to define the requirements for the Use Cases, the detailed HITSP set of Security and Privacy constructs and the design map of existing standards and specifications that will be used to meet the stated requirements. It is intended to describe the process by which the Use Cases were analyzed, candidate standards were identified and the design was developed.

1.2 AUDIENCE

The Requirements, Design and Standards Selection document is to be used by the HITSP Technical Committees or Work Groups to document their analysis and decisions, other analysts who need to understand and evaluate the requirements, design and select standards, and by those intending to test the resulting Interoperability Specifications against the Use Case requirements. Understanding and using the relevant set of Interoperability Specifications is a key requirement for establishing interoperability compliance.

1.3 HOW TO USE THIS REQUIREMENTS, DESIGN AND STANDARDS SELECTION DOCUMENT

The Requirements, Design and Standards Selection document is divided into five main related sections. Each section provides background information for the Security and Privacy set of constructs. Section 1.0 provides a brief introduction to the document. Users of this document who are familiar with the content may choose to proceed to Section 2.0. In Section 2.0, the Requirements Analysis provides a general overview of the Use Case and the specific requirements of the Use Case including a mapping of the Use Case requirements to the extracted business requirements, the data requirements of the Use Case, and an identification of the scenarios, business actors, their interactions, and data elements used in those interactions. The design for the Interoperability Specification is provided in Section 3.0. This includes the scope of the design, mapping of business requirements to the specific technical requirements, actor interactions and groupings, detailed descriptions of data used by the Use Case actors, and a description of existing or new HITSP constructs that will be used by the Interoperability Specification. Section 4.0 describes the Standards Selection process, provides a table of the candidate standards, a Gaps and



Overlaps discussion and plan for resolution. Section 5.0 describes the next steps in the HITSP standards harmonization process and Section 6.0 provides relevant appendix material.

1.3.1 CONVENTIONS, ACRONYMS AND RESOURCES/REFERENCES

The following sections include relevant materials referenced throughout this document.

The conventions are used to convey the full descriptions and usage of standards in the HITSP Interoperability Specifications and constructs and are contained in the [HITSP Conventions List](#).

The acronyms used in this document are contained in the [HITSP Acronyms List](#).

The [HITSP Harmonization Framework](#) describes the current framework within which the Interoperability Specifications are built.

This document references the following Interoperability Specifications and Harmonized Use Cases:

- Electronic Health Records (Laboratory Results Reporting) Interoperability Specification ([IS01](#)) and [Use Case](#)
- Biosurveillance (Visit, Utilization, and Lab Result Message) Interoperability Specification ([IS02](#)) and [Use Case](#)
- Consumer Empowerment (Registration and Medication History) Interoperability Specification ([IS03](#)) and [Use Case](#)

1.4 **COPYRIGHT PERMISSIONS**

COPYRIGHT NOTICE

© 2007 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.



2.0 REQUIREMENTS ANALYSIS

This section provides a high level description of the Security and Privacy requirements that are extracted from the Biosurveillance, EHR-Lab, and Consumer Empowerment Use Cases. It includes the following information:

- Mapping from the Use Case Requirements to the Derived Business Requirements – this table lists the requirements grouped by actor for each event and related action
- Data Element Requirements – this table will be used to further describe the data requirements for each specified business requirement and the business actor that is responsible for the data. The data and information requirements will be provided in the relevant HITSP constructs after the standards for meeting security and privacy requirements have been selected
- Business Actors – this table defines the business actors that are included for the Security and Privacy constructs
- High level UML Interaction (Business Sequence) Diagram – this diagram is used to describe the interaction and relationship between the security and privacy key capabilities (potential HITSP constructs) in each scenario that is documented

2.1 USE CASE SYNOPSIS

This section provides a synopsis of the Security and Privacy requirements for the 2006 set of AHIC Use Cases, including any applicable scenarios that are part of the Use Case. The aim is to harmonize HITSP selected standards based on the EHR-Lab, Biosurveillance and Consumer Empowerment Use Case requirements and priorities with relevant security and privacy standards. Specifically, the focus is on identifying and constraining the standards needed for standards-based security and privacy frameworks that provide the mechanisms needed to protect patient privacy and maintain confidentiality, integrity and availability (which are governed by policy). Standards-based security and privacy frameworks will need to support federal, state, local, and healthcare enterprise security and privacy policies and processes.

Implicitly and in some cases explicitly, the Biosurveillance, Consumer Empowerment, and EHR-Lab Use Cases require a secure infrastructure and certain security or privacy functions.

The Biosurveillance Use Case describes the process or interaction that each primary stakeholder will invoke in the capture, discovery, anonymization, and transmission of relevant data. The Use Case addresses the transmission of essential data from ambulatory care and emergency department visits, utilization, and laboratory result data from electronically enabled healthcare delivery and public health systems in a standardized and appropriately anonymized format to authorized Public Health Agencies with less than one day lag time. The Biosurveillance Interoperability Specification is also required to support the ability for authorized public health personnel to go back to the data source to seek to re-link the biosurveillance data to the data source, and/or the subject of the data, as part of an appropriate public



health investigation. Therefore, the management of data to ensure proper routing, security, privacy, and timely reporting is critical to enabling biosurveillance activities.

The security and privacy considerations for the Consumer Empowerment Use Case surround the identification of the principle stakeholders and flow of events for the authorized and secure exchange of consumers' registration summaries and medication histories. Namely, enabling consumers to establish permissions and access rights for viewing their individually identifiable health information; authenticating consumers, designated caregivers, and health professionals; querying other organizations for data and matching to the consumer; accepting "batch" data from other organizations and matching to the appropriate consumers; and finally accessing, viewing, and sharing registration summaries and medication histories.

For the EHR-Lab Use Case, the goal is to allow a clinician to order and electronically obtain laboratory test results, and to electronically obtain historical and other relevant test results for the purpose of the clinical care of a patient. There is a requirement for interoperability between clinical care providers' systems (which may include electronic health records), laboratory systems and the necessary supporting network, information and security services. Further security considerations include making use of services that manage patient identity, result delivery and notification, and that guarantee confidentiality, integrity and patient privacy.

In summary, the requirements for security and privacy are interwoven and directly derivable from the Use Cases described above. A more detailed summary of the Use Cases and the HITSP Interoperability Specifications is contained in the [Executive Summary for IS01, IS02 and IS03](#) document.

2.2 USE CASE REQUIREMENTS

This section describes the Use Case requirements at a high level for the following harmonized AHIC Use Cases:

- EHR-Lab Scope for security and privacy
- Consumer Empowerment Scope for security and privacy
- Biosurveillance Scope for security and privacy

The AHIC Use Cases provided the scope for the development of named standards and implementation level guidance necessary for interoperable solutions. Although there are common key security and privacy capabilities used by all, each Use Case presents a unique set of security and privacy requirements.

The Biosurveillance Use Case describes the process or interaction that each primary stakeholder will invoke in the capture, discovery, anonymization, and transmission of relevant data. In this regard, the Biosurveillance Use Case requires a secured and authenticated communication channel to ensure the



integrity and confidentiality of the transaction and mutual trust between the communicating parties when transmitting and receiving relevant data among public health agencies. Another important consideration in the Biosurveillance Use Case is the collection and communication of a security audit trail to support authorized public health investigators' needs for accountability information.

For the EHR-Lab Use Case, there is again a concentration of requirements around the provision of a secure and authenticated communication channel, and the collection and communication of audit information to track access and queries of an EHR. In addition to these requirements, the EHR-Lab Use Case requires patient consents/authorizations and security controls which enforce various policies, the verification of patient consent and authorization, the identification, administration and authentication of users of the EHR, management, and the verification of the integrity of transmitted and received laboratory messages and documents.

The Consumer Empowerment Use Case identifies the need for the authorized and secure exchange of consumers' registration summaries and medication histories. The security and privacy considerations listed for the Biosurveillance and EHR-Lab Use Cases are pertinent to the Consumer Empowerment Use Case as authenticated consumers establish permissions and access rights for viewing of their personal health record (PHR) data, setup and operate the PHR system, and have their registration and medication summaries searched, viewed and shared by providers of care.

An important consideration for all the Use Cases is that HITSP is providing the mechanism to support various policies on security and privacy which are not set nor defined by HITSP. Examples include variations among Federal, State, and local laws, regulations, and case law.

2.2.1 MAPPING OF USE CASE REQUIREMENTS TO BUSINESS REQUIREMENTS

This section contains an extraction of business actors, required interactions and conditions/scenarios from the Use Case into a matrix/table.

In the table below, the security and privacy requirements for the Biosurveillance, EHR-Lab and Consumer Empowerment Use Cases are listed by business actor, Use Case, event and action number. Note that in the table below, the first row refers to a "Default set of requirements." This set of requirements is referenced later in the table by different business actors for specific Use Case events. The requirements that make up the "Default set of requirements" are used as a group for the business actor and event that is being described, whenever the "Default set of requirements" is referenced. The Interoperability Requirements listed in the table need to be supported by mechanisms to enable the assessment of whether each requirement is met and whether capabilities are available to support them.



Table 2.2.1-1 Mapping of Use Case Requirements to Business Requirements

Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
All applicable actors	All applicable Use Cases	All applicable scenarios	Default set of requirements	Communicating parties have transmission integrity Data are transmitted using a trusted path Session used to transmit data has authenticity Data are transmitted with confidentiality and transmission integrity, trusted path, session authenticity Data to be collected/audited are identified Data to be reported for audit are formatted Data to be reported for audit are collected Reports are provided for analysis of audit data Audit data are retained for analysis Automated responses are provided for audited data Alerts and alarms are provided for security audit Identity of users is recorded whenever PHI is accessed Time of access is recorded whenever PHI is accessed Identity of users is recorded whenever registration data are accessed Time of access is recorded whenever registration data are accessed Clock synchronization source is determined EHR and PHR time clocks are synchronized to a predetermined source to ensure both are consistent
1.1.0.0 Individual Health	Biosurveillance	1: Transmission and Receipt of Relevant Biosurveillance Data 1.1.3.0	1.1.2.0 Anonymize data required by public health agencies	Data ready for transmission is anonymized
			1.1.5.0 Transmit Relevant Data To Public Health Agencies	Default set of requirements
1.2.0.0 Integrated healthcare data suppliers		2: Anonymize and Transmit data	1.2.2.0 Anonymize data required by public health agencies	Data ready for transmission is anonymized
			1.2.5.0 Transmit relevant data to public health agencies	Default set of requirements
1.3.0.0 Public Health Agencies		3: Receive data	1.3.2.0 Receive Biosurveillance data	Anonymized data are transmitted securely to PHA Communicating parties have transmission integrity Data are transmitted using a trusted path Session used to transmit data has authenticity Data are transmitted with confidentiality and transmission integrity, trusted path, session authenticity
2.1.0.0 Consumer	Consumer Empowerment	1: Consumer creates account to host registration summary & medication history	2.1.1.0 Select a provider of PHR services	Default set of requirements



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.1.2.0 Establish/Change permissions	<ul style="list-style-type: none"> Default set of requirements Patient consent directives are captured electronically in the PHR Patient consent is withheld Patient health information is masked from specific users Patient consent is withdrawn and captured in PHR Patient consent is revoked and captured in PHR Patient consent directives are transmitted to the EHR Processing of patient consent directives is logged in audit trail Provider access to patient health information is verified in accordance with the consumer consent. Patient consent directives are enforced to allow or block access to patient health information Users are authenticated to assure that the user is the person or application that claims the identity Data access policy is enforced
			2.1.3.0 Log on to system	<ul style="list-style-type: none"> Default set of requirements Users of the system are identified Identified users of the system are provided with their login credentials Identified users are assigned to their appropriate group Identified and credentialed users update their login information Users and groups are managed on an enterprise and cross-enterprise Directory services are managed on an enterprise and cross-enterprise User data are located by an entity with the ability to search across systems Registration and medication data are accessed based on user permission for data access Registration data are modified, updated or corrected by identified users Selective registration data or medication data are blocked from users Requests for changes to registration or medication data are made by users to providers/sources of data Users are authenticated to assure that the user is the person or application that claims the identity Data access policy is enforced



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.1.4.0 View registration and medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified and credentialed users update their login information</p> <p>Users and groups are managed on an enterprise and cross-enterprise</p> <p>Directory services are managed on an enterprise and cross-enterprise</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted is checked for integrity of contents</p> <p>Data transmitted is secured to ensure it is not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.1.5.0 Modify registration and medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified and credentialed users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.1.6.0 Close account	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified and credentialed users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted is checked for integrity of contents</p> <p>Data transmitted is secured to ensure it is not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>
2.2.0.0 Provider of PHR Services		2: Consumer visits Healthcare Provider and provides registration summary information2.3.0.0	2.2.1.0 Create account	<p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.2.2.0 Gather registration and/or medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified and credentialed users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted is checked for integrity of contents</p> <p>Data transmitted is secured to ensure it is not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.2.3.0 Process request for registration and/or medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified and credentialed users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.2.4.0 Close account	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed on an enterprise and cross-enterprises</p> <p>Directory services are managed on an enterprise and cross-enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
2.3.0.0 Healthcare Provider		3: Authorized Healthcare Provider reviews medication history	2.3.1.0 View registration and/or medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.3.2.0 Integrate registration data into EHR or other care system	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			2.3.3.0 Process requested data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
2.4.0.0 Data or Network System		4: Process request for medication data	2.4.1.0 Process request for registration and/or medication data	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p> <p>Authenticity of data transmitted is guaranteed or assured</p>
3.1.0.0 Patient	EHR-Lab	1: Ordering clinician receives results integrated into the EHR; providers of care receive test results or notification of test results	3.1.2.0 Identify providers of care, update as needed	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
3.2.0.0 Clinician		2: Clinician queries for historical test results and receives results either integrated into the EHR or viewed using a clinical data system (non-EHR system)	3.2.1.0 Integrate results and view in EHR	<p>Default set of requirements</p> <p>Patient consent directives are captured electronically in the PHR</p> <p>Patient consent is withheld</p> <p>Patient health information is masked from specific users</p> <p>Patient consent is withdrawn and captured in PHR</p> <p>Patient consent is revoked and captured in PHR</p> <p>Patient consent directives are transmitted to the EHR</p> <p>Processing of patient consent directives is logged in audit trail</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users of the system are identified</p> <p>Identified users of the system are provided with their login credentials</p> <p>Identified users are assigned to their appropriate group</p> <p>Identified users update their login information</p> <p>Users and groups are managed in an enterprise and across enterprises</p> <p>Directory services are managed in an enterprise and across enterprises</p> <p>User data are located by an entity with the ability to search across systems</p> <p>Registration and medication data are accessed based on user permission for data access</p> <p>Registration data are modified, updated or corrected by identified users</p> <p>Selective registration data or medication data are blocked from users</p> <p>Requests for changes to registration or medication data are made by users to providers/sources of data</p> <p>Data transmitted are checked for integrity of contents</p> <p>Data transmitted are secured to ensure they are not altered in violation of policy</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p>
			3.2.2.0 Receive notification of laboratory test results	Default set of requirements
			3.2.3.0 Query for laboratory (historical) test results	<p>Default set of requirements</p> <p>Provider access to patient health information is verified in accordance with the consumer consent.</p> <p>Patient consent directives are enforced to allow or block access to patient health information</p> <p>Users are authenticated to assure that the user is the person or application that claims the identity</p> <p>Data access policy is enforced</p>



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			3.2.4.0 View results using another clinical data system (non-EHR system)	Default set of requirements Provider access to patient health information is verified in accordance with the consumer consent. Patient consent directives are enforced to allow or block access to patient health information Data transmitted are checked for integrity of contents Data transmitted are secured to ensure they are not altered in violation of policy Data access policy is enforced
3.3.0.0 Laboratory		3: Process lab order	3.3.1.0 Process Laboratory Order	Default set of requirements
3.4.0.0 Data Repository		4: Process lab result	3.4.1.0 Store laboratory results	Default set of requirements Data transmitted are checked for integrity of contents Data transmitted are secured to ensure they are not altered in violation of policy
			3.4.2.0 Notify locator service of laboratory results	Default set of requirements Users are authenticated to assure that the user is the person or application that claims the identity
			3.4.3.0 Process Request for Laboratory Test Results	Default set of requirements Users of the system are identified Identified users of the system are provided with their login credentials Identified users are assigned to their appropriate group Identified users update their login information Users and groups are managed in an enterprise and across enterprises Directory services are managed in an enterprise and across enterprises User data are located by an entity with the ability to search across systems Registration and medication data are accessed based on user permission for data access Registration data are modified, updated or corrected by identified users Selective registration data or medication data are blocked from users Requests for changes to registration or medication data are made by users to providers/sources of data Users are authenticated to assure that the user is the person or application that claims the identity
3.5.0.0 Locator Service		5: Notification of Results	3.5.1.0 Publish availability of laboratory test results	Default set of requirements



Perspective/ Business Actor	Use Case	Scenario	Event	Interoperability Requirement(s)
			3.5.2.0 Process query to provide laboratory test result location(s)	Default set of requirements Provider access to patient health information is verified in accordance with the consumer consent. Patient consent directives are enforced to allow or block access to patient health information Users of the system are identified Identified users of the system are provided with their login credentials Identified users are assigned to their appropriate group Identified users update their login information Users and groups are managed in an enterprise and across enterprise Directory services are managed in an enterprise and across enterprise User data are located by an entity with the ability to search across systems Registration and medication data are accessed based on user permission for data access Registration data are modified, updated or corrected by identified users Selective registration data or medication data are blocked from users Requests for changes to registration or medication data are made by users to providers/sources of data

2.2.2 DATA AND INFORMATION REQUIREMENTS MATRIX

This section will contain an extraction of data and information requirements with a listing of the actual data elements and information that meet the described data requirements. The data and information requirements will be provided after the standards for security and privacy are selected, and will be included in the appropriate Security and Privacy Construct.

Table 2.2.2-1 Data Element and Information Requirements

Requirement Number	Description	Use Case/Scenario
The data and information requirements will be provided after the standards for security and privacy are selected.	Secure patient data are provided, including (but not limited to):	

2.2.3 IDENTIFICATION OF BUSINESS ACTORS, INTERACTIONS, AND SCENARIOS

This section describes the business actors that need to be integrated in order to meet the interoperability requirements for each scenario. A business actor is a representation of a person, IT system, organization or any combination that is engaged, and benefits from the real world information interchange defined by a



business Use Case. The table below describes the optionality of the actors involved and a description of the actor roles.

