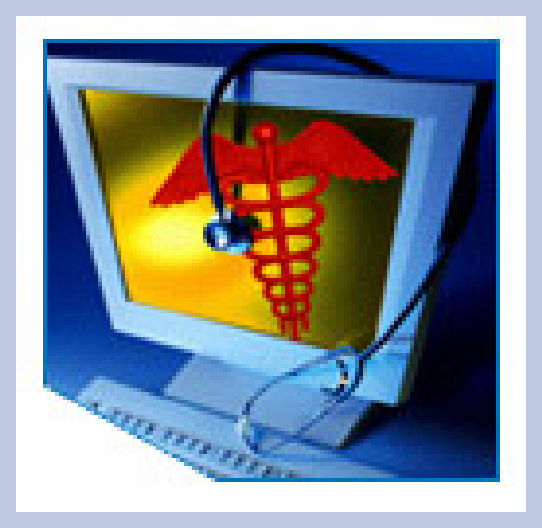
August 27, 2008
Version 1.2

HITSP Collect and Communicate Security Audit Trail Transaction

HITSP/T15



Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)

DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	July 20, 2007
1.0.1	Review Copy	Security and Privacy Technical Committee	October 5, 2007
1.1	Released for Implementation	Security and Privacy Technical Committee	October 15, 2007
1.1.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	August 20, 2008
1.2	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	August 27, 2008

TABLE OF CONTENTS

1.0 INTRODUCTION 5

1.1 Overview 5

1.2 Transaction Document Map 5

1.3 Copyright Permissions 6

1.4 Reference Documents 7

2.0 TRANSACTION DEFINITION 8

2.1 Context Overview 8

2.1.1 Transaction Constraints 10

2.1.2 Technical Actors 10

2.1.3 Actor Interactions 10

2.1.4 Pre-conditions 11

2.1.4.1 Process Triggers 12

2.1.5 Post-conditions 12

2.1.5.1 Required Outputs 13

2.1.6 Data Flows 13

2.2 List of HITSP Constructs 13

2.2.1 Construct Dependencies 13

2.2.2 Additional Constraints on Required Constructs 14

2.3 Standards 14

2.3.1 Regulatory Guidance 14

2.3.2 Selected Standards 14

2.3.3 Informative Reference Standards 15

3.0 TECHNICAL IMPLEMENTATION 16

3.1 Conformance 16

3.1.1 Conformance Criteria 16

3.1.2 Conformance Scoping, Subsetting and Options 16

4.0 APPENDIX 17

5.0 CHANGE HISTORY 18

5.1 October 5, 2007 18

5.2 October 15, 2007 18

5.3 August 20, 2008 18

5.4 August 27, 2008 18

FIGURES AND TABLES

Figure 1.2-1 Collect and Communicate Security Audit Trail Transaction Document Map 6
Figure 2.1.3-1 Actor Interactions 11

Table 1.4-1 Reference Documents 7
Table 2.1.1-1 Transaction Constraints 10
Table 2.1.2-1 Technical Actors 10
Table 2.1.4-1 Pre-conditions 12
Table 2.1.4.1-1 Process Triggers 12
Table 2.1.5-1 Post-conditions 12
Table 2.1.5.1-1 Required Outputs 13
Table 2.2-1 List of HITSP Constructs 13
Table 2.2.1-1 Construct Dependencies 13
Table 2.2.2-1 Additional Constraints on Required Constructs 14
Table 2.3.1-1 Regulatory Guidance 14
Table 2.3.2-1 Selected Standards 15
Table 2.3.3-1 Informative Reference Standards 15

1.0 INTRODUCTION

As an introduction to the HITSP Collect and Communicate Security Audit Trail Transaction, this section provides a high level overview of the information sharing scenario enabled by following this specification, provides a document map of the construct relationships for this specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Transaction Definition.