Table 2.2.3-1 Business Actors

Business Actor	Description	Use Case/Scenario
Authorized Third Party Consumer	An entity authorized by the patient to access the PHR. This includes, but is not limited to, disability insurers, schools, relatives, etc. and entities who request medical information for purposes other than for providing healthcare services or payment for healthcare services.	Out of scope for current Use Cases
Clinical Information System (Document Source)	Information system that supports the clinical care and information management for ambulatory, inpatient, and emergency department settings for organizations, such as hospitals, physician practices, which manage the delivery of care and submission of utilization resource information.	BIO, CE, EHR
Clinician	In ambulatory and emergency department settings, the healthcare providers within healthcare delivery organizations with direct patient interface in the delivery of care, including physicians, nurses, and clinical supervisors. These business actors are involved in the entry of source data into the system. In the case of reportable conditions, these business actors will also enter supplemental public health data elements into the data capture form.	BIO, EHR
Consumer	The individual who receives healthcare services and selects a provider of PHR services to maintain their personal health record consisting of registration data and medication history. This individual determines which Business Actors are authorized to review, access, and update their personal health record.	CE
Electronic Health Record (EHR) System	The Electronic Health Record (EHR) is a secure, real-time, point-of-care, patient-centric information resource for clinicians.	CE, EHR
Emergency Operations Center (Biosurveillance System)	Local, state, and federal government organizations and personnel that exist to help protect and improve the health of their respective constituents. A critical effort under this charge is collecting health information to monitor for the existence of emerging health threats appearing in the population and manage these threats once manifested.	BIO
Healthcare delivery organization	Organizations, such as hospitals, physician practices, which manage the delivery of care and submission of utilization resource information. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	BIO, CE, EHR
Health Plan/Intermediary	The organization or its designated intermediary that pays for healthcare, may participate as a data or network system of registration summary information, and can act as a provider of PHR services.	BIO, CE



Business Actor	Description	Use Case/Scenario
Laboratory	The entity that produces the laboratory results. Organizations operating from the Provider of Care perspective may also operate under the laboratory perspective if laboratory testing services are performed by the organization.	EHR
Laboratory Information System	Information system that supports the testing, analysis, and information management for laboratory organizations. Medical laboratories, in either in a hospital or ambulatory environment, which analyze specimens as ordered by clinicians to assess the health status of patients. Laboratories, depending on how they are affiliated with hospitals, can be part of either Individual Healthcare Facilities or Integrated Healthcare Data Suppliers. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	EHR
Locator Service	Document Registry	EHR
Message Source (Bio Message Sender)	Information system supporting the clinical care and information management for ambulatory, inpatient, and emergency department settings for organizations, such as hospitals, physician practices, which manage the delivery of care and submission of utilization resource information.	BIO
Patient	Receiver of care from a healthcare professional.	EHR
Personal Health Record (PHR) Service Provider	A system managing the set of health related information used by the consumer and providing access to this health information to other care or service providers as appropriate. This may include information generated by pharmacy information systems, pharmacy, health plan systems, clinician/healthcare providers, physicians' and hospitals' electronic health record systems, as well as patient generated information.	CE
Pharmacy Benefit Manager (PBM)/Pharmacy	The organization that has been delegated authority from the payer to process pharmaceutical claims, intermediary, pharmacy or sub network to provide data for medication history, and can act as a provider of PHR services.	CE
Provider of Care	May be an individual, an organization or "system." When appropriate, the Provider of Care perspective is further specified as an 'ordering Provider of Care' (responsible for ordering the laboratory test) or a 'provider of care' (providing care to the patient, but not the ordering Provider of Care).	BIO, EHR



Business Actor	Description	Use Case/Scenario
Public Health Agencies (local/state/federal)	Local, state, and federal government organizations and personnel that exist to help protect and improve the health of their respective constituents. A critical effort under this charge is collecting health information to monitor for the existence of emerging health threats appearing in the population and manage these threats once manifested. Staffs of these agencies interact with the Biosurveillance Information System to verify and validate system indications of public health threats, and to assert acknowledgements that may be required by system processes.	BIO
Public Health Agencies Biosurveillance Information System (BIS)	The Biosurveillance Information System provides support to, clinicians, epidemiologists and case managers to identify and manage public health threats using data received from the clinical information systems.	BIO
Radiology Information System	Information system that supports the testing, analysis, and information management for radiology service organizations. Radiology services, depending on how they are affiliated with hospitals, can be part of either Individual Healthcare Facilities or Integrated Healthcare Data Suppliers. These business actors are responsible for updating interface engine rules and triggers in response to Use Case modifications of requested data feeds.	BIO
Regional Capture Center (Data Source System)	Network or collaborative of regional inpatient healthcare delivery organizations utilizing a common service to capture and forward on resource availability information to BIS Emergency Operations Centers. This may be a service facilitated by a RHIO.	BIO
Regional Health Information Organization (RHIO)	A Regional Health Information Organization is a multi-stakeholder organization that enables the exchange and use of health information, in a secure manner, for the purpose of promoting the improvement of health quality, safety and efficiency.	CE
Repository	The system that provides the laboratory test results	EHR
Patient ID Cross-Referencing Service	An application that references a patient data base for the purpose of identifying a particular patient based on one of many IDs or by matching patient demographics.	EHR

2.2.4 HIGH-LEVEL UML INTERACTION (BUSINESS SEQUENCE) DIAGRAM

This section contains an explanation of the conceptual relationship between the security and privacy key capabilities (potential HITSP constructs) which have been identified from the requirements analysis of the existing harmonized AHIC Use Cases.

The security and privacy requirements of the current Use Cases can be grouped together into key capabilities that are necessary to support the events detailed in the current Use Cases. These key capabilities can then be used to support the AHIC Use Case events and actions independently, or coupled with other capabilities.



Table 2.2.4-1 Key Capabilities/Potential Constructs

Capability/ Potential Construct #	Short Title	Description
1	Secured Communication Channel	Provides the mechanisms to ensure integrity and confidentiality of transactions and mutual trust between the communicating parties. It includes mutual node authentication, integrity and confidentiality of the transmission contents. There is a relationship between this key capability and the "Manage Entity Identity Credentials" key capability to authorize the session (the nodes must be allowed to communicate with each other). This key capability supports both application and machine credentials, and user machines (user nodes). An example is a secured communication between a PHR system and EHR system, or EHR system to a Laboratory.
2	Collect and Communicate Security Audit Trail	Provides the mechanisms to define and identify security relevant events and data to be collected, communicated or audited 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, as well as sending out alerts or alarms and automated responses. This construct may be used as a part of, but is distinct from a disclosure log.
3	Privacy Consents	Describes the mechanisms needed to communicate permissions provided with the consent to access, use, collect or disclose healthcare information, and also supports the delegation of the patient's right to consent. The mechanisms support policies including multi-jurisdictional requirements or regulations, and also include standard vocabulary that supports granularity and sensitivity. An example of this capability is a restriction placed on the disclosure of a laboratory result for substance use under 42 CFR Part 2. Several scenarios exist such as: a. Patient has the right to invoke the consent and the entity has no ability to deny the consent b. The patient can request the conditions of the consent can be invoked but it may be refused c. Consent can be invoked when the law requires the consent to happen (deemed consent) d. Voluntary consent (regardless of whether law permits it)
4	Verify Privacy Consents	Provides the mechanisms to enforce the rules defined by Privacy Consents construct (number 3). For example, the mechanisms allow the verification of a provider's access to a particular laboratory result in accordance with the consumer's consent.
5	Manage Entity Identity Credentials	Provides the mechanisms to support management of system/individual credentials. This is identity proofing of IT users of a system (such as providers, clerks, systems, nodes). Examples of this capability include a user being initially identified and given their IT credentials, users' being assigned to groups, and definitions of their memberships.
6	Document Integrity	Provides the mechanisms to ensure the integrity of a document whether it is at rest or in transit. 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.
7	Authenticate User	Provides the mechanisms to ensure that the user is the person or application that claims the identity provided. An example of this is the validation and authentication of a consumer logging on to a PHR system.
8	Manage and Control Data Access	Provides the mechanism to administer security authorizations which control the enforcement of security policies, including role-based access control, entity based access control, and context based access control. An example of this is a functional role that has the permission to perform an act (consumer updating a 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 may include the Emergency Contact Registry Query Transaction (ECON).
9	Non-Repudiation	Provides the mechanisms to support non-repudiation, which refers to the concept of ensuring the irrefutability of claimed actions, such as the transmission of a document or message (e.g. a lab result) from a particular entity at a particular time.



Capability/ Potential Construct #	Short Title	Description
10	<i>Failsafe/Emergency Access</i>	<i>This capability has been subsumed by constructs 4 and 8 and is no longer needed as a separate construct.</i>
11	Consistent Time	Describes a mechanism by which all the systems identified in the Use Case can be synchronized to a consistent time. An example of this capability is the ability of an audit repository that has received audit events from all the participating systems to report the events in the order in which they actually occurred respective to a consistent time base.

The following UML logical diagram describes the conceptual relationship between the key security and privacy capabilities outlined above.

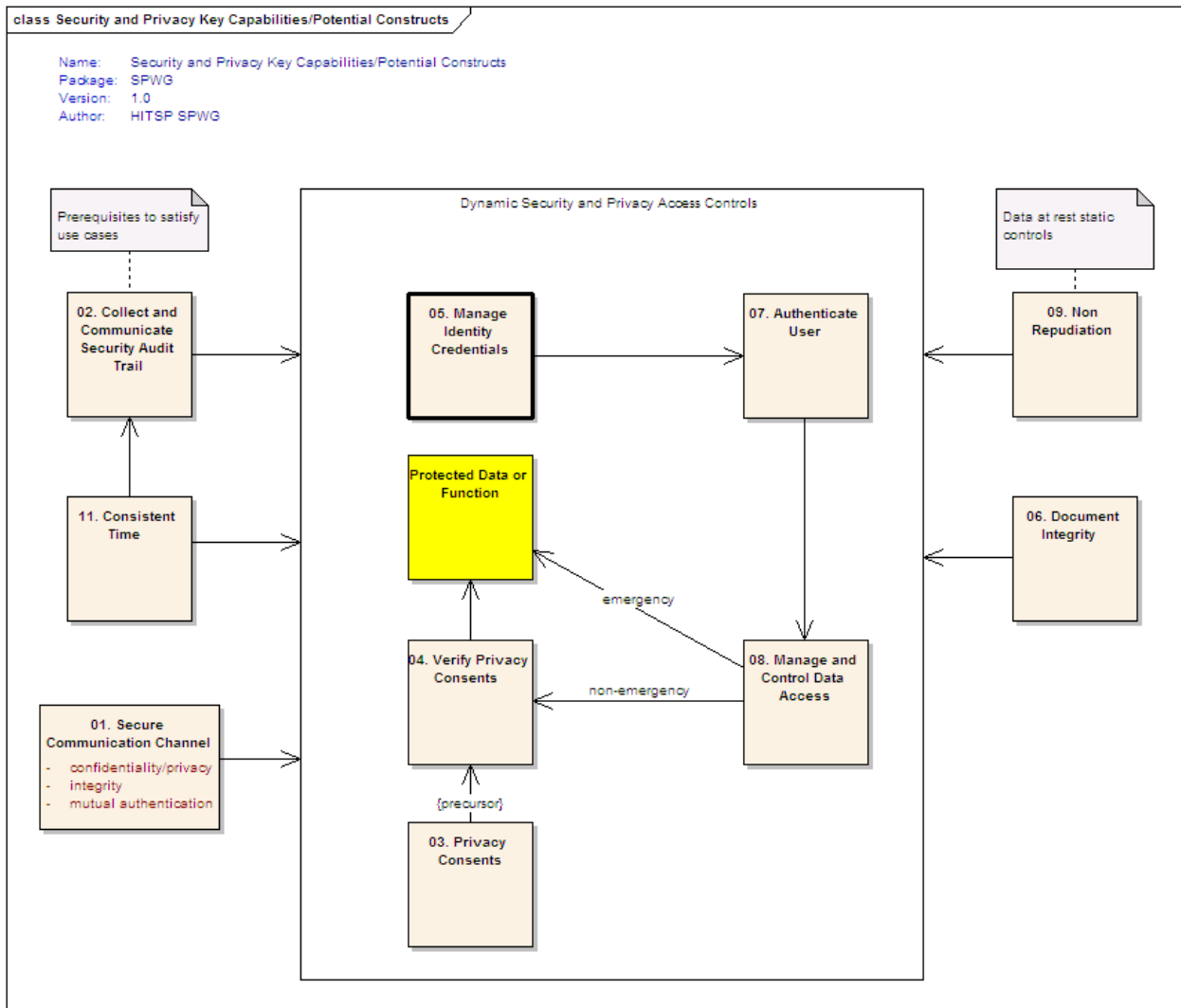
Each box represents a “potential HITSP construct”, which will contain selected standards and corresponding implementation guidance. As our work to develop these constructs continues, they can be considered “key capabilities” for the security and privacy requirements as identified through analysis of each of the existing AHIC Use Cases.

The Dynamic Security and Privacy Access Controls (depicted in the center of the diagram) represent the relationship of the constructs to the use and disclosure of individually identifiable patient information within the context of the AHIC Use Cases. The boxes on the left of the diagram represent prerequisites to these dynamic security and privacy access controls, while the boxes on the right of the diagram are static controls (applicable to data at rest).

Potential Construct number 5, “Manage Entity Identity Credentials”, is the starting point for how we represent access to the health information (end point). This would represent the identity of an entity (e.g. a node or a user’s digital identity) which is then authenticated using construct number 7, “Authenticate User”. The level and type of data access for each authenticated entity is subsequently determined by construct number 8, “Manage and Control Data Access” (e.g. role based access control). In a non-emergency situation, access to the target data would be subsequently verified by construct number 4, “Verify Patient Consent, Authorizations”. In some cases (e.g. “emergency access”), construct number 8 will have the capability of changing/elevating an entities privileges to facilitate direct access to the target data without the need for additional privacy consent-based restrictions. In other words, in an emergency situation construct number 4 may be bypassed.



Figure 2.2.4-1 Security and Privacy Key Capabilities/Potential Constructs



The diagram does not describe a process flow, nor does it imply functional or data relationships. The relationships depicted in the diagram in Figure 2.2.4-1 illustrate the interdependencies between the key capabilities. It shows that Secure Communication Channel, Collect and Communicate Audit Trail, and Consistent Time are key capabilities that are necessary to support security and privacy. They are prerequisite conditions of all the events that are supported.

In addition to the access flow diagram illustrated above, a matrix is presented in the table below which identifies all the relationships and interdependencies between each of the potential constructs/key capabilities.



Table 2.2.4-2 Logical Relationships Between Key Capabilities

Direct Relationship between Constructs	Secured Communication Channel	Collect and Communicate Security Audit Trail	Privacy Consents	Verify Privacy Consents	Manage Entity Identity Credentials	Document integrity	Authenticate User (include Across Enterprises)	Manage and Control Data Access	Non-Repudiation	Consistent Time
Secured Communication Channel										
Collect and Communicate Security Audit Trail	X									
Privacy Consents		X								
Verify Privacy Consents		X	X							
Manage Entity Identity Credentials	X	X	X	X						
Document integrity		X								
Authenticate User (include Across Enterprises)		X			X					
Manage and Control Data Access	X	X		X	X		X			
Non-Repudiation		X			X	X	X			
Consistent Time	X	X	X	X			X	X	X	



3.0 DESIGN

The design for the HITSP Security and Privacy constructs is the result of the requirements analysis and iterative standards selection process. This section describes the events and actions of the design from the specified requirements. It also provides a detailed mapping of the specified requirements to the business and technical actors, and where appropriate, data elements. Groupings of specific actions and actors are illustrated to further describe the relevant interactions as existing or new HITSP constructs required for interoperability.

3.1 SCOPE OF DESIGN

This section describes the scope of the design as it relates to the requirements for the Use Cases that were identified in section 2.2 above. The scope identifies the assumptions that provide the boundaries for the specification, and the constraints that limit the use of the specification. In addition, any pre-conditions, post-conditions and triggers that underlie the interactions between the various actors, data and transactions will be provided.

The Security and Privacy Technical Committee has identified 10 key capabilities (potential HITSP constructs) that are necessary to support the security and privacy requirements of the current Use Cases (described in section 2.2.4). These capabilities have been identified, out of the pool of considerations as the minimum necessary to effectively support the listed perspectives and events of the Use Cases. In the future, the Security and Privacy Technical Committee will continue to expand the scope of the mechanisms selected to support the existing Use Cases, to include the security and privacy requirements for assigned AHIC Harmonized Use Cases.

The following is out of scope:

1. Emergency Room 'break glass' requirements are going to be deferred to the Emergency Response EHR Use Case, so emergency room events are specifically scoped out of this Use Case.
2. Protection of the document (lab results) while at rest is out of scope for a non-EHR system. This is placed out of scope by the AHIC EHR-Lab Use Case.

3.1.1 ASSUMPTIONS

This section provides an overview of the assumptions, including the circumstances, actors, policies and/or technologies that need to be in place for the design to be completed as specified. Assumptions are different from constraints which are specifically used to narrow the definition, or indicate limitations of the specified interactions.



Table 3.1.1-1 Assumptions

Assumption	Use Case Scenario or Key Capability
System can identify that it is a legally reportable condition that is required to be reported, and patient cannot make independent decisions regarding reporting of condition (i.e. deemed consent)	BIO
The presumption is that communications will take place over the public network.	All
Assumptions for each of the security and privacy constructs will be identified during their detailed development.	All

3.1.2 CONSTRAINTS

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

Table 3.1.2-1 Constraints

Constraint	Use Case Scenario or Key Capability
Constraints for each of the security and privacy constructs will be identified during their detailed development.	All

3.1.3 PRE-CONDITIONS

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

Table 3.1.3-1 Pre-conditions

Pre-condition	Use Case Scenario or Key Capability
Pre-conditions for security and privacy constructs will be identified during their detailed development. It is the security and privacy constructs themselves that address many of the preconditions outlined in the HITSP Interoperability Specifications.	All

3.1.4 POST-CONDITIONS

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



Table 3.1.4-1 Post-conditions

Post-condition	Use Case Scenario or Key Capability
Post-conditions for security and privacy constructs will be identified during their detailed development.	All

3.1.5 PROCESS TRIGGERS

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

Table 3.1.5-1 Process Triggers

Trigger	Key Capability
Triggers for security and privacy constructs will be identified during their detailed development.	All

3.2 DESIGN

This section will provide a detailed description of the technical design, along with an analysis of the main interactions and decisions between all actors, actions and data in support of the specific requirements for each scenario of the Use Cases. In addition, this section provides the data element details (where appropriate) and an overview of the planned constructs used to meet the business and technical requirements for the Use Cases. Opportunities for reuse of existing HITSP constructs are outlined, along with a description of any necessary updates to existing constructs.

3.2.1 MAPPING OF BUSINESS ACTORS TO TECHNICAL ACTORS

This section contains a mapping of business actors to technical actors that need to be integrated in order to meet the interoperability requirements for each scenario. A Business Actor is a representation of a person, IT system, organization or any combination that is engaged, and benefits from the real world information interchange defined by a business Use Case, while a Technical Actor represents an entity internal to a software application, which is engaged in one or more specific transactions to support a specific aspect of a real world information interchange (e.g. set of message exchanges). The table below describes the optionality of the actors involved and the correlation between active actors.



Table 3.2.1-1 Mapping of Business Actor(s) to Technical Actor(s)

Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
Public Health Agencies (local/state/federal) (Bio Message Receiver)	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Bio-Data Receiver	O	An authorized entity that is receiving resource availability data (e.g. BIS/Emergency Operations Center)
Clinician	Secure Communications Channel Collect and Communicate Security Audit Trail Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Bio-Data Sender	O	Bio- Data Sender The holder of resource data who is communicating that data to the message receiver, typically the resource management information system (e.g. Census System/Bed Capacity System)
<ul style="list-style-type: none"> • Electronic Health Record (EHR) System • Personal Health Record (PHR) Service Provider • Provider of Care 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Document Consumer	R	The Document Consumer Actor queries a Document Registry Actor for documents meeting certain criteria, and retrieves selected documents from one or more Document Repository actors.
<ul style="list-style-type: none"> • Locator Service • Regional Health Information Organizations (RHIO) 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Document Registry	R	The Document Registry Actor maintains metadata about each registered document in a document entry. This includes a link to the Document in the Repository where it is stored. The Document Registry responds to queries from Document Consumer actors about documents meeting specific criteria. It also enforces some healthcare specific technical policies at the time of document registration.



Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
<ul style="list-style-type: none"> Electronic Health Record (EHR) System Personal Health Record (PHR) Service Provider Regional Health Information Organizations (RHIO) Repository 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Document Repository	R O O R	The Document Repository is responsible for both the persistent storage of these documents as well as for their registration with the appropriate Document Registry. It assigns a Uniform Resource Identifier (URI) to documents for subsequent retrieval by a Document Consumer.
<ul style="list-style-type: none"> Electronic Health Record (EHR) System Health Plan/Intermediary Laboratory Personal Health Record (PHR) Service Provider Pharmacy Benefit Manager (PBM)/Pharmacy 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Document Source	R O R R O	The Document Source Actor is the producer and publisher of documents. It is responsible for sending documents to a Document Repository Actor. It also supplies metadata to the Document Repository Actor for subsequent registration of the documents with the Document Registry Actor.
Clinician	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Laboratory Result Receiver	O	This actor is the recipient of laboratory result messages (i.e., the ordering clinician or other authorized provider of care)
Laboratory	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Laboratory Result Sender	O	This actor sends laboratory results as messages or as documents to the ordering clinician or other authorized providers of care.



Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
Public Health Agencies (local/state/federal) (Bio Message Receiver)	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Document Integrity Manage and Control Data Access Non-repudiation Consistent Time	Message Receiver	O	An authorized entity that is receiving resource availability data (e.g. BIS/Emergency Operations Center)
Radiology Information Systems (Bio Message Sender)	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Message Sender	O	The holder of resource data who is communicating that data to the message receiver, typically the resource management information system (e.g. Census System/Bed Capacity System)
Provider of Care	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Consistent Time	Notification Receiver	R	This actor receives notifications of availability for documents in a Cross Enterprise Document Sharing (XDS) registry, and may optionally send acknowledgments of them.
Laboratory	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Notification Sender	O	This actor sends notifications of availability for documents in a Cross Enterprise Document Sharing (XDS) registry, and receives acknowledgements of these notifications.



Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
<ul style="list-style-type: none"> Electronic Health Record (EHR) System Health Plan/Intermediary Patient Identifier Service Personal Health Record (PHR) Service Provider Pharmacy Benefit Manager (PBM)/Pharmacy 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Consistent Time	Patient Demographics Consumer	O	The Patient Demographics Consumer queries the Patient Demographics Supplier to obtain patient demographic data. It may receive matches for one or more patients that enable the selection of the desired patient.
<ul style="list-style-type: none"> Patient Identifier Service Regional Health Information Organizations (RHIO) 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Consistent Time	Patient Demographics Supplier	O	Receives patient registration and update messages from other systems in the enterprise (e.g., ADT Patient Registration systems), which may or may not represent different Patient ID Domains. It responds to queries for information.
Provider of Care	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Consistent Time	Patient Identifier Cross Reference Consumer	O	This actor allows a system in a Patient Identifier Domain to determine the identification of a patient in a different Patient Identifier Domain by using the services of a Patient Identifier Cross-Reference Manager Actor.
Patient Identifier Service	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Consistent Time	Patient Identifier Cross Reference Manager	R	Serves a well-defined set of Patient Identifier Domains. Responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains. Based on information provided in each Patient Identifier Domain by a Patient Identification Source Actor, it manages the cross-referencing of patient identifiers across Patient Identifier Domains.



Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
Electronic Health Record (EHR) System	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Authenticate Users Manage and Control Data Access Consistent Time	Patient Identity Source	O	The Patient Identity Source Actor is a provider unique identifier for each patient and maintains a collection of identity traits. Each Patient Identifier Domain requires this Actor to assign patient identities and to notify other Actors (e.g. a Patient Identifier Cross-Reference Manager or a Registry Actor) of all events related to patient identification (creation, update, merge, etc.).
<ul style="list-style-type: none"> Health Plan/Intermediary Patient Identifier Service Personal Health Record (PHR) Service Provider Pharmacy Benefit Manager (PBM)/Pharmacy 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Authenticate Users Consistent Time	Patient Identity Source	O	The Patient Identity Source Actor is a provider unique identifier for each patient and maintains a collection of identity traits. Each Patient Identifier Domain requires this Actor to assign patient identities and to notify other Actors (e.g. a Patient Identifier Cross-Reference Manager or a Registry Actor) of all events related to patient identification (creation, update, merge, etc.).
<ul style="list-style-type: none"> Electronic Health Record (EHR) System Health Plan/Intermediary Personal Health Record (PHR) Service Provider Pharmacy Benefit Manager (PBM)/Pharmacy 	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Authenticate Users Manage and Control Data Access Consistent Time	PIX Consumer	O	The Patient Identifier Cross-reference Consumer either queries for sets of cross-reference patient identifiers. It may also receive notifications about cross-reference changes.
Regional Health Information Organizations (RHIO)	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Consistent Time	PIX Manager	O	The Patient Identifier Cross-reference Manager Actor is responsible for creating, maintaining and providing lists of identifiers that are aliases of one another across different Patient Identifier Domains.



Business Actor	Scenario/ Key Capability	Technical Actor(s)	Required = R Optional = O	Actor Role
<ul style="list-style-type: none"> Regional Health Information Organizations (RHIO) Electronic Health Record (EHR) System Laboratory Information System Radiology Information System Healthcare Delivery Organization Clinician 	Secure Communications Channel Collect and Communicate Security Audit Trail Manage Entity Identity Credentials Consistent Time	Pseudonymization Service (P & A Service)	O	Supplier of alternative identification information that permits a patient to be referred to by a key that suppresses his/her actual identification information.
Consumer	Secure Communications Channel Collect and Communicate Security Audit Trail Privacy Consents Verify Privacy Consents Manage Entity Identity Credentials Document Integrity Authenticate Users Manage and Control Data Access Non-repudiation Consistent Time	Document Consumer Document Source	O	The individual who receives healthcare services and selects a provider of PHR services to maintain their personal health record consisting of registration data and medication history. This individual determines which Business Actors are authorized to review, access, and update their personal health record.

*Required = R

3.2.2 TECHNICAL DESIGN

The technical design incorporates the comprehensive business and technical requirements and a detailed analysis of the interactions and decisions undertaken for the primary actions in each Use Case scenario. UML sequence diagrams will be used in this section of each detailed HITSP construct to expand on the earlier diagrams illustrated in the Requirements Analysis sections of the document. They will incorporate the detailed data requirements for the selected standards, with the technical actors, independent transactions and groupings of dependent transactions. The independent transactions and groupings of transactions described in these more detailed interaction diagrams will be used to determine which HITSP constructs are necessary. Diagrams show all common or independent actors, data, actions, and groupings of actions around common actors. Transactions that make use of existing HITSP constructs are shown explicitly, indicating opportunities for reuse.

This section will be completed after the standards are selected.



3.2.3 LIST OF TRANSACTIONS

This section maps the transactions described above to the Use Case actions and events defined in the Requirements Analysis section, as well as the applicable scenarios. Actions and events not listed here (but which exist in the Use Case) that have been purposefully omitted are described in the Scope of Design section. Transactions are referenced in the UML diagrams shown in section 3.2.2 using a letter designation.

Table 3.2.3-1 Event/Action Codes and Related Transactions

Transaction Name	Event/Action Code	Content	Capability/Potential Construct Numeric Designation	Applicable Scenarios	Use Case
Secured Communication Channel	3.1.2.0	T.B.D.	1	Scenario 1, Scenario 2, Scenario 4, Scenario 5	EHR
	3.2.1.0				
	3.2.2.0				
	3.2.3.0				
	3.2.4.0				
	3.4.3.0				
	3.5.1.0				
	3.5.2.0				
	2.1.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
	2.1.2.0				
	2.1.3.0				
	2.1.4.0				
	2.1.5.0				
	2.1.6.0				
	2.2.1.0				
2.2.2.0					
2.2.3.0					
2.2.4.0					
2.3.1.0					
2.3.2.0					
2.3.3.0					
2.4.1.0					
1.1.5.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3	BIO	
1.2.5.0					
1.3.2.0					
Collect and Communicate Security Audit Trail	3.2.3.0	T.B.D.	2	Scenario 2, Scenario 3, Scenario 4, Scenario 5	EHR
	3.2.4.0				
	3.3.1.0				
	3.4.1.0				
	3.4.2.0				
	3.4.3.0				
	3.5.2.0				



Transaction Name	Event/ Action Code	Content	Capability/Potential Construct Numeric Designation	Applicable Scenarios	Use Case
	2.1.1.0 2.1.2.0 2.1.3.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
	1.1.5.0 1.2.5.0 1.3.2.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3	BIO
Privacy Consents	3.1.2.0 3.2.1.0	T.B.D.	3	Scenario 1, Scenario 2	EHR
	2.1.2.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
Verify Privacy Consents	3.1.2.0 3.2.1.0 3.2.3.0 3.2.4.0 3.5.2.0	T.B.D.	4	Scenario 1, Scenario 2, Scenario 5	EHR



Transaction Name	Event/ Action Code	Content	Capability/Potential Construct Numeric Designation	Applicable Scenarios	Use Case
	2.1.2.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
Manage Entity Identity Credentials	3.2.1.0 3.4.3.0 3.5.2.0	T.B.D.	5	Scenario 2, Scenario 4, Scenario 5	EHR
	2.1.1.0 2.1.3.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
	1.1.5.0 1.2.5.0 1.3.2.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3	BIO
Document Integrity	3.2.1.0 3.2.4.0 3.4.1.0	T.B.D.	6	Scenario 2, Scenario 4	EHR
	2.1.4.0 2.1.5.0 2.1.6.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE



Transaction Name	Event/ Action Code	Content	Capability/Potential Construct Numeric Designation	Applicable Scenarios	Use Case
Authenticate Users	3.2.1.0 3.2.3.0 3.4.2.0 3.4.3.0	T.B.D.	7	Scenario 2, Scenario 4	EHR
	2.1.2.0 2.1.3.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
Manage and Control Data Access	3.2.3.0 3.2.4.0	T.B.D.	8	Scenario 2	EHR
	2.1.2.0 2.1.3.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
Non-repudiation	2.1.6.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.	9	Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE



Transaction Name	Event/Action Code	Content	Capability/Potential Construct Numeric Designation	Applicable Scenarios	Use Case
Consistent Time	3.2.1.0 3.2.2.0 3.2.3.0 3.2.4.0 3.4.3.0 3.5.1.0 3.5.2.0	T.B.D.	11	Scenario 2, Scenario 4, Scenario 5	EHR
	2.1.1.0 2.1.2.0 2.1.3.0 2.1.4.0 2.1.5.0 2.1.6.0 2.2.1.0 2.2.2.0 2.2.3.0 2.2.4.0 2.3.1.0 2.3.2.0 2.3.3.0 2.4.1.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3, Scenario 4	CE
	1.1.5.0 1.2.5.0 1.3.2.0	T.B.D.		Scenario 1, Scenario 2, Scenario 3	BIO

3.2.4 DATA DETAIL

This section details the data elements and related transactions that were extracted from the selected standards and describes any corresponding HITSP imposed constraints (e.g., required or optional).

This section will be documented for each individual construct.

Table 3.2.4-1 Data Element Constraints

Data Element	Transaction	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
<Data Element>	<transaction short name>	<description of constraint>	< Pre-condition, post-condition, general >	<Reason for this constraint>



3.2.5 PLANNED HITSP CONSTRUCTS

This section describes the HITSP constructs (including Interoperability Specifications, Transaction Packages, Transactions and Components) that are expected to be used for Security and Privacy. It may create a new construct or reuse a component, transaction or a grouping of transactions (transaction package) based on commonality, if a new set of requirements and context are successfully fulfilled by the existing construct.

3.2.5.1 NEW HITSP CONSTRUCTS

The table below provides a description of the new HITSP constructs that will be created to meet the Security and Privacy requirements for the Use Cases. The Interoperability Requirements listed in the table need to be supported by mechanisms to enable the assessment of whether each requirement is met and whether capabilities are available to support them.

Table 3.2.5.1-1 New HITSP Constructs

New Construct	Construct Description	Common Actors	Requirement
Secured Communication Channel	<u>Key Functionality:</u> Mutual Node Authentication, session transmission, confidentiality and transmission integrity, trusted path, session authenticity	Bio-Data Receiver Bio-Data Sender Document Consumer Document Registry Document Repository Document Source Form Filler Form Manager Form Receiver (Biosurveillance Information System) Laboratory Result Receiver Laboratory Result Sender Message Receiver Message Sender Notification Receiver Notification Sender Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identifier Cross Reference Manager Patient Identity Source PIX Consumer PIX Manager Pseudonymization Service (P & A Service) Regional Capture Center (Data Source System) Emergency Operations Center	Data ready for transmission is anonymized. Anonymized data are transmitted securely to Public Health Agency Communicating parties have transmission integrity Data are transmitted using a trusted path Session used to transmit data has authenticity Data are transmitted with confidentiality and transmission integrity, trusted path, session authenticity



New Construct	Construct Description	Common Actors	Requirement
		(Biosurveillance System)	
Collect and Communicate Security Audit Trail	<u>Key Functionality:</u> Time, Auditable events, record content, monitoring analysis reporting (includes anomaly detection and analysis) and reduction, audit protection, alerts and alarms, support for accounting of disclosures	Bio-Data Receiver Bio-Data Sender Document Consumer Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Message Receiver Message Sender Notification Receiver Notification Sender Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identifier Cross Reference Manager Patient Identity Source PIX Manager Pseudonymization Service (P & A Service)	Data to be collected/audited are identified Data to be reported for audit are formatted Data to be reported for audit are collected Reports are provided for analysis of audit data Audit data are retained for analysis Automated responses are provided for audited data Alerts and alarms are provided for security audit Identity of users is recorded whenever Protected Health Information is accessed Time of access is recorded whenever Protected Health Information is accessed Identity of users is recorded whenever registration data are accessed Time of access is recorded whenever registration data are accessed
Privacy Consents	<u>Key Functionality:</u> masking (may include flagging and blocking info from patient), electronic capture of consent directives, granularity, sensitivity	Document Consumer Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Consumer Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identity Source	Patient consent directives are captured electronically in the PHR Patient consent is withheld Patient health information is masked from specific users Patient consent is withdrawn and captured in PHR Patient consent is revoked and captured in PHR Patient consent directives are transmitted to the EHR Processing of patient consent directives is logged in audit trail
Verify Privacy Consents	<u>Key Functionality:</u> enforcing the rules defined by Privacy Consent	Bio-Data Sender Document Consumer Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Consumer Message Receiver Message Sender	Provider access to patient health information is verified in accordance with the consumer consent. Patient consent directives are enforced to allow or block access to patient health information



New Construct	Construct Description	Common Actors	Requirement
		Notification Receiver Notification Sender Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identity Source PIX Manager Pseudonymization Service (P & A Service)	
Manage Entity Identity Credentials	<u>Key Functionality:</u> identity proofing and registration, user and group management, security credential management, self service (e.g. changing password, profile management), enterprise and cross-enterprise (federated) provisioning, directory services	Bio-Data Receiver Bio-Data Sender Document Consumer Document Registry Document Source Message Receiver Consumer Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identity Source PIX Manager Pseudonymization Service (P & A Service)	Users of the system are identified Identified users of the system are provided with their login credentials Identified users are assigned to their appropriate group Identified and credentialed users update their login information Users and groups are managed on an enterprise and cross-enterprise Directory services are managed on an enterprise and cross-enterprise User data are located by an entity with the ability to search across systems Registration and medication data are accessed based on user permission for data access Registration data are modified, updated or corrected by identified users Selective registration data or medication data are blocked from users Requests for changes to registration or medication data are made by users to providers/sources of data
Document Integrity	<u>Key Functionality:</u> Assurance that something has not been altered in violation of policy	Bio-Data Receiver Bio-Data Sender Document Consumer Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Message Receiver Message Sender Notification Receiver Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer PIX Manager	Data transmitted are checked for integrity of contents Data transmitted are secured to ensure they are not altered in violation of policy
Authenticate User	<u>Key Functionality:</u> Identification and	Bio-Data Receiver	Users are authenticated to assure that the user is the person or application that claims the identity



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

New Construct	Construct Description	Common Actors	Requirement
	authentication	Bio-Data Sender Document Consumer Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Message Sender Consumer Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identity Source PIX Manager	
Manage and Control Data Access	<u>Key Functionality:</u> Enforcement of the access policy	Bio-Data Receiver Bio-Data Sender Document Consumer Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Message Receiver Message Sender Consumer Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identity Source PIX Manager	Data access policy is enforced
Non-repudiation	<u>Key Functionality:</u> Guaranteed or assured authenticity	Bio-Data Receiver Bio-Data Sender Document Registry Document Repository Document Source Laboratory Result Receiver Laboratory Result Sender Message Receiver Message Sender Consumer PIX Manager	Authenticity of data transmitted is guaranteed or assured
Consistent Time	<u>Key Functionality:</u> Synchronization of clocks to a predetermined source	Bio-Data Receiver Bio-Data Sender Document Consumer	Clock synchronization source is determined EHR and PHR time clocks are synchronized to a predetermined source to ensure both are consistent



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

New Construct	Construct Description	Common Actors	Requirement
		Document Registry Document Repository Document Source Consumer Notification Receiver Notification Sender Patient Demographics Consumer Patient Demographics Supplier Patient Identifier Cross Reference Consumer Patient Identifier Cross Reference Manager PIX Manager Pseudonymization Service (P & A Service)	

3.2.5.2 EXISTING HITSP CONSTRUCTS

The table below provides a description of the existing HITSP constructs that will use the Security and Privacy constructs described in this document or will be used by these Security and Privacy constructs for this Use Case. It also specifies whether the construct will require modification based on the new sets of requirements that are being satisfied by the construct.

Table 3.2.5.2-1 Existing HITSP Constructs

Existing Construct	Construct Description	Common Actors	Requirement	Requires Modification ?
HITSP/IS01	HITSP Interoperability Specification: Electronic Health Record (EHR) Laboratory Results Reporting	All	The IS will be modified to require the use of the appropriate Security and Privacy constructs	Y
HITSP/IS02	HITSP Interoperability Specification: Biosurveillance	All	The IS will be modified to require the use of the appropriate Security and Privacy constructs	Y



Existing Construct	Construct Description	Common Actors	Requirement	Requires Modification ?
HITSP/IS03	HITSP Interoperability Specification: Consumer Empowerment	All	The IS will be modified to require the use of the appropriate Security and Privacy constructs	Y
HITSP/TP13	Manage Sharing of Documents Transaction Package			N
HITSP/TP14	Send Lab Result Message to Ordering Clinician and Providers of Care Transaction Package			N
HITSP/TP49	Sharing Radiology Results Transaction Package			N
HITSP/T18	View Lab Result from a Web Application Transaction			N
HITSP/T24	Pseudonymize Transaction			N
HITSP/T25	Anonymize Transaction			N
HITSP/C29	Notification of Document Availability Component			N
HITSP/C36	HITSP Interoperability Specification: Laboratory Result Message Component			N
HITSP/C41	Radiology Results Message Component			N
HITSP/C44	Secure Web Connection Component			N
HITSP/C45	Acknowledgements Component			N
HITSP/C50	Retrieve Form for Data Capture Transaction Package			N

3.2.5.3 CONSTRUCT ROADMAP FOR THE SECURITY AND PRIVACY CONSTRUCTS

Each Interoperability Specification (IS) is comprised of a suite of constructs that, taken as a whole, provide a detailed map to existing standards and specifications that will satisfy the requirements imposed by a given Use Case. The Interoperability Specification for each Use Case identifies and constrains standards where necessary, and creates groupings of specific actions and actors to further describe the relevant contexts using Transaction Packages, Transactions, and Components. Each of the Security and Privacy constructs will be used by the HITSP constructs such as the Interoperability Specifications to describe the relevant security and privacy contexts for use within those constructs. The roadmap



diagrams which show how each of the Security and Privacy constructs is used by the HITSP constructs will be provided in the next phase of the design process.

REVIEW COPY



4.0 CANDIDATE STANDARDS

This section presents the candidate standards that may support the major Use Case events described in the requirements analysis. In the next phase, the Security and Privacy Technical Committee will select the standards based on the following process:

- **Evaluation:** The Technical Committee evaluates the standards using the Tier 2 Readiness Criteria. The Tier 2 worksheets used to evaluate the list of standards are linked in the Appendix. Standards considered for use may include provisional or to be named standards
- **Selection:** Based on the Tier 2 evaluations, named standards are selected and listed in Table 4.1-1. It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. During the actual construction of HITSP set of Security and Privacy constructs, the Technical Committee may need to refine this listing based on detailed analysis.
- **Gap and Overlap Analysis and Recommendations:** The Technical Committee also identifies, and analyzes gaps and overlaps within the standards industry as they related to the specific Use Case. The TC will provide a description of the gaps, including missing or incomplete standards, provide a description of all overlaps, or competition among standards for the relevant Use Cases, and recommendations for resolving these gaps and overlaps.

Thus the following section lists a summary of the candidate standards that will be further refined in the next phase of design work.

4.1 TABLE OF CANDIDATE STANDARDS

This section presents the candidate standards that may support the Use Case events described in the requirements analysis. As used by HITSP, the term “standard” refers, but is not limited to Specifications, Implementation Guides, Code Sets, Terminologies, and Integration Profiles. A standard should be produced through a well-defined approach that supports a business process and

1. has been agreed upon by a group of experts
2. has been publicly vetted
3. provides rules, guidelines, or characteristics
4. helps to ensure that materials, products, processes, and services are fit for their intended purpose
5. is available in an accessible format
6. is subject to an ongoing review and revision process

Table 4.1-2 shows the candidate standard and the key capability which it may support. The legend relating key capabilities/potential construct names to identification numbers is shown in Table 4.1-1. During the next phase of design, the standards listed here will be further refined using the Tier 2 Criteria.



Final standards selection does not occur until the HITSP set of Security and Privacy constructs are completed. Thus there may be additions or deletions to the list of selected standards produced during the next phase of design. The columns labeled 1 through 11 refer to the numeric designations for the constructs described in Table 3.2.3-1 and Table 4.1-1.