1.1 OVERVIEW

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

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

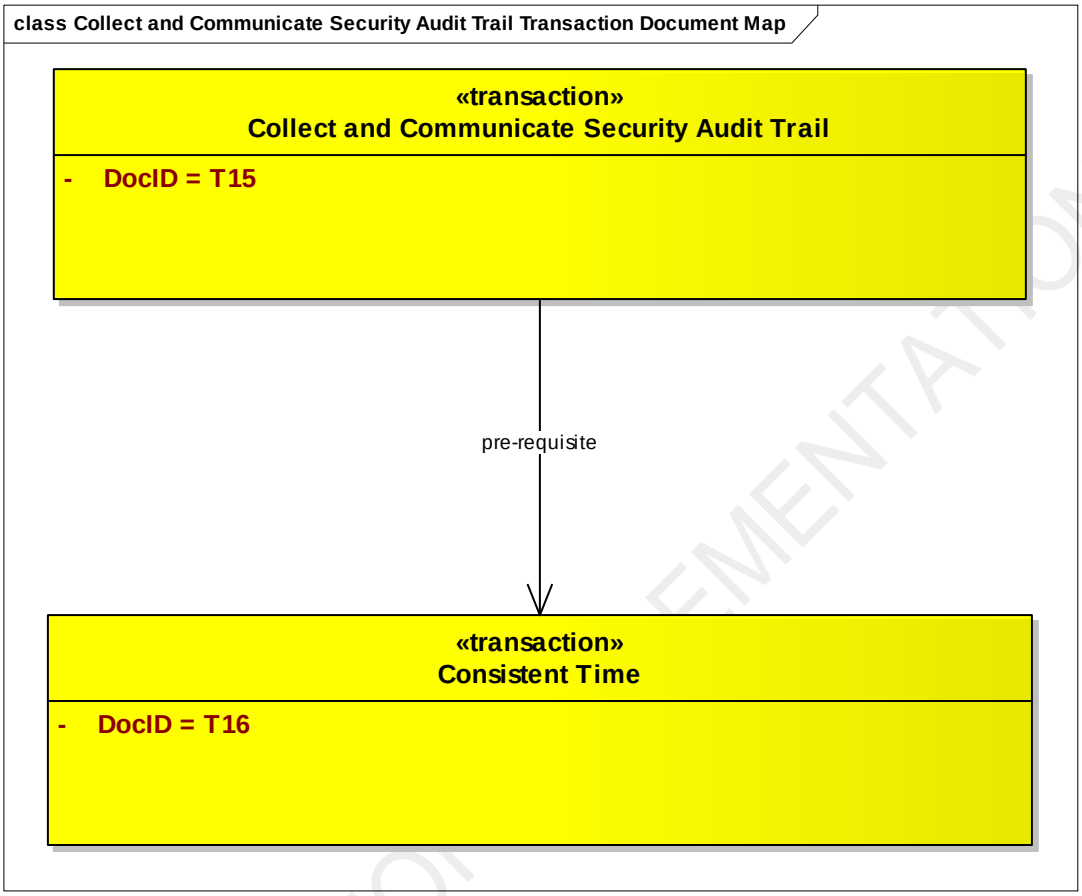
Applicable standards for security and privacy audit reports and automated response actions have been identified, but specific applications of those standards are subject to implementation-defined polices and are therefore not in the scope of this document.

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

1.2 TRANSACTION DOCUMENT MAP

Each HITSP specification describes a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications that will satisfy the requirements for the HITSP construct. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). Interoperability Specifications define the context(s) in which any other HITSP construct may be used. The current Collect and Communicate Security Audit Trail Transaction specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 Interoperability Specification Document Map from the relevant IS to better understand the context, dependencies, and relationships between the constructs used to meet the IS requirements. The Document Map in Figure 1.2-1 depicts how this construct integrates and constrains HITSP constructs to support the information exchange, within the defined context of this document. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

Figure 1.2-1 Collect and Communicate Security Audit Trail Transaction Document Map



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2008 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.

ASTM International materials used in this document have been extracted, with permission from E-2147-01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, copyright ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428. Copies of this standard are available through the ASTM Web Site at www.astm.org.

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

1.4 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.

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

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
TN900 - Security and Privacy Technical Note	Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following: • The scope, reference policy background, and Security and Privacy principles used in the development of the constructs • A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs • A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases • A list of identified gaps and the recommended approaches to resolving those gaps • A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications • A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management • A glossary of terms used in all the Security and Privacy construct documents • A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.

2.0 TRANSACTION DEFINITION

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

2.1 CONTEXT OVERVIEW

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

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

1. Data to be collected/audited are identified
2. Data to be reported for audit are formatted
3. Data to be reported for audit are collected
4. Reports are provided for analysis of audit data
5. Audit data are retained for analysis
6. Automated responses are provided for audited data
7. Alerts and alarms are provided for security audit
8. Identity of users is recorded whenever a protected resource is accessed
9. Time of access is recorded whenever protected resource is accessed
10. Identity of users is recorded whenever registration data are accessed
11. Time of access is recorded whenever registration data are accessed

This HITSP Transaction references the Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication (ATNA) Integration Profile to accomplish audit trail assurances in support of document-sharing and to support audit trails for message-based communications.