Table 4.1-1 Legend for Table 4.1-2: Mapping of Key Capability/Potential Construct Numbers to Names

Key Capability/Potential Construct Number	Key Capability/Potential Construct Name
1	Secured Communication Channel
2	Collect and Communicate Security Audit Trail
3	Privacy Consents
4	Verify Privacy Consents
5	Manage Entity Identity Credentials
6	Document integrity
7	Authenticate Users (include Across Enterprises)
8	Manage and Control Data Access
9	Non-repudiation
11	Consistent Time

Table 4.1-2 Candidate Standards Linked to Requirements

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number											Comment/Notes	
			1	2	3	4	5	6	7	8	9	11			
ISO	IS22857	Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information		x	x	x									
ISO	TS21091	Health informatics -- Directory services for security, communications and identification of professionals and patients		x		x	x	x	x	x	x	x			
ISO	IS17090 part1,2,3	Health informatics -- Public key infrastructure	x	x	x		x	x	x	x	x	x			
ISO	(currently DTS, previously published as DR) DTS 21089	Trusted end-to-end information flows	x	x			x	x	x	x	x				
ISO	TS26000 part1,2	Health informatics - Privilege management and Access Control		x	x	x					x				
ISO	IS27799	Health informatics: Security management in health using IS17799	x	x	x	x	x	x	x	x	x	x			
ISO	TS21547	Health informatics: Secure archiving of electronic health records Part1 Principles and Requirements, Part 2 Guidelines		x					x						
ISO	DTS21298	Health informatics: Functional and structural roles			x	x	x				x				



Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number									Comment/Notes		
			1	2	3	4	5	6	7	8	9		11	
ISO	DTS 25238	Classification of safety risk from health informatics products												
CEN	DTR	TR Assuring patient safety of health informatics products												
ISO	TR18307	Requirements for interoperability and interoperability of messaging standards	x	x			x	x	x	x	x	x	x	
CEN	prEN_13606-4	Health informatics — Electronic health record communication — Part 4: Security requirements and distribution rules			x	x	x			x				
ASTM	E1869	Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records	x	x	x	x	x	x	x	x	x	x		
ASTM	E1985	Standard Guide for User Authentication and Authorization			x	x			x	x				
ASTM	E1986	Standard Guide for Information Access Privileges to Health Information		x	x	x	x		x	x				
ASTM	E1987	Standard Guide for Individual Rights Regarding Health Information			x	x				x				
ASTM	E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems		x										
ASTM	E2086	Standard Guide for Internet and Intranet Healthcare Security	x											
ASTM	E2085	Standard Guide on Security Framework for Healthcare Information	x											
ASTM	E1762	Standard Guide for Electronic Authentication of Healthcare Information						x				x		
ASTM	E2084	Standard Specification for Authentication of Healthcare Information Using Digital Signatures						x				x		
ASTM	E2212-02a	Standard Practice for Healthcare Certificate Policy	x				x							
ASTM	PMI	Privilege Management Infrastructure									x			
OASIS	WSS:SOAP Message Security	Web Services Security: Soap Message Security 1.1	x	x			x	x	x	x	x			
OASIS	WSS:SOAP Message Security	Web Services Security: Soap Message Security 1.0	x						x					
OASIS	ws-secureconversation-1.3-spec-cs-01	WS-SX: WS-Secure Conversation 1.3	x					x				x		
OASIS	ws-trust-1.3-spec-cs-01	WS-SX: WS-Trust 1.3					x		x					



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number											Comment/Notes
			1	2	3	4	5	6	7	8	9	11		
OASIS	XACML	eXtensible Access Control Markup Language (XACML)			x	x				x	x			
OASIS	WSRM	Web Services Reliable Messaging	x											
OASIS	SAML	Security Assertion Markup Language (SAML)			x	x	x			x				
OASIS	SPML	Service Provisioning Markup Language								x				
DICOM	Supplement 86	Digital Signatures in Structured Reports							x			x		
DICOM	Supplement 99	Extended Negotiation of User Identity								x				
WS-I		Basic Security Profile Working Group Draft	x	x			x	x	x	x				
WS-I		Kerberos Token Profile Working Group Draft								x				
WS-I		Threats and Countermeasures	x											
WS-I		REL Token Profile Working Group Draft								x	x			
WS-I		SAML Token Profile Working Group Draft					x			x				
IEEE	IEEE Std 802.1X-2004	IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control	x											
IEEE	IEEE Std 802.11i-2004	Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amend. 6: Medium Access Control (MAC) Security Enhancements	x											
IEEE	IEEE Std 1363-2000	IEEE Standard Specifications for Public-Key Cryptography					x	x				x		
IEEE	IEEE Std 1363a-2004	IEEE Standard Specifications for Public-Key Cryptography -- Amendment 1: Additional Techniques								x				
IEEE	P802.1AE	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security	x											
IEEE	P802.1af	Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control - Amendment 1: Authenticated Key Agreement for Media Access Control (MAC) Security	x											
IEEE	P802.11w	Amendment to Standard for Information Technology - Telecommunications and Information Exchange between systems - Local and Metropolitan Area networks - Specific requirements - Part 11	x											
IEEE	P1073.2.1.3	Health informatics - Point-of-care medical device communication - Application profile - Clinical context management (CCoM)	x											
IEEE	P1363	Standard Specifications for Public Key Cryptography (revision)	x									x		



Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number									Comment/Notes		
			1	2	3	4	5	6	7	8	9		11	
IEEE	P1363.1	Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices	x									x		
IEEE	P1363.2	Standard Specification for Password-Based Public-Key Cryptographic Techniques	x									x		
IEEE	P1363.3	Standard for Identity-Based Cryptographic Techniques using Pairings	x									x		
IEEE	P1609.1	Standard for Wireless Access in Vehicular Environments (WAVE)- Resource Manager	x											
IEEE	P1609.2	Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages	x											
IEEE	P1619	Standard Architecture for Encrypted Shared Storage Media										x		
IEEE	P1619.1	Standard Architecture for Encrypted Variable Block Storage Media										x		
IEEE	P1667	Standard Protocol for Authentication in Host Attachments of Transient Storage Devices										x		
Liberty Alliance	ID-FF 1.2 (FINAL)	The Identity Federation Framework	x				x		x	x				
Liberty Alliance	ID-WSF 1.1 (FINAL)	The Identity Web Services Framework	x				x		x	x				
Liberty Alliance	ID-WSF 2.0 (DRAFT)	The Identity Web Services Framework, Draft Release 2	x				x		x	x				
Liberty Alliance	ID-WSF DST 2.0 (FINAL)	The Data Services Template	x				x		x	x				
Liberty Alliance	ID-SIS	A collection of Identity Services Interface Specifications	x				x		x	x				
IETF/W3C	XaDES	XML Advanced Electronic Signatures							x			x		
IETF/W3C	XML-Dsig	Signature Syntax and Processing							x			x		
IETF/W3C	Canonical XML	Canonical XML							x			x		
IETF/W3C	Exclusive XML Canonicalization	Exclusive XML Canonicalization							x			x		
IETF/W3C	XPath Filter	Xpath Filter							x			x		
IETF/W3C	Additional XML Security URIs	Additional XML Security URIs							x			x		
IETF/W3C	XML Signature Requirements	XML Signature Requirements							x			x		
IETF	SSL	Secure Sockets Layer	x											
IETF	TLS	The Transport Layer Security Protocol Version 1.0	x											
IETF	LDAP	Lightweight Directory Access Protocol	x	x	x		x	x	x	x	x	x		



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number									Comment/Notes	
			1	2	3	4	5	6	7	8	9		11
IETF	X.500	The CCITT and ISO standard for electronic directory services	x	x	x		x	x	x	x	x		
IETF	RFC 3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	x	x	x		x	x	x	x	x		
IETF		MIME Security with Open PGP	x				x				x		
IETF		Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)							x				
IETF		AES Ciphersuites for TLS	x										
IETF		Upgrading to TLS Within HTTP/1.1	x										
IETF	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	x	x	x		x	x	x	x	x		
IETF	RFC 1510	Kerberos Authentication Service							x				
IETF	RFC 1777	Lightweight Directory Access Protocol (v2)		x		x	x	x	x	x	x		
IETF	RFC 1964	Kerberos v5 GSS-API Mechanism							x				
IETF	RFC 2025	GSS-API Simple Public Key Mechanism (SPKM)							x				
IETF	RFC 2743	Generic Security Service Application Program Interface Version 2, Update 1							x				
IETF	RFC 2246	The TLS Protocol Version 1.0	x										
IETF	RFC 3546	Transport Layer Security (TLS) Extensions	x										
IETF	RFC 3377	Lightweight Directory Access Protocol (v3): Technical Specification		x		x	x	x	x	x	x		
IETF	RFC 3771	The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message		x		x	x	x	x	x	x		
IETF	RFC 2259	Internet X.509 Public Key Infrastructure Operational Protocols—LDAPv2	x	x	x	x	x	x	x	x	x		
IETF	RFC 2401	Security Architecture for the Internet Protocol	x	x				x	x	x			
IETF	RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP.											
IETF	RFC 2402	IP Authentication Header							x				
IETF	RFC 2403	The Use of HMAC-MD5-96 within ESP and AH						x					
IETF	RFC 2404	The Use of HMAC-SHA-196 within ESP and AH						x					
IETF	RFC 2406	IP Encapsulating Security Payload (ESP)	x						x	x			
IETF	RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	x						x	x			
IETF	RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	x						x	x			



Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number											Comment/ Notes
			1	2	3	4	5	6	7	8	9	11		
IETF	RFC 2409	The Internet Key Exchange (IKE)	x							x	x			
IETF	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework					x							
IETF	RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol	x	x	x		x	x	x	x	x			
IETF	RFC 3852	Cryptographic Message Syntax (CMS).	x	x	x		x	x	x	x	x			
IETF	RFC 2631	Diffie-Hellman Key Agreement Method	x							x	x			
IETF	RFC 3881	Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications		X										
ISO	ISO/IEC 10536-1,2,3	Identification Cards -- Contactless integrated circuit(s) cards					x		x					
ISO	ISO/IEC 1443-1,2,3	Identification Cards -- Contactless integrated circuit(s) cards -- Proximity cards					x		x					
ISO	ISO/IEC 15693	Identification Cards -- Contactless integrated circuit(s) cards -- Vicinity cards					x		x					
ISO	ISO 10166-1,2	Information Technology -- Text and office systems -- Document Filing and Retrieval (DFR)									x			
ISO	ISO 9594-1,2	Information Technology -- Open Systems Interconnection -- The Directory	x	x	x		x	x	x	x	x			
ISO	ISO 9796-2,1	Information Technology -- Security techniques -- Digital signature schemes giving message recovery			x	x		x				x		
ISO	ISO/IEC 10164-1,2	Information Technology -- Open Systems Interconnection -- Systems Management	x	x						x	x		x	
ISO	ISO/IEC 10164-7	Information Technology--Open Systems Interconnection--Systems Management: Security Alarm Reporting Function		x										
ISO	ISO/IEC 10164-8	Information Technology--Open Systems Interconnection--Systems Management: Security Audit Trail Function		x										
ISO	ISO/IEC 10736	Information Technology -- Telecommunications and information exchange between systems -- Transport layer security protocol	x											
ISO	ISO/IEC 11577	Information Technology -- Open Systems Interconnection -- Network layer security protocol	x											
ISO	ISO 15408	Common Criteria Toolkit	x	x			x	x	x	x	x	x	x	
ISO	ISO/IEC 9594-8	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks				x	x	x	x	x	x			



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number									Comment/Notes	
			1	2	3	4	5	6	7	8	9		11
ANSI/Xn	ANSI X9.30 Part 1:	Public Key Cryptography for the Financial Services Industry - Part 1: The Digital Signature Algorithm (DSA) (technically aligned with NIST FIPS PUB 186)				x	x	x	x	x	x		
ANSI/Xn	ANSI X9.30 Part 2:	Public Key Cryptography for the Financial Services Industry - Part 2: The Secure Hash Algorithm (SHA-1)				x	x	x	x	x	x		
ANSI/Xn	ANSI X9.30 Part 3:	Certificate Management for DSA				x	x	x	x	x	x		
ANSI/Xn	ANSI X9.31	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) (technically aligned with ISO/IEC 9796)				x	x	x	x	x	x		
ANSI/Xn	ANSI X9.45:	Enhanced Management Controls Using Digital Signatures and Attribute Certificates				x	x	x	x	x	x		
ANSI/Xn	X12.58	Security Structures (version 2)	x							x			
ANSI/Xn	X9.52	Triple Data Encryption Algorithm Modes of Operation	x										
ECMA	ECMA1-219	Authentication and Privilege Attribute Security Applications with Related Key Distribution Functions							x	x			
FIPS	FIPS 140-2	Security Requirements for Cryptographic Modules. FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules	x				x		x		x		
FIPS	FIPS PUB 180-2	Secure Hash Standard (SHS)				x		x			x		
FIPS	FIPS PUB 181:	Secure Hash Standard, 1994 (technically aligned with ANSI X9.30-1)	x						x				
IEEE	IEEE 802.10	Interoperable LAN/MAN Security (SILS), 1992-1996 (multiple parts)	x										
IEEE	IEEE 802.11	Wireless LANs	x										
ITU	ITU-T X.501	Information Technology Open Systems Interconnection—The Directory: Models	x	x	x		x	x	x	x	x		
RSA Laboratories	PKCS #1:	RSA Cryptography Standard					x						
RSA Laboratories	PKCS #8:	Private-Key Information Syntax Standard			x	x		x			x		
RSA Laboratories	PKCS #11:	Cryptographic Token Interface Standard	x			x	x		x				
RSA Laboratories	PKCS #12:	Personal Information Exchange Syntax Standard	x				x						
IHE	ATNA	Audit Trail and Node Authentication Profile	x	x									



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number									Comment/Notes	
			1	2	3	4	5	6	7	8	9		11
IHE	DSG	Document Digital Signature			x	x		x			x		
IHE	XUA	Cross-Enterprise User Authentication							x				
IHE	EUA	Enterprise User Authentication							x				
IHE	BPPC	Patient Consent			x	x							
IHE	CT	Consistent Time										x	
Health Level Seven	HL7 v3 RBAC vocabulary	V3 Role based access control			x					x			
Health Level Seven	HL7 EHR-S	EHR functional Criteria: Conformance Criteria	x	x	x	x	x	x	x	x	x	x	
Health Level Seven	HL7 v3	Medical Records: Consent Topic			x	x				x	x		
NIST	FIPS 140-2	Security Requirements for Cryptographic Modules (May 2001)	x					x				x	
NIST	FIPS 180-2	Secure Hash Standard (SHS) (Aug 2002)						x					
NIST	FIPS 186-2	Digital Signature Standard (technically aligned with ANSI X9.30-1)						x	x			x	
NIST	FIPS 197	Advanced Encryption Standard (Nov 2001)								x			
NIST	FIPS 198	The Keyed-Hash Message Authentication Code (HMAC) (Mar 2002)	x					x				x	
NIST	SP 800-15	Minimum Interoperability Specification for PKI Components Version 1 (Sept 1997)	x				x						
NIST	SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations (June 2005)	x										
NIST	SP 800-53	Recommended Security Controls for Federal Information Systems (Dec 2006)	x	x			x	x	x	x	x	x	
NIST	SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (Apr 2006)	x						x				
NIST	SP 800-66	An Introductory Resource Guide for Implementing the HIPAA Security Rule	x	x			x	x	x	x	x		
NIST	SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (May 2004)	x								x		
NIST	SP 800-77	Guide to IPsec VPNs (Dec 2005)	x								x		
NIST	SP 800-81	Secure Domain Name System (DNS) Deployment Guide (May 2006)	x										
NIST	SP 800-92	Guide to Security Log Management (Sep 2006)		x									
NIST	SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS) (Feb 2007)		x									



**HITSP Security and Privacy Requirements, Design and Standards Selection
for BIO, EHR-Lab, and CE Use Cases**

Review Copy
20070413 V1.0

Standards Organization	Designation	Standard Name	Key Capability/Potential Construct Number											Comment/Notes
			1	2	3	4	5	6	7	8	9	11		
NIST	SP 800-95	Guide to Secure Web Services (Draft)	x	x			x			x		x		
NIST	SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (Feb 2007)	x							x				

4.2 GAPS WHERE THERE ARE NO STANDARDS

This section will describe gaps in standards. Gaps occur in the following two cases, where HITSP has:

- Identified requirements derived from the context that have no standards that meet all tiers of HITSP criteria to merit endorsement for that context
- Identified a single standard that encompasses and singly fulfills a set of tightly-coupled standards from the given context, yet is lacking in fulfilling one or more of the tightly-coupled requirements

The gap is only relative to a specific Use Case event. Recommended resolutions will be developed through a series of steps including the Technical Committee or Work Group's initial recommendations, cross team validation of the gap, provisional recommendations and peer review by the team. Gaps will be documented after the Tier 2 standards selection criteria have been applied.

The table below identifies the Use Case events and known associated gaps, along with the recommended resolutions.

Table 4.2-1 Use Case Events and Associated Gaps

Event Code	Event Description	Identified Gaps	Recommended Resolution
		Gaps will be documented after the Tier 2 standards selection criteria has been applied	

4.3 STANDARD OVERLAPS

This section will describe the instances where there are overlaps among standards for the Use Case. The overlap is only relative to the specific Use Case event. Overlaps refer to instances where some of the requirements are met by multiple standards. The overlap is only relative to the specified Use Case event. Recommended resolutions will be developed through a series of steps including the Committee's initial recommendations, cross team validation of the overlap, provisional recommendations and peer review by the team. Standard overlaps will be documented after the Tier 2 standards selection criteria have been applied.



Table 4.3-1 Standard Overlaps

Event Code	Event Description	Standard Overlap	Recommended Resolution
		Standard overlaps will be documented after the Tier 2 standards selection criteria has been applied	

REVIEW COPY



5.0 NEXT STEPS

The first step in the HITSP harmonization process is requirements analysis and design. Upon completion of the Requirements, Design and Standards Selection document for security and privacy, the following steps will occur:

- This document will be submitted to the HITSP Panel and interested Public for comment
- After the comment period, the Technical Committee will disposition the comments, maintaining a written log of all dispositions assigned to the TC
- Persuasive comments will be used to inform the construction of the HITSP set of Security and Privacy constructs
- Non-persuasive comments or comments that are not applicable to the construction of the constructs will be deferred with reason/explanation (e.g., need additional information or further analysis during construction)
- In parallel to the steps described above, the Technical Committee will complete its selection of standards, to be published as an addendum to this document, and begin the construction of the Security and Privacy constructs



6.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

6.1 DESCRIPTION OF CANDIDATE STANDARDS

The following table contains descriptions of the candidate standards.

Table 6.1-1 Description of Candidate Standards

Designation	Standard Name	Description
DTS	Classification of safety risk from health informatics products	
ISO 9735-2	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 2: Syntax rules specific to batch EDI	This part of the International Standard ISO 9735 specifies syntax rules specifically for the formatting of batch messages to be interchanged between computer application systems. For the transfer of packages in a batch environment.
ISO 9735-4	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 4: Syntax and service report message for batch EDI (message type -- CONTRL)	This part of the International Standard ISO 9735 defines the syntax and service report message for batch EDI, CONTRL.



Designation	Standard Name	Description
TS21091	Health informatics -- Directory services for security, communications and identification of professionals and patients	This Technical Specification defines minimal specifications for directory services for healthcare using the X.500 framework. This Technical Specification provides the common directory information and services needed to support the secure exchange of healthcare information over public networks. This Technical Specification addresses the health directory from a community perspective in anticipation of supporting inter-enterprise, inter-jurisdiction, and international healthcare communications. Besides technical security measures that are discussed in other ISO standards, communication of healthcare data requires a reliable accountable "chain of trust." In order to maintain this chain of trust within a public key infrastructure, users (relying parties) must be able to obtain current correct certificates and certificate status information through secure directory management. In addition to the support of security services such as access control and confidentiality, a standard shall provide specification for other aspects of communication, such as addresses and protocols of communication entities. This Technical Specification also supports directory services aiming to support identification of health professionals and organizations and the patients/consumers. The latter services include aspects sometimes referred to as master patient indices. The healthcare directory will only support standard LDAP Client searches. Specific implementation guidance, search criteria and support are out of scope of this document.
TS26000 part1,2	Health informatics - Privilege Management and Access Control	
(currently DTS, previously published as DR) DTS 21089	Trusted end-to-end information flows	
Additional XML Security URIs	Additional XML Security URIs	



Designation	Standard Name	Description
ANSI INCITS 100-	Information Systems - Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation with Packet-Switched Data Communications Networks (PSDN), or between Two DTEs, by Dedicated Circuit	Conforms to the requirements of CCITT Recommendation X.25, ISO 7776:1986, and ISO 8208:1987, and covers both the DTE/DCE and DTE/DTE interfaces.
ANSI X9.30 Part 1:	Public Key Cryptography for the Financial Services Industry - Part 1: The Digital Signature Algorithm (DSA) (technically aligned with NIST FIPS PUB 186)	Defines a method for digital signature generation and verification for the protection of messages and data using the Digital Signature Algorithm (DSA). This standard is used in conjunction with the hash function, as defined in American National Standard for Public Key Cryptography - Part 2: The Secure Hash Algorithm (SHA-1), BSR X9.30.2. In addition, this standard provides the criteria for the generation of public and private keys that are required by the algorithm and the procedural controls required for the secure use of the algorithm. Specific sections include definitions and common abbreviations, application, the DSA, Generation of Primes for the DSA, Random Number Generation for the DSA.
ANSI X9.30 Part 2:	Public Key Cryptography for the Financial Services Industry - Part 2: The Secure Hash Algorithm (SHA-1)	Produces a 160-bit representation of the message, called the message digest, when a message with a bit length less than 2^{64} is input. The message digest is used during the generation of a signature for the message. The message digest is computed during the generation of a signature for the message. The SHA-1 is also used to compute a message digest for the received version of the message during the process of verifying the signature. Any change to the message in transit will, with a very high probability, result in a different messages digest, and the signature will fail to verify. The Secure Hash Algorithm (SHA-1) described in this standard is required for use with the Digital Signature Algorithm and may be used whenever a secure hash algorithm is required.