The text for the IHE ITI-TF-1 V4.0 begins here:

> As described in Section 9 of IHE ITI-TF-1 V4.0, the Audit Trail and Node Authentication (ATNA) Integration Profile establishes security measures which, together with the Security Policy and Procedures of the enterprise, provide patient information confidentiality, data integrity, and user accountability. The goals of the Audit Trail and Node Authentication Integration Profile are:
>
> - *User Accountability (Audit Trail)*
>
> To allow a security officer in an institution to audit activities, to assess compliance with a secure domain policy, to detect instances of non-compliant behavior, and to facilitate detection of improper creation, access, modification and deletion of protected resources. Protected resources include the patient-identifiable information records (e.g. Registration, Order, Study/Procedure, Reports, Images, and Presentation States). It may be accessed by users or

exchanged between the systems. This includes information exported to and imported from every secured node in the secure domain. The audit trail contains information so that questions can be answered such as:

  - For certain users: which patient's personal health information was accessed?
  - For certain patient personal health information: which users accessed it?
  - What user authentication failures were reported?
  - What node authentication failures were reported?

- *Access Control*
  ATNA contributes to access control by limiting network access between nodes and limiting access to each node to authorized users. Network communications between secure nodes in a secure domain are restricted to only other secure nodes in that domain. Secure nodes limit access to authorized users as specified by the local authentication and access control policy.
- *Audit Record Repository*
  Provides an Audit Record Repository as the simplest means to implement security requirements. An immediate transfer of Audit Records from all the IHE actors to the Audit Record Repository is required when possible, reducing the opportunities for tampering and making it easier to audit the department, but disconnected nodes may store audit data for transfer to the Audit Record Repository upon reconnection to the secure domain network. The Audit Record Repository actor may be implemented as a single instance in a security domain, as fully distributed instances, as related with message passing between, or in other configurations based on policy.
- *Protected Data Integrity*
  To allow tracking of the life of protected information (creation, modification, deletion and location) and its data integrity during this process.

The text for the IHE ITI-TF-1 V4.0 ends here.

The format and content of audit reports are subject to local implementation policy and set by the organizations, guided by the ASTM E2147 standard. HITSP does not specify these policies or their application (see Section 2.1.5.1 Outputs).

The specific choice and operation of automated actions is subject to local implementation policy and set by the organizations, guided by the ISO 10164-7 standard. HITSP does not specify these policies or their application (see Section 2.1.5.1 Outputs).

Many events are auditable, but the choice to create and communicate the audit record or to report the data, commonly called "selective auditing", and "selective audit reporting", is subject to local implementation policy. HITSP does not specify these policies or their application.

2.1.1 TRANSACTION CONSTRAINTS

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

Table 2.1.1-1 Transaction Constraints

Constraint
The transport protocol for audit record communication shall be BSD syslog, per the IHE ATNA specification
The "provisional format" for audit records defined in IHE ATNA shall not be used

Note: We anticipate that the Internet Engineering Task Force will publish a syslog-protocol that will provide a more robust alternative to BSD syslog.

2.1.2 TECHNICAL ACTORS

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

All Technical Actors for this Transaction are described further in Appendix A of IHE ITI-TF-2 V4.0.