Designation	Standard Name	Description
ANSI X9.30 Part 3:	Certificate Management for DSA	
ANSI X9.31	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) (technically aligned with ISO/IEC 9796)	Covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry.
ANSI X9.45:	Enhanced Management Controls Using Digital Signatures and Attribute Certificates	Defines strategies for reducing the security and financial risks associated with electronic business systems using digital signatures. Attribute certificates would be used to convey authorizations and restrictions that inform verifiers when an entity's signature would be considered valid. Attributes might include specified dollar amounts, cosignature requirements, preapproved counterparties, confirm to (address), and time of day. The benefits of this standard are cost reduction, enhanced security, greater manageability, and greater flexibility for business transactions.
ATNA	Audit Trail and Node Authentication Profile	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements.



Designation	Standard Name	Description
BPPC	Patient Consent	Basic Patient Privacy Consents (BPPC) enables XDS Affinity Domains to be more flexible in the privacy policies that they support by providing mechanisms to record patient privacy consents, enforce these consents, and create Affinity Domain defined consent vocabularies that identify information sharing policies.
Canonical XML	Canonical XML	Canonical XML [XML-C14N] specifies a standard serialization of XML that, when applied to a subdocument, includes the subdocument's ancestor context including all of the namespace declarations and attributes in the "xml:" namespace. However, some applications require a method which, to the extent practical, excludes ancestor context from a canonicalized subdocument. For example, one might require a digital signature over an XML payload (subdocument) in an XML message that will not break when that subdocument is removed from its original message and/or inserted into a different context. This requirement is satisfied by Exclusive XML Canonicalization.
CT	IT Infrastructure Technical Framework (Consistent Time)	The Consistent Time Integration Profile defines mechanisms to synchronize the time base between multiple actors and computers. Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time Profile provides a median synchronization error of less than 1 second.
DICOM Part 15:	Security and System Management Profiles	This Standard specifies Security and System Management Profiles to which implementations may claim conformance. Security and System Management Profiles are defined by referencing externally developed standard protocols, such as TLS, ISCL, DHCP, and LDAP, with attention to their use in a system that uses DICOM Standard protocols for information interchange.
DSG	Document Digital Signature	The Document Digital Signature (DSG) content profile specifies the use of digital signatures for documents that are shared between organizations. This is an infrastructure document content profile that does not include specific workflow (ie: e-prescription and patient referrals). This document provides an infrastructure which may be further managed by their relative domains to ensure cohesiveness. The infrastructure to do the signing, verification, and identity



Designation	Standard Name	Description
		management exists and is not defined in this document content profile. The specific Private Key Infrastructure (PKI) is not identified by this profile. Whichever infrastructure is selected shall adhere to ISO TS-17090 standards for PKI in healthcare.
DTR	TR Assuring patient safety of health informatics products	
DTS21298	Health informatics: Functional and Structural Roles	
DTS25237	Health informatics: Pseudonymisation	
E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)	This guide covers a set of requirements outlining the properties of a national system creating a universal healthcare identifier (UHID). Use of the UHID is expected to be limited to the population of the United States. This guide sets forth the fundamental considerations for a UHID that can support at least four basic functions effectively: (1) Positive identification of patients when clinical care is rendered; (2) Automated linkage of various computer-based records on the same patient for the creation of lifelong electronic healthcare files; (3) Provision of a mechanism to support data security for the protection of privileged clinical information; and (4) The use of technology for patient records handling to keep healthcare operating costs at a minimum.
E1762	Standard Guide for Electronic Authentication of Healthcare Information	This guide covers defining a document structure for use by electronic signature mechanisms. Describing the characteristics of an electronic signature process. Defining minimum requirements for different electronic signature mechanisms. Defining signature attributes for use with electronic signature mechanisms. Describing acceptable electronic signature mechanisms and technologies. Defining minimum requirements for user identification, access control, and other security requirements for electronic signatures and outlining technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism.



Designation	Standard Name	Description
E1869	Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records	This guide covers the principles for confidentiality, privacy, access, and security of person identifiable health information. The focus of this standard is computer-based systems; however, many of the principles outlined in this guide also apply to health information and patient records that are not in an electronic format. Basic principles and ethical practices for handling confidentiality, access, and security of health information are contained in a myriad of federal and state laws, rules and regulations, and in ethical statements of professional conduct. The purpose of this guide is to synthesize and aggregate into a cohesive guide the principles that underpin the development of more specific standards for health information and to support the development of policies and procedures for electronic health record systems and health information systems.
E1985	Standard Guide for User Authentication and Authorization	This guide covers mechanisms that may be used to authenticate healthcare information (both administrative and clinical) users to computer systems, as well as mechanisms to authorize particular actions by users. These actions may include access to healthcare information documents, as well as specific operations on those documents (for example, review by a physician). This guide addresses both centralized and distributed environments, by defining the requirements that a single system shall meet and the kinds of information which shall be transmitted between systems to provide distributed authentication and authorization services. This guide addresses the technical specifications for how to perform user authentication and authorization. The actual definition of who can access what is based on organizational policy.
E1986	Standard Guide for Information Access Privileges to Health Information	This guide covers the process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider, and organizational data in the healthcare domain. It addresses a wide range of data and data elements not all traditionally defined as healthcare data, but all elemental in the provision of data management, data services, and administrative and clinical healthcare services. In addition, this guide addresses specific requirements for granting access privileges to patient-specific health information during health emergencies.



Designation	Standard Name	Description
E1987	Standard Guide for Individual Rights Regarding Health Information	This guide outlines the rights of individuals, both patients and providers, regarding health information and recommends procedures for the exercise of those rights. This guide is intended to amplify Guide E 1869.
E1988	Standard Guide for Training of Persons who have Access to Health Information	This guide addresses the privacy, confidentiality, and security training of employees, agents and contractors who have access to health information. This access shall be authorized and required to meet job responsibilities. Training is essential to developing an understanding about, and sensitivity for, individually identifiable health information. Anyone in a setting that collects, maintains, transmits, stores or uses health information, or provides health services, or a combination thereof, shall provide privacy, confidentiality, and security awareness training to all staff and business.
E2017	Standard Guide for Amendments to Health Information	This guide addresses the criteria for amending individually-identifiable health information. Certain criteria for amending health information are found in federal and state laws, rules and regulations, and in ethical statements of professional conduct.
E2084	Standard Specification for Authentication of Healthcare Information Using Digital Signatures	This specification covers the use of digital signatures to provide authentication of healthcare information, as described in Guide E 1762. It describes how the components of a digital signature system meet the requirements specified in Guide E 1762. This includes specification of allowable signature and hash algorithms, management of public and private keys, and specific formats.
E2085	Standard Guide on Security Framework for Healthcare Information	This guide covers a framework for the protection of healthcare information. It addresses both storage and transmission of information. It describes existing standards used for information security which can be used in many cases, and describes which (healthcare-specific) standards are needed to complete the framework. Appropriate background information on security (and particularly cryptography) is included. The framework is designed to accommodate a very large (national or international), distributed user base, spread across many organizations, and it therefore recommends the use of certain (scaleable) technologies over others.



Designation	Standard Name	Description
E2086	Standard Guide for Internet and Intranet Healthcare Security	This guide covers mechanisms that can be used to protect healthcare information which is being transmitted over networks using the Internet Protocol Suite (IPS). This includes the actual Internet itself, as well as corporate intranets constructed from off-the-shelf components implementing these protocols. An organization's security policy will determine when these mechanisms are used, based on risk analysis.
E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems	This specification is for the development and implementation of security audit/disclosure logs for health information. It specifies how to design an access audit log to record all access to patient identifiable information maintained in computer systems and includes principles for developing policies, procedures, and functions of health information logs to document all disclosure of health information to external users for use in manual and computer systems. The process of information disclosure and auditing should conform, where relevant, to the Privacy Act of 1974 (1).
E2212-02a	Standard Practice for Healthcare Certificate Policy	This practice covers a policy ("the policy") for digital certificates that support the authentication, authorization, confidentiality, integrity, and non-repudiation requirements of persons and organizations that electronically create, disclose, receive, or otherwise transact health information.
ECMA1-219	Authentication and Privilege Attribute Security Applications with Related Key Distribution Functions	



Designation	Standard Name	Description
EUA	Enterprise User Authentication	This Integration Profile is a means to establish one name per user that can then be used on all of the devices and software that participate in this integration profile, greatly facilitating centralized user authentication management and providing users with the convenience and speed of a single sign-on. This profile leverages Kerberos (RFC 1510) and the HL7 CCOW standard (user subject).
Exclusive XML Canonicalization	Exclusive XML Canonicalization	Canonical XML [XML-C14N] specifies a standard serialization of XML that, when applied to a subdocument, includes the subdocument's ancestor context including all of the namespace declarations and attributes in the "xml:" namespace. However, some applications require a method which, to the extent practical, excludes ancestor context from a canonicalized subdocument. For example, one might require a digital signature over an XML payload (subdocument) in an XML message that will not break when that subdocument is removed from its original message and/or inserted into a different context. This requirement is satisfied by Exclusive XML Canonicalization.
FIPS 140-2	Security Requirements for Cryptographic Modules. FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules	This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.



Designation	Standard Name	Description
FIPS 201	Personal ID Verification of Federal Employees & Contractors	<p>This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card.</p>
FIPS PUB 112	Password Usage	<p>This standard identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system.</p>
FIPS PUB 180-2	Secure Hash Standard (SHS)	<p>This standard specifies four secure hash algorithms - SHA-1, SHA-256, SHA-384, and SHA-512 - for computing a condensed representation of electronic data (message). When a message of any length < 264 bits (for SHA-1 and SHA-256) or < 2128 bits (for SHA-384 and SHA-512) is input to an algorithm, the result is an output called a message digest.</p>



Designation	Standard Name	Description
FIPS PUB 181:	Secure Hash Standard, 1994 (technically aligned with ANSI X9.30-1)	This Automated Password Generator Standard specifies an algorithm to generate passwords for the protection of computer resources. This standard is for use in conjunction with FIPS PUB 112, Password Usage Standard, which provides basic security criteria for the design, implementation, and use of passwords. The algorithm uses random numbers to select the characters that form the random pronounceable passwords. The random numbers are generated by a random number subroutine based on the Electronic Codebook mode of the Data Encryption Standard (DES) (FIPS PUB 46-1). The random number subroutine uses a pseudorandom DES key generated in accordance with the procedure described in Appendix C of ANSI X9.17.
FIPS PUB 186-2:	Digital Signature Standard (technically aligned with ANSI X9.30-1)	This standard specifies algorithms appropriate for applications requiring a digital, rather than written, signature.
FIPS PUB 190	Guideline for Use of Advanced Authentication Technology Alternatives	This guideline describes the primary alternative methods for verifying the identities of computer system users, and provides recommendations to Federal agencies and departments for the acquisition and use of technology which supports these methods.
FIPS PUB 197	Advanced Encryption Standard (AES)	This standard specifies the Rijndael algorithm ([3] and [4]), a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard. The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".
FIPS PUB 198	The Keyed-Hash Message Authentication Code (HMAC)	This standard specifies an algorithm for applications requiring message authentication. Message authentication is achieved via the construction of a message authentication code (MAC). MACs based on cryptographic hash functions are known as HMACs. The HMAC specification in this standard is a generalization of HMAC as specified in Internet RFC 2104, HMAC, Keyed-Hashing for Message Authentication, and ANSI X9.71, Keyed Hash Message Authentication Code.



Designation	Standard Name	Description
FIPS PUB 46-2	Data Encryption Standard (DES)	This publication specifies a FIPS approved cryptographic algorithm as required by FIPS 140-1. This publication provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.
FIPS PUB 46-3	Data Encryption Standard (DES)	The Data Encryption Standard (DES) specifies two FIPS approved cryptographic algorithms as required by FIPS 140-1. When used in conjunction with American National Standards Institute (ANSI) X9.52 standard, this publication provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specify both enciphering and deciphering operations which are based on a binary number called a key.
FIPS PUB 74	Guidelines for Implementing and Using the NBS Data Encryption Standard	This publication provides guidelines to be used by Federal organizations when these organizations specify that cryptographic protection is required for sensitive or valuable computer data, Protection of computer data during transmission between electronic components or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by that data. These guidelines are to be applied in conjunction with FIPS PUB 46 and FIPS PUB 81 when implementing and using the Data Encryption Standard.
FIPS PUB 81	DES Modes of Operation	This publication defines four modes of operation for the DES which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.



Designation	Standard Name	Description
HL7	DSTU RBAC	
HL7 EHR-S	EHR Functional Criteria: Conformance Criteria	The HL7 EHR System Functional Model provides a reference list of over 160 functions that may be present in an Electronic Health Record System (EHR-S). The function list is described from a user perspective with the intent to enable consistent expression of system functionality. This EHR-S Functional Model, through the creation of Functional Profiles, enables a standardized description and common understanding of functions sought or available in a given setting (e.g. intensive care, cardiology, office practice in one country or primary care in another country).
HL7 v3	Medical Records: Consent Topic	
HL7 v3 ATS	Abstract Transport Specification	
HL7 v3 RBAC vocabulary	V3 Role Based Access Control	
ID-FF 1.2 (FINAL)	Identity Federation Framework	Liberty Identity Federation Framework (ID-FF), offers a viable approach for implementing such a single sign-on with federated identities. It establishes a standardized, multi-vendor, Web-based single sign-on with simple federated identities based on today's commonly deployed technologies.
ID-SIS	Identity Services Interface Specifications	The Liberty Identity Service Interface Specification (ID-SIS) uses the Web Services Framework (ID-WSF) and Federation Framework (ID-FF) specifications to provide networked identity services, such as contacts, presence detection, or wallet services that depend on networked identity.
ID-WSF 1.1 (FINAL)	Identity Web Services Framework	The Liberty Identity Web Services Framework defines a SOAP based invocation framework with a layered architecture. The framework does not specify any contents for the SOAP body, allowing the development of identity services within the context of the Liberty Identity Web Services Framework.
ID-WSF 2.0 (DRAFT)	Identity Web Services Framework, Draft Release 2	This specification defines a framework for describing and discovering web services in general and identity web services in particular. An identity web service is defined as a type of web service whose operations are indexed by identity. Such services maintain information about, or on behalf of, Principals—as represented by their identities—and/or perform actions on behalf of Principals.



Designation	Standard Name	Description
ID-WSF DST 2.0 (FINAL)	Data Services Template	Provides protocols for the querying and modifying of data attributes when implementing a data service using the Liberty Identity Web Services Framework (ID-WSF).
IEEE 802.11	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	This standard defines the protocol and compatible interconnection of data communication equipment via the "air", radio or infrared, in a local area network (LAN) using the carrier sense multiple access protocol with collision avoidance (CSMA/CA) medium sharing mechanism. The medium access control (MAC) supports operation under control of an access point as well as between independent stations. The protocol includes authentication, association, and re-association services, an optional encryption/decryption procedure, power management to reduce power consumption in mobile stations, and a point coordination function for time bounded transfer of data.
IEEE Std 1363-2000	IEEE Standard Specifications for Public-Key Cryptography	This standard specifies common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, and cryptographic schemes based on those primitives. It also specifies related cryptographic parameters, public keys, and private keys.
IEEE Std 1363a-2004	IEEE Standard Specifications for Public-Key Cryptography -- Amendment 1: Additional Techniques	This standard specifies common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, and cryptographic schemes based on those primitives.
IEEE Std 802.11i-2004	Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amend. 6: Medium Access Control (MAC) Security Enhancements	Enhanced security services and mechanisms for the IEEE 802.11 medium access control (MAC) beyond those features and capabilities provided by the wired equivalent privacy (WEP) mechanism of the base standard, IEEE Std 802.11, 1999 Edition, are defined in this amendment. This amendment retains the WEP feature for purposes of backwards compatibility with existing IEEE 802.11 devices, but WEP is deprecated in favor of the new security features provided in this amendment.



Designation	Standard Name	Description
IEEE Std 802.1X-2004	IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control	Port-based network access control makes use of the physical access characteristics of IEEE 802 Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.
IFC-3067	Incident Data Exchange Format Data Model and XML Implementation	
IS17090 part1,2,3	Health Informatics -- Public key infrastructure	
IS 22857	Health Informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information	ISO 22857:2004 provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organization should adopt to ensure compliance with those principles.
IS27799	Health Informatics: Security management in health using IS17799	
ISO/IEC 10166-1	Information technology -- Text and office systems -- Document Filing and Retrieval (DFR) -- Part 1: Abstract service definition and procedures	Specifies a client-server type model (according to ISO/IEC 10031-1), functions and services, a specific model for managing documents, the service using the principles established by ISO/IEC 10021-3, and the usage of other services.



Designation	Standard Name	Description
ISO/IEC 10166-2	Information technology -- Text and office systems -- Document Filing and Retrieval (DFR) -- Part 2: Protocol specification	Specifies: the abstract syntax of the access protocol; how the access protocol supports the abstract service as defined in ISO/IEC 10166-1; the mapping of the access protocol onto the services used; the requirements for conformance with the access protocol.
ISO 10181-1,2,3,4,5,6,7:	Information Technology -- Open Systems Interconnection -- Security frameworks for open systems	ISO/IEC 10181 series of standards address the application of security services in an Open Systems environment, where the term Open Systems is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. Specify a general framework for the provision of access control. Specify a non-repudiation framework. Specify a general framework for the provision of confidentiality services. Specify a general framework for the provision of integrity services. And specify a security audit and alarms framework
ISO 15000/1	Electronic business eXtensible Markup Language (ebXML) -- Part 1: Collaboration-protocol profile and agreement specification (ebCPP) (available in English only)	This specification contains the detailed definitions of the Collaboration-Protocol Profile (CPP) and the Collaboration-Protocol Agreement (CPA). As defined in the ebXML Business Process Specification Schema [ebBPSS], a Business Partner is an entity that engages in Business Transactions with another Business Partner(s). The Message-exchange capabilities of a Party MAY be described by a Collaboration-Protocol Profile (CPP). The Message-exchange agreement between two Parties MAY be described by a Collaboration-Protocol Agreement (CPA).
ISO 15000/2	Electronic business eXtensible Markup Language (ebXML) -- Part 2: Message service specification (ebMS) (available in English only)	This specification defines the ebXML Message Service Protocol enabling the secure and reliable exchange of messages between two parties. It includes descriptions of: <ul style="list-style-type: none"> • the ebXML Message structure used to package payload data for transport between parties, • the behavior of the Message Service Handler sending and receiving those messages over a data communications protocol. This specification is independent of both the payload and the communications protocol used.



Designation	Standard Name	Description
ISO 15000/3	Electronic business eXtensible Markup Language (ebXML) -- Part 3: Registry information model specification (ebRIM)	This document specifies the information model for the ebXML Registry.
ISO 15000/4	Electronic business eXtensible Markup Language (ebXML) -- Part 4: Registry services specification (ebRS) (available in English only)	This document defines the interface to the ebXML Registry Services as well as interaction protocols, message definitions and XML schema.
ISO 15408	Common Criteria Toolkit	ISO/IEC 15408 will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. It is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. It addresses protection of information from unauthorized disclosure, modification, or loss of use and is applicable to IT security measures implemented in hardware, firmware or software. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.