Table 2.1.2-1 Technical Actors

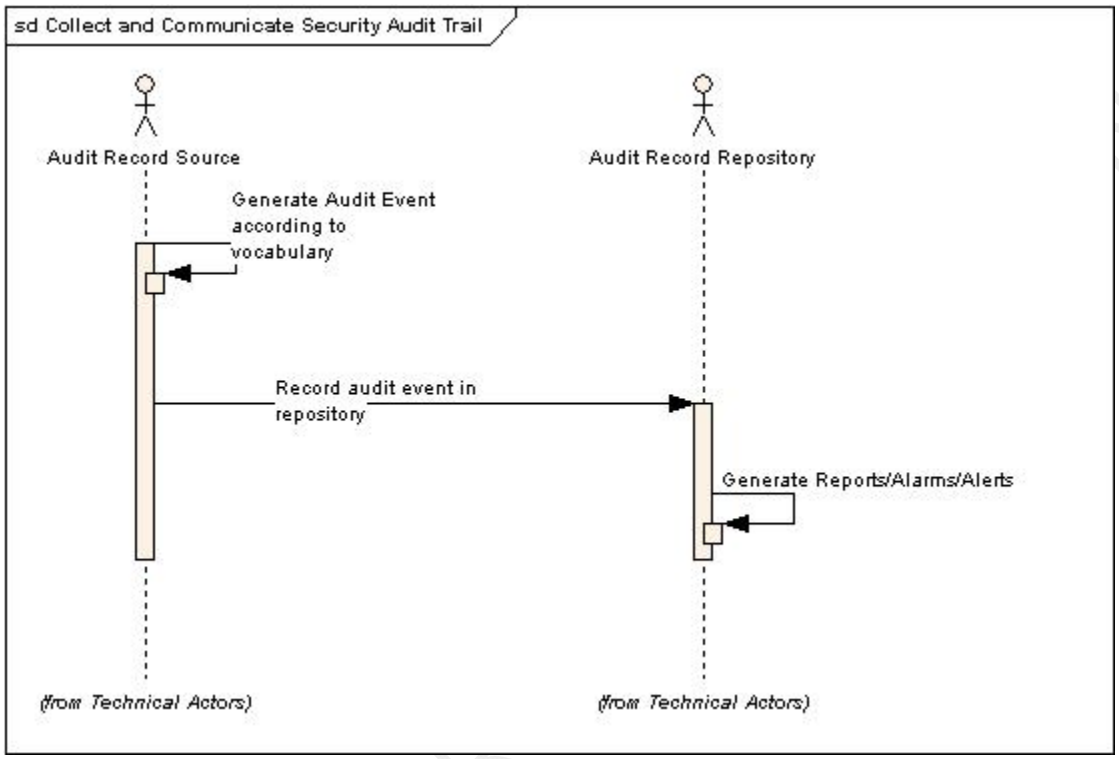
Technical Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
<any actor grouped with a Secure Node actor>	Any actor from the HITSP Interoperability Specification that is grouped with Secure Node	IHE ITI-TF-2 V4.0 ATNA	R
Audit Record Source	The actor that, on behalf of another actor that performs an action requiring logging, creates and communicates an Audit Record to the Audit Record Repository	IHE ITI-TF-2 V4.0 ATNA	R
Audit Record Repository	This actor provides a repository for audit events. IHE does not specify what analysis and reporting features should be implemented for an audit repository	IHE ITI-TF-2 V4.0 ATNA	R

2.1.3 ACTOR INTERACTIONS

The following sections document the content of the Transaction and the basic process flows that are supported by the Transaction. It describes the underlying events that fulfill the Transaction, the sequence

and timing of the events, and the specific actors involved. Process flow diagrams are provided to illustrate the process relationships.

Figure 2.1.3-1 Actor Interactions



An audit trigger event occurs within the audit record source. This causes the audit record source to format and produce an audit record, according to locally-defined policies, and send it to the Audit Record Repository. The Audit Record Repository will subsequently perform reporting, alarming, or alerting according to locally-defined policies.

Locally defined policies at the audit record source may specify selective suppression of auditing records for certain events that have been determined to be inconsequential.

Locally-defined policies at the Audit Record Repository will specify report format, production times, and distribution. They may also specify automated alarms or alerts for certain events of high importance, suppress reporting or report certain types of events until threshold values for similar/recurring events occur, enable selective reporting to investigate user activity, etc.

2.1.4 PRE-CONDITIONS

This section describes the necessary conditions that must be in place prior to the start of the workings of the Transaction. The pre-conditions are used to convey any conditions that must be true at the outset of a Transaction. They describe the context that must be established before the Transaction is executed. They

are not however the triggers that initiate the Transaction. Where one or more pre-conditions are not met, the behavior of the Transaction should be considered uncertain.

Table 2.1.4-1 Pre-conditions

Pre-condition
Consistent Time construct is a pre-requisite for this Transaction
Secure Nodes is a pre-condition to this Transaction
A policy defining what is to be audited exists
Audit record source is initialized to the audit policy
Audit Record Repository is active and designated as the destination for recorded audit events
Policy defining the protection of the log and audit exists and is being enforced
Identities are managed

2.1.4.1 Process Triggers

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

Table 2.1.4.1-1 Process Triggers

Process Trigger
An action requiring logging occurs
Audit records are created (trigger for communicated)
Audit records are received (triggers for reports/alarms/alerts)

Various Transaction triggers are described in Table 3.20.6-1 of IHE ITI-TF-2 V4.0. These are the minimum transaction triggers in order to maintain commonality with an established standard, satisfy the implied policy issues in the Use Cases that call for auditing and still allow for organizations to further define audit policy that can be supported by a log standard.