Designation	Standard Name	Description
ISO 7498-2	Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture	Provides a general description of security services and related mechanisms, which can be ensured by the Reference Model, and of the positions within the Reference Model where the services and mechanisms may be provided. Extends the field of application of ISO 7498 to cover secure communications between open systems. Adds to the concepts and principles included in ISO 7498 but does not modify them. Is not an implementation specification, nor a basis for assessing the conformance of actual implementations.
ISO 7816 -1,2,3,4,5,6	Identification cards -- Integrated circuit(s) cards with contacts	ISO 7816 is an international standard related to electronic identification cards, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). It is an extension of ISO 7810.
ISO 8824-1,2,3,4	Information technology -- Abstract Syntax Notation One (ASN.1)	ISO/IEC 8824 consists of the following parts, under the general title Information technology — Abstract Syntax Notation One (ASN.1): — Part 1: Specification of basic notation for the definition of data types and values. — Part 2: Information object specification. — Part 3: Constraint specification. — Part 4: Parameterization of ASN.1 specifications
ISO 8825-1,2,3,4,5	Information technology -- ASN.1 encoding rules	ISO/IEC 8825 consists of the following parts, under the general title Information technology — ASN.1 encoding rules: Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Part 2: Specification of Packed Encoding Rules (PER) Part 3: Specification of Encoding Control Notation (ECN) Part 4: XML Encoding Rules (XER) Part 5: Mapping W3C XML schema definitions into ASN.1



Designation	Standard Name	Description
ISO 8879	Information processing -- Text and office systems -- Standard Generalized Markup Language (SGML)	This International Standard: (1) Specifies an abstract syntax known as the Standard Generalized Markup Language (SGML). The language expresses the description of a document's structure and other attributes, as well as other information that makes the markup interpretable. (2) Specifies a reference concrete syntax that binds the abstract syntax to specific characters and numeric values, and criteria for defining variant concrete syntaxes. (3) Defines conforming documents in terms of their use of components of the language. (4) Defines conforming systems in terms of their ability to process conforming documents and to recognize markup errors in them. (5) Specifies how data not defined by this International Standard (such as images, graphics, or formatted text) can be included in a conforming document.
ISO 9594-2	Information technology -- Open Systems Interconnection -- The Directory: Models	ISO/IEC 9594-2:2001 provides a number of different models for the Directory as a framework for the other ITU-T Recommendations in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User view on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model
ISO 9735-1	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 1: Syntax rules common to all parts	This part of the International Standard ISO 9735 specifies common syntax rules for the formatting of batch and interactive messages to be interchanged between computer application systems. It includes the terms and definitions for all parts of ISO 9735.



Designation	Standard Name	Description
ISO 9735-3	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 3: Syntax rules specific to interactive EDI	This part of the International Standard ISO 9735 specifies syntax rules specifically for the transfer of interactive messages to be interchanged between computer application systems. For the transfer of packages in an interactive environment
ISO 9735-5	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)	This part of the International Standard ISO 9735 specifies syntax rules for EDIFACT security. It provides a method to address message/package level, group level and interchange level security for authenticity, integrity and non-repudiation of origin, in accordance with established security mechanisms.
ISO 9735-6	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 6: Secure authentication and acknowledgement message (message type - AUTACK)	This part of the International Standard ISO 9735 for EDIFACT security defines the secure authentication and acknowledgement message AUTACK.



Designation	Standard Name	Description
ISO 9735-7	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 7: Security rules for batch EDI (confidentiality)	This part of the International Standard ISO 9735 for batch EDIFACT security addresses message/package level, group level and interchange level security for confidentiality in accordance with established security mechanisms.
ISO 9735-8	Electronic data interchange for administration, commerce and transport (EDIFACT) -- Application level syntax rules (Syntax version number: 4, Syntax release number: 1) -- Part 8: Associated data in EDI	This part of the International Standard ISO 9735 specifies syntax rules for associated data in EDI to be interchanged between computer application systems. This provides a method to transfer data which cannot be carried by means of either a batch or interactive EDIFACT message. The data may be created by other applications (such as STEP, CAD, etc.), and is referred to in this part as associated data.
ISO 9796-2,1	Information technology -- Security techniques -- Digital signature schemes giving message recovery	ISO/IEC 9796-2 specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. The security of all three schemes is based on the difficulty of factorizing large numbers. All three schemes can provide either total or partial message recovery.
ISO/IEC 10164-1	Information technology -- Open Systems Interconnection -- Systems Management: Object Management Function	Defines a systems management function which may be used by an application process to interact for the purpose of systems management. Among others, establishes user requirements for the state management function, establishes a model that relates the services and generic definitions provided by this function to user requirements, defines the services provided by the function, specifies the protocol that is necessary in order to provide the services, defines the relationship between the service and management operations and notifications, defines relationships with other systems management functions.



Designation	Standard Name	Description
ISO/IEC 10164-2	Information technology -- Open Systems Interconnection -- Systems Management: State Management Function	Defines a systems management function which may be used by an application process to interact for the purpose of systems management. Among others, establishes user requirements for the state management function, establishes models that relate the service and generic definitions provided by this function to user requirements, defines the services provided by the function, specifies the protocol that is necessary in order to provide the services, defines the relationship between the service and management operations and notifications, defines relationships with other systems management functions.
ISO/IEC 10164-7	Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function	Establishes user requirements for the service definition needed to support the security alarm reporting function, defines the service provided by the security alarm reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, and specifies conformance requirements. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management.
ISO/IEC 10164-8	Information technology -- Open Systems Interconnection -- Systems Management: Security audit trail function	Establishes user requirements for the service definition needed to support the security audit trail reporting function, defines the service provided by the security audit trail reporting function, specifies the protocol that is necessary in order to provide the service, defines the relationship between the service and management notifications, defines relationships with other systems management functions, specifies conformance requirements.
ISO/IEC 10536-1,2,3	Identification cards -- Contactless integrated circuit(s) cards	This standard specifies the dimensions, location, nature and assignment of each of the coupling areas to be provided for interfacing slot or surface card coupling devices (CCDs) with contactless integrated circuit(s) cards (CICCs) of the ID-1 card type.



Designation	Standard Name	Description
ISO/IEC 10736	Information technology -- Telecommunications and information exchange between systems -- Transport layer security protocol	Defines the transport layer security protocol. Does not specify the management functions and protocols needed to support this security protocol. Defines a protocol which may be used for Security Association establishment. Specifies one algorithm for authentication and key distribution which is based on public key crypto systems.
ISO/IEC 11577	Information technology -- Open Systems Interconnection -- Network layer security protocol	Specifies a protocol to be used by End Systems and Intermediate Systems in order to provide security services in the Network layer, which is defined by CCITT Rec.X.213, ISO/IEC 8348 and ISO 8648. The protocol defined herein is called the Network Layer Security Protocol (NLSP).
ISO/IEC 11586 – 6	Information technology -- Open Systems Interconnection -- Generic upper layers security: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma	This International Standard defines a Protocol Implementation Conformance Statement (PICS) proforma for the detailed expression of the conformance requirements of ITU-T Rec.X.833 ISO/IEC 11586-4 and Annex D of ITU-T Rec.X.830 ISO/IEC 11586-1.
ISO/IEC 11586-1	Information technology -- Open Systems Interconnection -- Generic upper layers security: Overview, models and notation	This International Standard defines a set of generic facilities to assist in the provision of security services in OSI applications.
ISO/IEC 11586-2	Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) service definition	This International Standard specifies a set of generic facilities to assist in the provision of security services in application layer protocols. Relates to the Security Exchange Service Element (SESE) and defines the service. Identical to ITU-T Rec.X.831.



Designation	Standard Name	Description
ISO/IEC 11586-3	Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) protocol specification	This International Standard defines a set of generic facilities to assist in the provision of security services in application layer protocols. Relates to the Security Exchange Service Element (SESE) and contains the protocol specification. Identical to ITU-T Rec.X.832.
ISO/IEC 11586-4	Information technology -- Open Systems Interconnection -- Generic upper layers security: Protecting transfer syntax specification	This International Standard defines a set of generic facilities to assist in the provision of security services in OSI applications. Defines the protecting transfer syntax specification. Identical to ITU-T Rec. X.833.
ISO/IEC 11586-5	Information technology -- Open Systems Interconnection -- Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma	This International Standard defines a Protocol Implementation Conformance Statement (PICS) proforma for the detailed expression of the conformance requirements of ITU-T Rec. X.832 ISO/IEC 11586-3 and Annex C of ITU-T Rec. X.830 ISO/IEC 11586-1
ISO/IEC 1443-1,2,3	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards	ISO/IEC 14443-1 specifies the physical characteristics of proximity cards, (PICC). It applies to identification cards of the ID-1 card type operating in proximity of a coupling device. ISO/IEC 14443-2 describes the electrical characteristics of two types of contactless interface between a proximity card and a proximity coupling device. The interface includes power and bi-directional communication. ISO/IEC 14443-3 describes polling for PICCs entering the field of a PCD, the byte format and framing, the initial REQ and ATQ command content, methods to detect and communicate with one card among several cards (anticollision) and other parameters required to initialize communications between a proximity card and a proximity coupling device.



Designation	Standard Name	Description
ISO/IEC 15693	Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards	ISO/IEC 10536 specifies (1) The physical characteristics of contactless integrated circuit(s) cards, (CICCs). It applies to identification cards of the ID-1 card type. (2) The dimensions, location, nature and assignment of each of the coupling areas to be provided for interfacing slot or surface card coupling devices (CCDs) with contactless integrated circuit(s) cards, (CICCs). It applies to identification cards of the ID-1 card type.(3) The nature and characteristics of the fields to be provided for power and bi-directional communications between card coupling devices (CCDs) and contactless integrated circuit(s) cards of the ID-1 card type in slot or surface operations.
ISO/IEC 9594-1	Information technology -- Open Systems Interconnection -- The Directory: Overview of concepts, models and services	ISO/IEC 9594-1 includes specifications for how information about objects, e.g. persons, is organized, created, maintained and retrieved. It provides provisions for protecting stored information through authentication and access control specifications. It also introduces the concepts of the Directory and the DIB (Directory Information Base), and overviews the services and capabilities which they provide. It is intended to give an introduction to the other parts of ISO/IEC 9594. It is not an implementation specification.
ISO/IEC 9594-8	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8:2005 provides specifications for how information about objects, e.g. persons, is organized, created, maintained and retrieved. Multiple entities are likely deployed to provide the directory service. Communication amongst these entities is authenticated and/or encrypted. It specifies three frameworks and a number of data objects that can be used to authenticate and secure the communication between two entities, e.g. between two directory service entities or between a web browser and web server. The data objects can also be used to prove the source and integrity of data structures such as digitally signed documents.



Designation	Standard Name	Description
ISO/IEC 9595	Information technology -- Open Systems Interconnection -- Common management information service	This International Standard defines an Application Service Element (the Common Management Information Service Element), which may be used by an application process in a centralized or decentralized management environment to exchange information and commands for the purpose of systems management, as defined by the OSI Management Framework in CCITT Rec. X.700 ISO/IEC 7498-4. This Recommendation International Standard is positioned in the application layer of ITU-T Rec. X.200 ISO/IEC 7498-1 and is defined according to the model provided by ITU-T Rec. X.207 ISO/IEC 9545.
ITU-T X.501	Information Technology Open Systems Interconnection—The Directory: Models	This International Standard provides a number of different models for the Directory as a framework for the other ITU-T Recommendations in the X.500 series. The models are the overall (functional) model, the administrative authority model, generic Directory Information models providing Directory User and Administrative User views on Directory information, generic Directory System Agent (DSA) and DSA information models and operational framework and a security model.
LDAP	Lightweight Directory Access Protocol	An application protocol for querying and modifying directory services running over TCP/IP.
NIST MISPC	Minimum Interoperability Specification for PKI Components Version 1	The Minimum Interoperability Specification for PKI Components (MISPC) provides a basis for interoperation between public key infrastructure (PKI) components from different vendors.



Designation	Standard Name	Description
P1073.0.1.1	Health informatics - Point-of-care medical device communication - Technical report - Guidelines for the use of RF wireless technology	This Technical Report provides a current analysis of the issues related to the use of radio frequency (RF) wireless technologies for the transport of external communications both to and from point-of-care (PoC) medical devices. At the time of this Technical Report, several different RF wireless technologies exist that might be applicable, each with different capabilities and characteristics, and each in different stages of maturity, standardization, and active implementation within medical devices and within healthcare facilities. It is additionally recognized that RF technologies are rapidly evolving, and new options may become available (or sufficiently established) after the publication of this Technical Report offering significant (and possibly superior) solutions for certain PoC medical device data transport needs.
P1073.2.1.3	Health informatics - Point-of-care medical device communication - Application profile - Clinical context management (CCoM)	This is an extension to Standard IEEE 1073.2.1.1, MDAP Base Standard. The scope is the synchronization of medical device operational contextual information, particularly security-related, in RF wireless contexts; patient identification; and clinical patient care logistical, particularly Admit, Discharge, and Transfer (ADT) information.
P1073.3.5.3	Health informatics - Point-of-care medical device communication - Transport profile - RF wireless - Local area network (wLAN)	This project is a subset of project number 1073.3.5 (Health informatics - Point-of-care medical device communication – RF Wireless Profile – Framework and Overview). The scope of this standard is medical device data communication profiles based on IEEE 802.11 Standards, particularly IEEE 802.11b/g with sufficient Quality of Service and Security attributes for mobile medical device applications across emergency, critical, acute, and sub-acute care areas of hospitals. As a result, multiple subsets of IEEE 802.11, particularly IEEE 802.e (QoS) and IEEE 802.11i (Security); IEEE 802.3 (“Ethernet”), and widely-used Internet protocols, such as DHCP, TCP/ and UDP/IP; will be integrated.



Designation	Standard Name	Description
P1073.3.5.5	Health informatics - Point-of-care medical device communication - Transport profile - RF wireless - Wide area (Mobile Phone) Network (wWAN)	<p>This project is an extension of, and linked to, project number 1073.0.1.1 (Health informatics - Point-of-care medical device communication - Technical report - Guidelines for the use of RF wireless technology) and a further extension of project number 1073.3.5 (Health Informatics - Framework and Overview Structure for Wireless Medical Data Transport using Personal Area, Local Area, Wide Area, and other Wireless Networks). The scope of this standard is to identify recommended protocols as well as to evaluate expected performance for the transport of medical data between IEEE-1073 point-of-care (POC) and / or body worn sensors along wireless wide area networks (WWAN) via gateway devices (e.g., mobile phones, PDAs) to an end server or attending healthcare professional in a home-based or mobile health scenario. Recommendations are made with the goal of developing common protocols for plug-and-play compatibility between medical devices and WWAN gateway equipment. Point-of-care (POC) or body worn sensor data are envisioned to range from non-critical physiologic parameters used for general health maintenance to critical parameters.</p>
P1363	Standard Specifications for Public Key Cryptography (revision)	<p>This standard specifies common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, and digital signatures, and cryptographic schemes based on those primitives. It also specifies related cryptographic parameters, public keys and private keys. The purpose of this standard is to provide a reference for specifications of a variety of techniques from which applications may select.</p>
P1363.1	Standard Specification for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices	<p>IEEE P1363.1 will specify cryptographic techniques based on hard problems over lattices. These techniques may offer tradeoffs in operating characteristics when compared with the methods already specified in IEEE 1363-2000 and draft P1363a. It is also intended that P1363.1 provide a second-generation framework for the description of cryptographic techniques, as compared to the initial framework provided in 1363-2000 and draft P1363a.</p>



Designation	Standard Name	Description
P1363.2	Standard Specification for Password-Based Public-Key Cryptographic Techniques	P1363.2 will specify public-key cryptographic techniques specifically designed to securely perform password-based authentication and key exchange. These techniques provide a way to authenticate people and distribute high-quality cryptographic keys for people, while preventing off-line brute-force attacks associated with passwords. A resulting high quality key may be more confidently used in combination with other cryptographic methods, such as symmetric encryption methods and public-key encryption, identification, and digital signature methods. P1363.2 will provide a reference for a variety of such password-based techniques within a suitable framework. It is not the purpose of this project to mandate any particular set of password-based techniques or security requirements (including key sizes). Rather, the purpose is to provide: (1) a reference for specification of a variety of techniques from which applications may select, (2) the appropriate theoretic background, and (3) extensive discussion of security and implementation considerations so that a solution provider can choose appropriate security requirements.
P1363.3	Standard for Identity-Based Cryptographic Techniques using Pairings	Specifications of pairing-based cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption, signcryption, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys and private keys. Class of computer and communications systems is not restricted.
P1609.1	Standard for Wireless Access in Vehicular Environments (WAVE)-Resource Manager	This standard specifies a WAVE DSRC Application known as the WAVE Resource Manager designed to allow Applications at remote sites to communicate with devices known as Onboard Units that are mounted in vehicles, through devices known as Roadside Units, mounted on the roadside. The WAVE Resource Manager, acting like an Application Layer, multiplexes the communications of multiple remote Applications each communicating with multiple Onboard Units. The purpose of the communication is to conduct information interchange, needed to implement the requirements of the remote WAVE DSRC Applications.



Designation	Standard Name	Description
P1609.2	Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages	Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages defines secure message formats and processing. This standard also defines the circumstances for using secure message exchanges and how those messages should be processed based upon the purpose of the exchange.
P1619	Standard Architecture for Encrypted Shared Storage Media	IEEE P1619 is an Institute of Electrical and Electronics Engineers (IEEE) standardization project for encryption of the stored data. It includes specifications for: (1) Disk encryption standard P1619, using the XTS-AES (XEX-based Tweaked CodeBook mode (TCB) with CipherText Stealing (CTS); the proper name should be XTC (XEX TCB CTS), but it is already used to denote a drug). (2) Tape encryption standard P1619.1 using four AES cryptographic modes: Counter mode with CBC-MAC (CCM), Galois/Counter Mode (GCM), CBC-HMAC-SHA, and XTS-HMAC-SHA (3) Disk encryption standard P1619.2 using a wide-block cipher. Current candidates: XCB, EME*, TET. (4) Key management standard P1619.3 for storage devices. P1619 has also standardized the key backup in the XML format.
P1619.1	Standard Architecture for Encrypted Variable Block Storage Media	IEEE P1619.1 is an Institute of Electrical and Electronics Engineers (IEEE) standardization project for tape encryption standard using four AES cryptographic modes: Counter mode with CBC-MAC (CCM), Galois/Counter Mode (GCM), CBC-HMAC-SHA, and XTS-HMAC-SHA.
P1667	Standard Protocol for Authentication in Host Attachments of Transient Storage Devices	
P1700	Standard for Information System Security Assurance Architecture (ISSAA)	The IEEE Standards Project 1700 is developing a draft Standard for an Information System Security Assurance Architecture (ISSAA) for ballot and during the process begin development of a suite of associated standards that represent components of that architecture.



Designation	Standard Name	Description
P2200	Standard for Baseline Operating Systems Security (TM) (BOSS TM)	IEEE Project 2200: Develop a draft Standard for Baseline Operating System Security for ballot and during the process consider issues that may require other related standards. This project is dormant, awaiting the identification of a chair
P2600	Standard for Information Technology: Hardcopy System and Device Security	This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users and others on the selection, installation, configuration and usage of hardcopy devices and systems including printers, copiers, and multifunction devices and the computer systems that support these devices. This standard identifies security exposures for these hardcopy devices and systems and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems and instructs users on appropriate ways to use these security capabilities.
P802.11w	Amendment to Standard [FOR] Information Technology- Telecommunications and Information Exchange between systems-Local and Metropolitan networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Protected Management Frames	The proposed project seeks to create enhancements to the IEEE 802.11 Medium Access Control layer to provide, as appropriate, mechanisms that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 management frames including but not limited to: action management frames, de-authentication and disassociation frames.
P802.1AE	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security	To secure Local or Metropolitan Area Networks, the IEEE 802.1AE Media Access Control (MAC) Security Task Group has proposed the IEEE P802.1AE Standard for Local and Metropolitan Area Networks: MAC Security (MACsec). MACsec introduces a new tag field, Security TAG (SecTAG), in Layer 2 frames.



Designation	Standard Name	Description
P802.1af	Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control - Amendment 1: Authenticated Key Agreement for Media Access Control (MAC) Security	This is a project of the 802.1 MAC Security Task Group. It is an amendment to IEEE std 802.1X. This standard extends 802.1X to establish security associations for 802.1ae MAC Security, and provide media access method independent association discovery. This standard facilitates the use of additional industry standard authentication, authorization, and key management protocols. This standard will facilitate secure communication over publicly accessible LAN/MAN media for which security has not otherwise been defined, and allow the use of IEEE Std 802.1X, already widespread and supported by multiple vendors, in additional applications
PKCS #1:	RSA Cryptography Standard	Defines the format of RSA encryption.
PKCS #10:	Certification Request Syntax Standard	Format of messages sent to a certification authority to request certification of a public key.
PKCS #11:	Cryptographic Token Interface Standard	An API defining a generic interface to cryptographic tokens
PKCS #12:	Personal Information Exchange Syntax Standard	Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.
PKCS #13:	Elliptic Curve Cryptography Standard	PKCS #13, the elliptic curve cryptography standard is still under development. It will address many aspects of elliptic curve cryptography, including parameter and key generation and validation, digital signatures, public-key encryption, key agreement, and ASN.1 syntax.
PKCS #15:	Cryptographic Token Information Format Standard	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15.[1]
PKCS #3:	Diffie-Hellman Key Agreement Standard	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.



Designation	Standard Name	Description
PKCS #5:	Password-Based Cryptography Standard	This document provides recommendations for the implementation of password-based cryptography, covering key derivation functions, encryption schemes, message-authentication schemes, and ASN.1 syntax identifying the techniques. The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. They are particularly intended for the protection of sensitive information such as private keys, as in PKCS #8 [25]. It is expected that application standards and implementation profiles based on these specifications may include additional constraints.
PKCS #6:	Extended-Certificate Syntax Standard	Defines extensions to the old v1 X.509 certificate specification. Obsolete by v3 of the same.
PKCS #7:	Cryptographic Message Syntax Standard	Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is now based on RFC 3852, an updated Cryptographic Message Syntax Standard (CMS).
PKCS #8:	Private-Key Information Syntax Standard	This standard describes syntax for private-key information, including a private key for some public-key algorithm and a set of attributes. The standard also describes syntax for encrypted private keys. The intention of including a set of attributes is to provide a simple way for a user to establish trust in information such as a distinguished name or a top-level certification authority's public key.
PKCS #9:	Selected Attribute Types	Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PMI	Privilege Management Infrastructure	In an X.509 Privilege Management Infrastructure, the access rights are held within the privilege attributes of attribute certificates issued to users. Each privilege attribute within an AC will describe one or more of the user's access rights. A target resource will then read a user's AC to see if he is allowed to perform the action that he is requesting.



Designation	Standard Name	Description
prEN_13606-4	Health informatics — Electronic health record communication — Part 4: Security requirements and distribution rules	This document specifies security requirements and mechanisms for managing access-rights to components of an electronic health record (EHR) of a patient. Furthermore mechanisms for auditing accesses to an EHR are defined. This Standard therefore addresses the important aspects of data safety and security in the context of exchanging patient related medical information. The implementation and usability of the security functions of an EHR system is supported through the provision of easily implementable but course-grained general access policies, as well as mechanisms for defining fine-grained, individual access policies.
RFC 1510	Kerberos Authentication Service	Kerberos provides a means of verifying the identities of principals, (e.g., a workstation user or a network server) on an open (unprotected) network. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography, i.e., shared secret key. (shared secret key - Secret and private are often used interchangeably in the literature. In our usage, it takes two (or more) to share a secret, thus a shared DES key is a secret key. Something is only private when no one but its owner knows it. Thus, in public key cryptosystems, one has a public and a private key.)



Designation	Standard Name	Description
RFC 1777	Lightweight Directory Access Protocol (v2)	<p>The protocol described in this document is designed to provide access to the X.500 Directory while not incurring the resource requirements of the Directory Access Protocol (DAP). This protocol is specifically targeted at simple management applications and browser applications that provide simple read/write interactive access to the X.500 Directory, and is intended to be a complement to the DAP itself. Key aspects of LDAP are:</p> <ul style="list-style-type: none"> - Protocol elements are carried directly over TCP or other transport, bypassing much of the session/presentation overhead. - Many protocol data elements are encoding as ordinary strings (e.g., Distinguished Names). - A lightweight BER encoding is used to encode all protocol elements.
RFC 1901	Introduction to Community-based SNMPv2	The purpose of this standard is to define the Community-based Administrative Framework for the SNMP version 2 framework (SNMPv2). This framework is derived from the original Internet-standard Network Management Framework (SNMPv1), which consists of these three standards: RFC 1155, RFC 1212, RFC 1157
RFC 1902	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)	This document specifies an Internet standards track protocol. Operations of the protocol are carried out under an administrative framework which defines authentication, authorization, access control, and privacy policies.
RFC 1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)	This standard defines the initial set of textual conventions available to all Management Information Base (MIB) modules. These newly defined types are termed textual conventions, and are used for the convenience of humans reading the MIB module.
RFC 1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)	Management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. These modules are written using a subset of OSI's Abstract Syntax Notation One (ASN.1) [1], termed the Structure of Management Information (SMI) [2]. The purpose of this standard is to define the notation used for these purposes and to define the acceptable lower-bounds of implementation, along with the actual level of implementation achieved.



Designation	Standard Name	Description
RFC 1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)	The management protocol, version 2 of the Simple Network Management Protocol, provides for the exchange of messages which convey management information between the agents and the management stations. The form of these messages is a message "wrapper" which encapsulates a Protocol Data Unit (PDU). The purpose of this standard is to define the operations of the protocol with respect to the sending and receiving of the PDUs.
RFC 1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)	This standard defines how the SNMPv2 maps onto an initial set of transport domains. Although several mappings are defined, the mapping onto UDP is the preferred mapping. As such, to provide for the greatest level of interoperability, systems which choose to deploy other mappings should also provide for proxy service to the UDP mapping.
RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	This standard defines managed objects which describe the behavior of a SNMPv2 entity.
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework	The purpose of this standard is to describe coexistence between version 2 of the Internet-standard Network management Framework [1-6], termed the SNMP version 2 framework (SNMPv2), and the original Internet-standard Network Management Framework (SNMPv1)
RFC 1909	Administrative Infrastructure for SNMPv2	This standard defines an administrative framework for SNMPv2, which realizes effective management in a variety of configurations and environments.
RFC 1910	User-based Security Model for SNMPv2	The Administrative Infrastructure for SNMPv2 provides effective management in a variety of configurations and environments. This document defines the security model for this administrative framework. The enforcement of access rights requires the means to identify the entity on whose behalf a request is generated. This SNMPv2 security model identifies an entity on whose behalf an SNMPv2 message is generated as a "user".



Designation	Standard Name	Description
RFC 1964	Kerberos v5 GSS-API Mechanism	This specification defines protocols, procedures, and conventions to be employed by peers implementing the Generic Security Service Application Program Interface (as specified in RFCs 1508 and 1509) when using Kerberos Version 5 technology (as specified in RFC 1510).
RFC 2025	GSS-API Simple Public Key Mechanism (SPKM)	This specification defines protocols, procedures, and conventions to be employed by peers implementing the Generic Security Service Application Program Interface (as specified in RFCs 1508 and 1509) when using the Simple Public-Key Mechanism. Although the Kerberos Version 5 GSS-API mechanism [KRB5] is becoming established in many environments, it is important in some applications to have a GSS-API mechanism which is based on a public-key, rather than a symmetric-key, infrastructure.
RFC 2246	The TLS Protocol Version 1.0	This document specifies Version 1.0 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
RFC 2259	Simple Nomenclature Query Protocol (SNQP)	The Simple Nomenclature Query Protocol (SNQP) allows a client to communicate with a descriptive name service or other relational-style query service. The protocol is useful to services that search many data repositories for query responses. Clients can pose queries on relations, list descriptions of relations, and obtain advice on reducing the search time and cost of their queries. Clients are informed of the age of information in caches, and may request more recent information. SNQP provides support for graphical user interfaces. It also supports different types of comparison operators, so services can use SNQP with a variety of back-end servers, e.g. relational database servers, CCSO servers, and servers providing relational views of X.500. SNQP is an ASCII protocol in the request-reply style of SMTP. It was specifically designed for use with the Nomenclature name and information service, and has been useful elsewhere.



Designation	Standard Name	Description
RFC 2401	Security Architecture for the Internet Protocol	<p>This standard specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. This document does not address all aspects of IPsec architecture. The following fundamental components of the IPsec security architecture are discussed in terms of their underlying, required functionality.</p> <ul style="list-style-type: none"> a. Security Protocols -- Authentication Header (AH) and Encapsulating Security Payload (ESP) b. Security Associations -- what they are and how they work, how they are managed, associated processing c. Key Management -- manual and automatic (The Internet Key Exchange (IKE)) d. Algorithms for authentication and encryption
RFC 2402	IP Authentication Header	<p>The IP Authentication Header (AH) standard is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays. This latter, optional service may be selected, by the receiver, when a Security Association is established. (Although the default calls for the sender to increment the Sequence Number used for anti-replay, the service is effective only if the receiver checks the Sequence Number.) AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is somewhat piecemeal. AH may be applied alone, in combination with the IP Encapsulating Security Payload (ESP) [KA97b], or in a nested fashion through the use of tunnel mode.</p>



Designation	Standard Name	Description
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH	This standard specifies the use of MD5 [RFC-1321] combined with HMAC [RFC-2104] as a keyed authentication mechanism within the context of the Encapsulating Security Payload and the Authentication Header. The goal of HMAC-MD5-96 is to ensure that the packet is authentic and cannot be modified in transit. HMAC is a secret key authentication algorithm. Data integrity and data origin authentication as provided by HMAC are dependent upon the scope of the distribution of the secret key. If only the source and destination know the HMAC key, this provides both data origin authentication and data integrity for packets sent between the two parties; if the HMAC is correct, this proves that it must have been added by the source.
RFC 2404	The Use of HMAC-SHA-196 within ESP and AH	This standard specifies the use of SHA-1 [FIPS-180-1] combined with HMAC [RFC-2104] as a keyed authentication mechanism within the context of the Encapsulating Security Payload and the Authentication Header. The goal of HMAC-SHA-1-96 is to ensure that the packet is authentic and cannot be modified in transit. HMAC is a secret key authentication algorithm. Data integrity and data origin authentication as provided by HMAC are dependent upon the scope of the distribution of the secret key. If only the source and destination know the HMAC key, this provides both data origin authentication and data integrity for packets sent between the two parties; if the HMAC is correct, this proves that it must have been added by the source.
RFC 2406	IP Encapsulating Security Payload (ESP)	The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion, e.g., through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.



Designation	Standard Name	Description
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for security association management and cryptographic key establishment for the Internet. This framework consists of defined exchanges, payloads, and processing guidelines that occur within a given Domain of Interpretation (DOI). This document defines the Internet IP Security DOI (IPSEC DOI), which instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	This standard describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. A Security Association protocol that negotiates, establishes, modifies and deletes Security Associations and their attributes is required for an evolving Internet, where there will be numerous security mechanisms and several options for each security mechanism. The key management protocol must be robust in order to handle public key generation for the Internet community at large and private key requirements for those private networks with that requirement. The Internet Security Association and Key Management Protocol (ISAKMP) defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks). All of these are necessary to establish and maintain secure communications (via IP Security Service or any other security protocol) in an Internet environment.
RFC 2409	The Internet Key Exchange (IKE)	This standard describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI. This is a hybrid protocol. The purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner. Processes which implement this standard can be used for negotiating virtual private networks (VPNs) and also for providing a remote user from a remote site (whose IP address need not be known beforehand) access to a secure host or network.



Designation	Standard Name	Description
RFC 2440	OpenPGP Message Format	This standard provides all necessary information needed to develop interoperable applications based on the OpenPGP format. It discusses implementation issues necessary to avoid security flaws. Open-PGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP.
RFC 2451	The ESP CBC-Mode Cipher Algorithms	This document describes how to use CBC-mode cipher algorithms with the IPsec ESP (Encapsulating Security Payload) Protocol. It not only clearly states how to use certain cipher algorithms, but also how to use all CBC-mode cipher algorithms.
RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol	This standard specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	This document specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs. The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response. This protocol specifies the data that needs to be exchanged between an application checking the status of a certificate and the server providing that status.



Designation	Standard Name	Description
RFC 2616	Hypertext Transfer Protocol/1.1	The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers [47]. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.
RFC 2631	Diffie-Hellman Key Agreement Method	This standard standardizes one particular Diffie-Hellman variant, based on the ANSI X9.42 draft, developed by the ANSI X9F1 working group. Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. An algorithm for converting the shared secret into an arbitrary amount of keying material is provided. The resulting keying material is used as a symmetric encryption key. The Diffie-Hellman variant described requires the recipient to have a certificate, but the originator may have a static key pair (with the public key placed in a certificate) or an ephemeral key pair.
RFC 2634	Enhanced Security Services for S/MIME	This standard describes four optional security service extensions for S/MIME. The services are: - signed receipts - security labels - secure mailing lists - signing certificates Also described are the procedures and the attributes needed for the four services. Note that some of the attributes described in this document are quite useful in other contexts and should be considered when extending S/MIME or other CMS applications.
RFC 2743	Generic Security Service Application Program Interface Version 2, Update 1	The Generic Security Service Application Program Interface (GSS-API), Version 2, as defined by RFC- 2743 obsoletes [RFC-2078], making specific, incremental changes in response to implementation experience and liaison requests. It is intended, to become the basis for subsequent progression of the GSS-API specification on the standards track for providing security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments.



Designation	Standard Name	Description
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP.	This standard specifies an Internet standards track protocol for the Internet community. It describes TCP's use of packet drops as an indication of congestion. It also explains that with the addition of active queue management (e.g., RED) to the Internet infrastructure, where routers detect congestion before the queue overflows, routers are no longer limited to packet drops as an indication of congestion. Routers can instead set the Congestion Experienced (CE) code point in the IP header of packets from ECN-capable transports. It also describes when the CE code point is to be set in routers, and describes modifications needed to TCP to make it ECN-capable. Also described are the issues involving the use of ECN within IP tunnels, and within IPsec tunnels in particular.
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.



Designation	Standard Name	Description
RFC 3377	Lightweight Directory Access Protocol (v3): Technical Specification	The specification for the Lightweight Directory Access Protocol version 3 (LDAPv3) nominally comprises eight RFCs which were issued in two distinct subsets at separate times -- RFCs 2251 through 2256 first, then RFCs 2829 and 2830 following later. RFC 2251 through 2256 do not mandate the implementation of any satisfactory authentication mechanisms and hence were published with an "IESG Note" discouraging implementation and deployment of LDAPv3 clients or servers implementing update functionality until a Proposed Standard for mandatory authentication in LDAPv3 is published. RFC 2829 was subsequently published in answer to the IESG Note. The purpose of this document is to explicitly specify the set of RFCs comprising LDAPv3, and formally address the IESG Note through explicit inclusion of RFC 2829.
RFC 3546	Transport Layer Security (TLS) Extensions	This document describes extensions that may be used to add functionality to Transport Layer Security (TLS). It provides both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms. The extensions may be used by TLS clients and servers. The extensions are backwards compatible - communication is possible between TLS 1.0 clients that support the extensions and TLS 1.0 servers that do not support the extensions, and vice versa.
RFC 3629	UTF-8, a transformation format of ISO 10646	UTF-8 has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values.
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	This standard presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially need to be covered in a certificate policy or a certification practice statement.



Designation	Standard Name	Description
RFC 3771	The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message	This document defines and describes the Intermediate Response message, a general mechanism for defining single-request/multiple-response operations in Lightweight Directory Access Protocol (LDAP). The Intermediate Response message is defined in such a way that the protocol behavior of existing LDAP operations is maintained. This message is intended to be used in conjunction with the LDAP Extended Request and Extended Response to define new single-request/multiple-response operations or in conjunction with a control when extending existing LDAP operations in a way that requires them to return intermediate response information.
RFC 3850	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling.	This standard specifies conventions for X.509 certificate usage by Secure/Multipurpose Internet Mail Extensions (S/MIME) agents. This specification is compatible with the Cryptographic Message Syntax [CMS] in that it uses the data types defined by CMS. It also inherits all the varieties of architectures for certificate-based key management supported by CMS.
RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification.	This standard defines Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.1. S/MIME provides a consistent way to send and receive secure MIME data. Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size.
RFC 3852	Cryptographic Message Syntax (CMS).	This standard describes the Cryptographic Message Syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content. The CMS describes an encapsulation syntax for data protection. It supports digital signatures and encryption. The syntax allows multiple encapsulations; one encapsulation envelope can be nested inside another. Likewise, one party can digitally sign some previously encapsulated data. It also allows arbitrary attributes, such as signing time, to be signed along with the message content, and provides for other attributes such as countersignatures to be associated with a signature.



Designation	Standard Name	Description
RFC 3881	Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications	This standard defines the format of data to be collected and minimum set of attributes that need to be captured for security auditing in healthcare application systems. The format is defined as an XML schema, which is intended as a reference for healthcare standards developers and application designers. It consolidates several previous documents on security auditing of healthcare data.
SAML	Security Assertion Markup Language (SAML)	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1	This specification supports interoperability for a large scale PKI that issues, revokes and manages digital signature public key certificates, to allow the use of those signatures to replace handwritten signatures in government services, commerce, and legal proceedings, and to allow distant parties, who have no previous relationship, to reliably authenticate each other and conduct business. Such a PKI, and the certificates it requires, may be excessive for some applications, and other more streamlined certificates and protocols may be more appropriate for more specialized and restricted applications.
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations	This Special Publication provides guidance to the selection and implementation of the TLS protocol while making effective use of Federal Information Processing Standards (FIPS) approved cryptographic algorithms, and suggests that TLS 1.0 configured with FIPS based cipher suites is the appropriate secure transport protocol.



Designation	Standard Name	Description
SP 800-53	Recommended Security Controls for Federal Information Systems	<p>This publication provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:</p> <ul style="list-style-type: none"> • Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems; • Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems; • Promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and • Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.
SP 800-63	Electronic Authentication Guideline	<p>This recommendation provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.</p>



Designation	Standard Name	Description
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	<p>This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, and does not supplement, replace, or supersede the HIPAA Security Rule itself. While CMS mentioned several of these publications in the preamble to the HIPAA Security Rule, CMS does not require their use in complying with the Security Rule.¹</p>
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	<p>This recommendation specifies the Triple Data Encryption Algorithm (TDEA) block cipher. The TDEA block cipher includes a Data Encryption Algorithm (DEA) cryptographic engine implemented as a component of TDEA as specified in Section 3. TDEA functions incorporating the DEA cryptographic engine shall be designed in such a way that they may be used in a computer system, storage facility, or network to provide cryptographic protection to binary coded data. The method of implementation will depend on the application and environment. TDEA implementations shall be subject to being tested and validated as accurately performing the transformations specified in the TDEA algorithm and in NIST Special Publication 800-38, Recommendation for Block Cipher Modes of Operation - Methods and Techniques.</p>



Designation	Standard Name	Description
SP 800-73	Interfaces for Personal Identity Verification	This document contains technical specifications to interface with the smart card to retrieve and use the identity credentials. These specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, communication interface, and application programming interface. Moreover, this specification enumerates requirements where the standards include options and branches. This document goes further by constraining implementers' interpretation of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.
SP 800-76	Biometric Data Specification for Personal Identity Verification	This document contains technical specifications for biometric data mandated in [FIPS]. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to declare what content is required and what is optional. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (Appendix A of SP 800-73-1). Biometric data used only outside the PIV Data Model is not within the scope of this standard.



Designation	Standard Name	Description
SP 800-77	Guide to IPsec VPNs	This publication seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical guidance on implementing security services based on Internet Protocol Security (IPsec). This document presents information that is independent of particular hardware platforms, operating systems, and applications, other than providing real-world examples to illustrate particular concepts. Specifically, the document includes a discussion of the need for network layer security services, a description of the types of services that are offered at the network layer, and how IPsec addresses these services. It uses a case-based approach to show how IPsec can be used to solve common network security issues. It also describes alternatives to IPsec and discusses under what circumstances each alternative may be appropriate.
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201 as well as the supporting infrastructure specified in FIPS 201 and the related Special Publications 800-73 (SP 800-73), Interfaces for Personal Identity Verification, and the forthcoming SP 800-76, Biometric Data Specification for Personal Identity Verification, [SP800-76] that rely on cryptographic functions.
SP 800-81	Secure Domain Name System (DNS) Deployment Guide	This publication seeks to assist organizations in understanding the secure deployment of Domain Name System (DNS) services in an enterprise. It provides practical guidance on securing each facet of DNS within an organization based on an analysis of the operating environment and associated threats.
SP 800-92	Guide to Computer Security Log Management	This publication seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in this publication covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an organization. The publication presents log management technologies from a high-level viewpoint, and it is not a step-by-step guide to implementing or using log management technologies.