2.1.5 POST-CONDITIONS

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

Table 2.1.5-1 Post-conditions

Post-condition
Audit Record is created, communicated, stored, and analyzed
Subsequent action initiated per policy, e.g., reports and other automated actions

2.1.5.1 Required Outputs

For the post-conditions specified above, this section further identifies the formats and usages of the required outputs that must be produced at the end of the Transaction in order for the Transaction to be deemed successfully completed.

Table 2.1.5.1-1 Required Outputs

Required Output	Format/Usage
Audit record	Defined in Section 3.20.7.1 of IHE-ITI-TF-2 V4.0
Security Audit Alarms	Defined in ISO 10164-7
Security Report	Defined in ASTM E2147-01

2.1.6 DATA FLOWS

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

All data flows associated with this Transaction are specified in Section 3.20 of IHE-ITI-TF-2 V4.0.

2.2 LIST OF HITSP CONSTRUCTS

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

Table 2.2-1 List of HITSP Constructs

Construct Name	Description	Event/Action Code	Content
No HITSP constructs are used by this Transaction			

2.2.1 CONSTRUCT DEPENDENCIES

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

Table 2.2.1-1 Construct Dependencies

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

2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

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

Table 2.2.2-1 Additional Constraints on Required Constructs

Data Element	Construct	Constraint	Constraint Type (Pre-condition, post-condition, general)	Purpose (Reason for this constraint)
No applicable dependencies				

2.3 STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. The standards used by this Transaction specification fall into the following categories:

- Regulatory guidance is a legal or other authoritative declaration that HITSP must abide by in standards selection (see Section 2.3.1)
- Selected standards are necessary for interoperability. These are standards that are used to meet information exchange requirements of associated constructs. For example, they are used to realize direct information exchange, to provide the transport mechanism, to specify the content, or to address security (see Section 2.3.2)
- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Transaction specification (see Section 2.3.3)

2.3.1 REGULATORY GUIDANCE

The following table provides a list of legal or other authoritative guidelines that HITSP must abide by, or has agreed to use as guidance in the selection of standards. Note that only the referenced sections of the regulations are relevant to the Transaction specification.

Table 2.3.1-1 Regulatory Guidance

Standard	Description
No applicable regulatory guidance	

2.3.2 SELECTED STANDARDS

The following table provides a list of standards that are used to meet interoperable information exchange requirements of this Transaction specification, and a detailed description of each standard.

Table 2.3.2-1 Selected Standards

Standard	Description
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration 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. The latest version of the IHE Technical Framework is available at www.ihe.net

2.3.3 INFORMATIVE REFERENCE STANDARDS

The following table lists standards that provide additional background information or guidance; however, they are not required for the implementation of the Transaction specification.

Table 2.3.3-1 Informative Reference Standards

Standard Name	Description/Usage
American Society for Testing and Materials (ASTM) Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01	E2147-01 "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, with the Privacy Act of 1974 (1)." For more information visit www.astm.org
International Organization for Standardization (ISO) Health informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992	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, 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. For more information visit www.iso.org

3.0 TECHNICAL IMPLEMENTATION

3.1 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

3.1.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also be constrained as specified in Table 2.1.1-1, and implement all of the required actors from Table 2.1.2-1, within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification with which this construct is associated.

3.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for actor scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.

4.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.

5.0 CHANGE HISTORY

The following sections provide the history of changes made to this document.

5.1 OCTOBER 5, 2007

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

845, 847, 1202, 1203, 1234, 1235, 1236, 1260

The full text of the comments along with the Technical Committee's disposition can be reviewed on the HITSP Public Web Site.

5.2 OCTOBER 15, 2007

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

5.3 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References. The IHE ITI TF Revision was updated to Revision 4 and more specific ATNA references were provided.

The following have been designated as Informative References:

- ASTM International Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01
- International Organization for Standardization (ISO) Health informatics -- Information technology -- Open Systems Interconnection -- Systems Management: Security alarm reporting function, Technical Specification #10164-- Part 7: Security Alarm Reporting Function, 1992

5.4 AUGUST 27, 2008

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