Designation	Standard Name	Description
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS)	This publication seeks to assist organizations in understanding intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems (IDPS). It provides practical, real-world guidance for each of four classes of IDPS products: network-based, wireless, network behavior analysis, and host-based. The publication also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software and network forensic analysis tools. It focuses on enterprise IDPS solutions, but most of the information in the publication is also applicable to standalone and small-scale IDPS deployments. This publication replaces NIST Special Publication 800-31, Intrusion Detection Systems.
SP 800-95	Guide to Secure Web Services (draft)	This document explains the security features of Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), the Universal Description, Discovery and Integration (UDDI) protocol, and related open standards in the area of Web services. It also provides specific recommendations to ensure the security of Web services-based applications.
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	This publication seeks to assist organizations in understanding, selecting, and implementing technologies based on Institute of Electrical and Electronics Engineers (IEEE) 802.11i, part of the IEEE 802.11 family of wireless networking standards. ² The document explains at length the security features and capabilities associated with IEEE 802.11i through its framework for Robust Security Networks (RSN), and provides extensive guidance on the planning and deployment of RSNs. The document also discusses previous IEEE 802.11 security measures and their shortcomings.
SPML	Service Provisioning Markup Language	OASIS SPML Version 2 (SPMLv2) defines a core protocol [SPMLv2] over which different data models can be used to define the actual provisioning data. The combination of a data model with the SPML core specification is referred to as a profile. The use of SPML requires that a specific profile is used, although the choice of which profile is used to negotiate out-of-band by the participating parties.



Designation	Standard Name	Description
SSL	Secure Sockets Layer	The Secure Sockets Layer (SSL) protocol provides communications privacy over the Internet that allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. It is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.
Supplement 55	Digital Imaging and Communications in Medicine (DICOM) Attribute Level Confidentiality Supplement: # 55	Adds a mechanism for selective protection of individual attributes within arbitrary DICOM service-object pair (SOP) instances. It may be used to achieve protection of identifying information, e.g., a reversible anonymization or pseudonymization of DICOM SOP instances while continuing to use unmodified lower level message and protocol services for network transfer, storage, and media exchange of composite image information objects. Visit medical.nema.org for more information.
Supplement 86	Digital Imaging and Communications in Medicine (DICOM) Digital Signatures in Structured Reports	This Supplement describes how Digital Signatures would be used within the context of a DICOM Structured Report. This supplement adds — a code sequence attribute to the Digital Signatures Macro that can be used to identify the purpose of a Digital Signature (e.g. author, verifier, etc.), — a mechanism for securely referencing a digitally signed object, — a mechanism for securely referencing an object that is not digitally signed, — a Digital Signature profile that describes the use of Digital Signatures in a Structured Report, — a modification of the Key Object Selection Document Template, which can be used to collect secure references to a related set of DICOM composite objects. The use of the mechanisms and profiles in this Supplement is intended to allow the reader of a structured report to determine — if the report has been altered since its creation, — if evidence referenced by the report has not been altered since the report creator utilized it, — the identities of the parties that signed the report, thus minimizing the chance of a fictitious report being created.



Designation	Standard Name	Description
Supplement 99:	Digital Imaging and Communications in Medicine (DICOM) Extended Negotiation of User Identity	Security and privacy mechanisms require a method for establishing the identity of the person or entity that is responsible for DICOM transactions. This supplement defines three identity methods by means of a common mechanism. These are (a) the un-authenticated identity assertion. A string containing the user's identity in plain text, e.g. user's name. (b) a username plus pass code to permit authentication. (c) the authenticated Kerberos system. Kerberos authentication is widely used and well established. It provides strong authentication for network users, and strong authentication for network servers. It establishes a network wide user identity that spans many operating systems and devices.
TLS	The Transport Layer Security Protocol Version 1.0	The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
TR18307	Requirements for Interoperability and interoperability of messaging standards	
TS21547	Health informatics: Secure Archiving of electronic health records Part1 Principles and Requirements, Part 2 Guidelines	
WSRM	OASIS Web Services Reliable Messaging TC WS-Reliability 1.1	Web Services Reliability (WS-Reliability) is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering. WS-Reliability is defined as SOAP header extensions and is independent of the underlying protocol. This specification contains a binding to HTTP.
WS-SecureConversation 1.3	OASIS Web Services Secure Exchange (WS-SX) Technical Committee WS-SecureConversation 1.3	The WS-SecureConversation specification defines extensions to allow security context establishment and sharing, and session key derivation. This allows contexts to be established and potentially more efficient keys or new key material to be exchanged, thereby increasing the overall performance and security of the subsequent exchanges. The security context is defined as a new WS-Security token type that is obtained using a binding of WS-Trust. This



Designation	Standard Name	Description
		standard builds on top of the WS-Security 1.1 family of standards
WS-Trust 1.3	OASIS Web Services Secure Exchange (WS-SX) Technical Committee -Trust 1.3	The WS-Trust specification uses the base mechanisms of WS-Security and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Specifically, WS-Trust provides methods for issuing, renewing, and validating security tokens and ways to establish assess the presence of, and broker trust relationships. This standard builds on top of the WS-Security 1.1 family of standards
WSS:SOAP Message Security	OASIS Web Services Security: Soap Message Security 1.0	This specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e., support multiple security token formats). For example, a client might provide one format for proof of identity and provide another format for proof that they have a particular business certification. Additionally, this specification describes how to encode binary security tokens, a framework for XML-based tokens, and how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the tokens that are included with a message.
WSS:SOAP Message Security	OASIS Web Services Security: Soap Message Security 1.1	This specification proposes a standard set of SOAP [SOAP11, SOAP12] extensions that can be used when building secure Web services to implement message content integrity and confidentiality. This specification refers to this set of extensions and modules as the "Web Services Security: SOAP Message Security" or "WSS: SOAP Message Security". This specification is flexible and is designed to be used as the basis for securing Web services within a wide variety of security models including PKI, Kerberos, and SSL. Specifically,



Designation	Standard Name	Description
		<p>this specification provides support for multiple security token formats, multiple trust domains, multiple signature formats, and multiple encryption technologies. The token formats and semantics for using these are defined in the associated profile documents. This specification provides three main mechanisms: ability to send security tokens as part of a message, message integrity, and message confidentiality. These mechanisms by themselves do not provide a complete security solution for Web services. Instead, this specification is a building block that can be used in conjunction with other Web service extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies. These mechanisms can be used independently (e.g., to pass a security token) or in a tightly coupled manner (e.g., signing and encrypting a message or part of a message and providing a security token or token path associated with the keys used for signing and encryption).</p>
X.500	The CCITT and ISO standard for electronic directory services	<p>X.500 is a series of computer networking standards covering electronic directory services. The X.500 series was developed by ITU-T, formerly known as CCITT. The directory services were developed in order to support the requirements of X.400 electronic mail exchange and name lookup. ISO was a partner in developing the standards, incorporating them into the Open Systems Interconnection suite of protocols. ISO/IEC 9594 is the corresponding ISO identification.</p>



Designation	Standard Name	Description
X12	Electronic Data Interchange	<p>In 1979, the American National Standards Institute (ANSI) chartered the Accredited Standards Committee (ASC) X12 to develop uniform standards for inter-industry electronic exchange of business transactions-electronic data interchange (EDI). Electronic Data Interchange (EDI) is the computer-to-computer exchange of business data in standard formats. In EDI, information is organized according to a specified format set by both parties, allowing a "hands-off" computer transaction that requires no human intervention or rekeying on either end. All information contained in an EDI transaction set is, for the most part, the same as on a conventionally printed document. The X12 and UN/EDIFACT standards specify only the format and data content of e-business transactions. They do not define how interchange partners shall establish the required communications link to exchange EDI data. Users may choose any EDI and communications software that supports use of the standards. The standards do not address this choice; they simply establish the format and define the data contents of the EDI messages and control standards. A complete set of X12 standards is called a release.</p>
X12.58	Security Structures (version 2)	<p>This ASC X12 standard is used to define the data formats required for authentication and encryption to provide integrity, confidentiality and verification of the originator at the functional group and transaction set levels.</p>
X3.92	Data Encryption Algorithm (DEA)	<p>Data Encryption Standard applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession. It is specified in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards.</p>



Designation	Standard Name	Description
X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	This standard specifies schemes for the agreement of symmetric keys using the Diffie-Hellman and MQV algorithms. These methods may be used by different parties to establish common shared secret information such as cryptographic keys. The shared secret information may be used with symmetrically-keyed algorithms to provide confidentiality, authentication, and data integrity services, or used as a key-encrypting key with other key management protocols. The key agreement schemes specified in ANSI X9.42 may be used as subroutines to build key establishment protocols.
X9.44	Key Establishment Using Factoring-Based Public Key Cryptography for the Financial Services Industry	This standard defines key establishment schemes that employ asymmetric cryptographic techniques. The arithmetic operations involved in the operation of the schemes take place in the algebraic structure of a multiplicative group of a finite ring. Both key agreement and key transport schemes are specified, but only in an informative appendix in the current draft. The schemes may be used by two parties to compute shared keying data that may then be used by symmetric schemes to provide cryptographic services, e.g. data confidentiality and data integrity.
X9.45	Enhanced Management Controls Using Digital Signatures and Attribute Certificates	Defines strategies for reducing the security and financial risks associated with electronic business systems using digital signatures. Attribute certificates would be used to convey authorizations and restrictions that inform verifiers when an entity's signature would be considered valid. Attributes might include specified dollar amounts, cosignature requirements, preapproved counterparties, confirm to (address), and time of day. The benefits of this standard are cost reduction, enhanced security, greater manageability, and greater flexibility for business transactions. This standard was first listed for public review in the June 5, 1998 issue of Standards Action. It is being resubmitted due to substantive changes to the text.
X9.52	Triple Data Encryption Algorithm Modes of Operation	Defines triple-DES algorithm for use in both wholesale and retail financial applications. As part of this definition, related standards that should be modified to accommodate the use of this algorithm on an optional basis are also identified.



Designation	Standard Name	Description
X9.55	Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists	Specifies extensions to the definitions of public-key certificates and certificate revocation lists in Public Key Cryptography for the Financial Services Industry: Certificate Management, BSR X9.57. These extensions are in the following areas: the keys involved, including key identifiers for subject and issuer keys, indicators of intended or restricted key usage, and indicators of certificate policy; name forms for a certificate subject, a certificate issuer, or a CRL issuer, and additional attribute information about a certificate subject; included in CA-certificates, i.e., certificates for CAs issued by other CAs, to facilitate the automated processing of certification paths when multiple certificate policies are involved, e.g., when policies vary for different applications in an environment or when interoperation with external environments occurs; and time at which the condition causing the revocation occurred; revocation information from one CA to be partitioned into separate CRLs to facilitate control of CRL sizes, and CRL extensions to support the use of partial CRLs indicating only changes since an earlier CRL issue.
X9.57	Public Key Cryptography for the Financial Services Industry: Certificate Management	Defines certificate management procedures and data elements.
X9.62	Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)	This Standard defines methods for digital signature generation and verification for the protection of messages and data using the Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA is the elliptic curve analogue of the Digital Signature Algorithm (ANS X9.30). The ECDSA shall be used in conjunction with an Approved hash function, as specified in X9 Registry Item 00003, Secure Hash Standard (SHS). The hash functions Approved at the time of publication of this document are SHA-1 (see NOTE), SHA-224, SHA-256, SHA-384 and SHA-512. This ECDSA Standard provides methods and criteria for the generation of public and private keys that are required by the ECDSA and the procedural controls required for the secure use of the algorithm with these keys. This ECDSA Standard also provides methods and criteria for the generation of elliptic curve domain parameters that are required by the ECDSA and the procedural controls required for the secure use of the algorithm with these domain parameters.



Designation	Standard Name	Description
XACML	eXtensible Access Control Markup Language (XACML)	eXtensible Access Control Markup 3 Language (XACML) Version defines an XML schema for an extensible access-control policy language.
XaDES	XML Advanced Electronic Signatures (XAdES)	XAdES extends the IETF/W3CXML-Signature Syntax and Processing specification [XMLDSIG] into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" [EU-DIR-ESIG] (also denoted as "the Directive" or the "European Directive" in the rest of the present document) and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. An advanced electronic signature aligned with the present document can, in consequence, be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later.
XML-DSig	XML-Signature Syntax and Processing (XML-DSig)	This document specifies XML syntax and processing rules for creating and representing digital signatures. XML Signatures can be applied to any digital content (data object), including XML. An XML Signature may be applied to the content of one or more resources. Enveloped or enveloping signatures are over data within the same XML document as the signature; detached signatures are over data external to the signature element. More specifically, this specification defines an XML signature element type and an XML signature application; conformance requirements for each are specified by way of schema definitions and prose respectively. This specification also includes other useful types that identify methods for referencing collections of resources, algorithms, and keying and management information.



Designation	Standard Name	Description
XPath Filter	XML-Signature XPath Filter 2.0	XML Signature [XML-DSig] recommends a standard means for specifying information content to be digitally signed and for representing the resulting digital signatures in XML. Some applications require the ability to specify a subset of a given XML document as the information content to be signed. The XML Signature specification meets this requirement with the XPath transform. However, this transform can be difficult to implement efficiently with existing technologies. This specification defines a new XML Signature transform to facilitate the development of efficient document subsetting implementations that interoperate under similar performance profiles.
XUA	IHE IT Infrastructure Technical Framework Cross-Enterprise User Authentication (XUA)	IHE proposes a Cross-Enterprise User Authentication (XUA) profile that will provide the user identity in transactions that cross enterprise boundaries. Enterprises may choose to have their own user directory and their own unique method of authenticating. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries.

6.2 SECURITY AND PRIVACY TECHNICAL COMMITTEE MEMBERS

The following table contains a list of the Security and Privacy Technical Committee members as of April 6, 2007.

Table 6.2-1 Security and Privacy Technical Committee Members

Name	Company/Organization	Technical Committee Participation
Mr. Michael Aisenberg	Liberty Alliance	Consumer Empowerment
Chris Apgar, CISSP	Oregon & SW Washington Healthcare, Privacy & Security Forum	Consumer Empowerment
Soloman I. Appavu Ph.D	Center for Healthcare Automation Ltd.	Consumer Empowerment
Dixie Baker, Ph.D	SAIC	Security and Privacy Technical Committee
Adam Birnbaum, CHP, CHSS, CPEHR	Blue Cross Blue Shield Association	Security and Privacy Technical Committee
Elaine A. Blechman, Ph.D	Professor, U. of Colorado-Boulder	Co-chair of Consumer Empowerment
Christopher Boyce CTO	vIDentity Systems, Inc. (VSI)	Care Delivery, Population Health, Consumer Empowerment



Name	Company/Organization	Technical Committee Participation
Kelly Martin Callahan	HIPAA Inc.	Consumer Empowerment
Ken Carlson	LSS Data Systems	Care Delivery
Lisa Carnahan	NIST - US Department of Commerce	Care Delivery, Population Health, Consumer Empowerment
Lester Chan, CISSP, CISM, CISA	California Office of HIPAA Implementation	Consumer Empowerment
John R. Christiansen	Christiansen IT Law	Consumer Empowerment
Jeff Collmann, Ph.D	HIMSS Privacy and Security Steering Committee	Consumer Empowerment
Kathleen Connor	FOX Systems Inc.	Consumer Empowerment
Ed Coyne	Veterans Health Administration, US Department of Veterans Affairs	Consumer Empowerment
William Crawford	Centers for Medicare and Medicaid Services	Consumer Empowerment
Mike Davis	Department of Veterans Affairs	Consumer Empowerment
Daniel Dean	WebMD Health	Consumer Empowerment
Richard S. Dick Ph.D	You Take Control	Consumer Empowerment
Gary Dickinson	Centrify Health/ Chair, US Technical Advisory Group To ISO TC 215, Health Informatics	Care Delivery, Population Health, Consumer Empowerment
Barry Dickman	MITRE	Consumer Empowerment
Pamela Dyckhoff	Availity, LLC	Care Delivery and Consumer Empowerment
Doug Eubank	digiChart, Inc.	Consumer Empowerment
Rachel Foerster	CAQH	Consumer Empowerment
Lisa Gallagher	HIMSS Privacy and Security Steering Committee	Consumer Empowerment
Ann Geyer	Tunitas Group	Consumer Empowerment
Melinna Giannini	ABC CODING SOLUTIONS	Consumer Empowerment
Rich Giddings	Achieve Healthcare Technologies	Consumer Empowerment
Michael J Griffiths R.Ph	Albertsons	Care Delivery
Adrian Gropper MD	MedCommons Inc.	Consumer Empowerment
Denise Haley	Philips Medical Systems	Consumer Empowerment, Care Delivery, and ER-EHR Use Case
Lois Hall	Department of Veterans Affairs	Consumer Empowerment
Vicki Hohner	FOX Systems Inc.	Consumer Empowerment
Elizabeth S. Holland	Centers for Medicare & Medicaid Services	Consumer Empowerment



Name	Company/Organization	Technical Committee Participation
Maryann Hondo	IBM	Consumer Empowerment
Al Jackson	RXHUB	Consumer Empowerment
Raja Kailar	Business Networks International, Inc.	Consumer Empowerment
Hetty Khan	National Center for Health Statistics/CDC	Consumer Empowerment
Wilma L Kidd, CIPP, MEd, BSW	WellPoint, Inc.	Consumer Empowerment
James F. Kragh	Good Health Network, Inc.	Consumer Empowerment
Jim Kretz	US Department of Health and Human Services	Consumer Empowerment
Joann Larson, R.N., M.S.	Kaiser Permanente	Population Health, Consumer Empowerment
Mike Levy	SSA	Consumer Empowerment
Ms. Jennifer Lis	Council for Affordable Quality Healthcare (CAQH)	Care Delivery and Consumer Empowerment
John Macaulay, MD	Anakam LLC	Consumer Empowerment
Yelena MacLeod	SSA	Consumer Empowerment
Glen Marshall	HL7	Consumer Empowerment
John E Mattison, MD	Kaiser Permanente - Information Technology	Consumer Empowerment
Ken McCaslin	Quest Diagnostics Incorporated	Care Delivery, Population Health, Consumer Empowerment
Tim McNeil	RXHUB	Consumer Empowerment
Lori Meldberg	Delta Dental of MN	Consumer Empowerment
John Moehrke	GE Healthcare	Care Delivery, Population Health, Consumer Empowerment
Aditya Naik	SSA	Care Delivery and Consumer Empowerment
Robert M. Plovnick, MD, MS	American Psychiatric Association	Consumer Empowerment
Martin Prahll	SSA	Care Delivery and Consumer Empowerment
Erik Pupo	Pearson Blueprint Technologies	Care Delivery, Population Health, Consumer Empowerment
Patrick Pyette	HIPAAAT Inc.	Consumer Empowerment
Marian Reed	McKesson Corporation	Consumer Empowerment
Lori Reed-Fourquet	eHealthSign, LLC	Population Health
Harry Rhodes, MBA, RHIA, CHPS	AHIMA	Consumer Empowerment



Name	Company/Organization	Technical Committee Participation
Scott M Robertson, PharmD	Kaiser Permanente - Information Technology	Care Delivery, Population Health, Consumer Empowerment
Ronald Ross	Cisco	Consumer Empowerment
Matt Scholl	NIST	Consumer Empowerment
Elliot Sloane, Ph.D.	IHE	Consumer Empowerment
Toby Slusher	Centers for Disease Control & Prevention	Consumer Empowerment
Debbie Somers	SSA	Care Delivery and Consumer Empowerment
Steve Steindel PhD	Centers for Disease Control & Prevention	Care Delivery, Population Health, Consumer Empowerment
Christina Stephan MD MBA	Liberty Alliance	Care Delivery
Kevin Stine	NIST	Consumer Empowerment
Michael Stokes	Microsoft	Security and Privacy Technical Committee
Walter G. Suarez	Institute for HIPAA/HIT	Population Health
Richard Swart	Utah State University	Consumer Empowerment
Richard Thoreson, Ph.D.	HHS/SAMHSA/CSAT	Care Delivery and Consumer Empowerment
Eric Tiffany	Liberty Alliance	Consumer Empowerment
Lisa Tompkins	Federal Health Architecture	Care Delivery and Consumer Empowerment
John Travis, CPA, FHFMA, MSA	Cerner	Consumer Empowerment
Amit V. Trivedi	The National Alliance for Health Information Technology	Consumer Empowerment
Alan Viars CEO	viDentity Systems, Inc. (VSI)	Care Delivery, Population Health, Consumer Empowerment
Michele M. Vilaret, R.Ph.	National Association of Chain Drug Stores (NACDS)	Consumer Empowerment
Ken Waldbillig	EMC Corporation	Care Delivery
Jeffrey Walko	WellPoint, Inc	Consumer Empowerment
Barry Walters	Anakam LLC	Consumer Empowerment
Lawrence Williams	Roadside Telematics Corporation	Consumer Empowerment
Lori Wood	Good Health Network	Consumer Empowerment
Sarah Quaynor	GSI/ANSI	HITSP Security and Privacy Technical Committee Support
Johnathan Coleman, CISSP, CISM	Security Risk Solutions, Inc.	HITSP Security and Privacy Technical Committee Facilitator

