HITSP Collect and Communicate Security Audit Trail Transaction

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

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Description of Change</th>
<th>Name of Author</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Review Copy</td>
<td>Security and Privacy Technical Committee</td>
<td>July 20, 2007</td>
</tr>
<tr>
<td>1.0.1</td>
<td>Review Copy</td>
<td>Security and Privacy Technical Committee</td>
<td>October 5, 2007</td>
</tr>
<tr>
<td>1.1</td>
<td>Released for Implementation</td>
<td>Security and Privacy Technical Committee</td>
<td>October 15, 2007</td>
</tr>
<tr>
<td></td>
<td>Template Updated to V2.4</td>
<td>Project Team</td>
<td>July 31, 2008</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>August 20, 2008</td>
</tr>
<tr>
<td>1.2</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>August 27, 2008</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>December 10, 2008</td>
</tr>
<tr>
<td>1.3</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>December 18, 2008</td>
</tr>
<tr>
<td></td>
<td>Template V2.5</td>
<td>Project Team</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Review Copy</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>June 30, 2009</td>
</tr>
<tr>
<td>1.4</td>
<td>Released for Implementation</td>
<td>Security, Privacy and Infrastructure Domain Technical Committee</td>
<td>July 8, 2009</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1.0 INTRODUCTION
   1.1 Overview
   1.2 Copyright Permissions
   1.3 Reference Documents
   1.4 Conformance
      1.4.1 Conformance Criteria
      1.4.2 Conformance Scoping, Subsetting and Options

2.0 TRANSACTION DEFINITION
   2.1 Context Overview
      2.1.1 Transaction Constraints
      2.1.2 Interfaces
      2.1.3 Interface Interactions
      2.1.4 Pre-conditions
         2.1.4.1 Process Triggers
      2.1.5 Post-conditions
         2.1.5.1 Required Output
      2.1.6 Data Flows
   2.2 List of HITSP Constructs
      2.2.1 Construct Dependencies
      2.2.2 Additional Constraints on Required Constructs
   2.3 Standards
      2.3.1 Regulatory Guidance
      2.3.2 Selected Standards
      2.3.3 Informative Reference Standards

3.0 APPENDIX

4.0 DOCUMENT UPDATES
   4.1 October 5, 2007
   4.2 October 15, 2007
   4.3 August 20, 2008
   4.4 August 27, 2008
   4.5 December 10, 2008
   4.6 December 18, 2008
   4.7 June 26, 2009
   4.8 July 8, 2009
FIGURES AND TABLES

Figure 2-1 Interface Interactions ................................................................................................................... 9

Table 1-1 Reference Documents ...................................................................................................................... 5
Table 2-1 Transaction Constraints .................................................................................................................. 8
Table 2-2 Interfaces ........................................................................................................................................ 8
Table 2-3 Pre-conditions .................................................................................................................................. 9
Table 2-4 Process Triggers .............................................................................................................................. 10
Table 2-5 Post-conditions .............................................................................................................................. 10
Table 2-6 Required Outputs .......................................................................................................................... 10
Table 2-7 List of HITSP Constructs ............................................................................................................. 10
Table 2-8 Construct Dependencies ............................................................................................................... 10
Table 2-9 Additional Constraints on Required Constructs .......................................................................... 11
Table 2-10 Regulatory Guidance .................................................................................................................. 11
Table 2-11 Selected Standards ....................................................................................................................... 11
Table 2-12 Informative Reference Standards ............................................................................................... 11
1.0 INTRODUCTION

1.1 OVERVIEW

The HITSP 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 policies 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 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2009 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.

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.

1.3 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 2.0.

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

<table>
<thead>
<tr>
<th>Reference Document</th>
<th>Document Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HITSP Acronyms List</td>
<td>Lists and defines the acronyms used in this document</td>
</tr>
<tr>
<td>HITSP Glossary</td>
<td>Provides definitions for relevant terms used by HITSP documents</td>
</tr>
<tr>
<td>TN900 - Security and Privacy</td>
<td>TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs</td>
</tr>
</tbody>
</table>

1.4 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.
1.4.1 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 implement all of the required interfaces 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 or Capability with which this construct is associated.

1.4.2 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 interface 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.
2.0 TRANSACTION DEFINITION

2.1 CONTEXT OVERVIEW

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 audit 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 a 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 (IHE 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 ATNA profile, Section 9.2 begins here:

User Accountability is provided through Audit Trail. The Audit Trail needs to allow a security officer in an institution to audit activities, to assess compliance with a secure domain’s policies, to detect instances of non-compliant behavior, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). PHI is considered to be the patient-identifiable information records (e.g., Registration, Order, Study/Procedure, Reports, Images, and Presentation States). PHI 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 some user: which patients’ PHI was accessed?
- For some patient PHI: which users accessed it?
- What user authentication failures were reported?
- What node authentication failures were reported?

The text for the IHE ATNA profile, Section 9.2 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 Required Output).

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 Required Output).

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

Table 2-1 Transaction Constraints

<table>
<thead>
<tr>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “provisional format” for audit records defined in IHE ATNA shall not be used</td>
<td></td>
</tr>
<tr>
<td>The transport protocol for audit record communication shall be BSD syslog, per the IHE ATNA specification</td>
<td></td>
</tr>
</tbody>
</table>

2.1.2 INTERFACES

All interfaces for this Transaction are described further in the Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework, Volume 2, Section 3.20 (IHE ITI-TF-2).

Table 2-2 Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Used in Component/Composite Standard</th>
<th>Required = R Optional = O Conditional = C&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Record Repository</td>
<td>Provides a repository for audit events</td>
<td>IHE ITI-TF-2</td>
<td>R</td>
</tr>
<tr>
<td>Audit Record Source</td>
<td>Creates and communicates an Audit Record to the Audit Record Repository on behalf of another interface that performs an action requiring logging</td>
<td>IHE ITI-TF-2</td>
<td>R</td>
</tr>
<tr>
<td>&lt;any interface grouped with a Secure Node interface&gt; (e.g., Node)</td>
<td>Any interface from the HITSP Interoperability Specification that is grouped with Secure Node (e.g., The originating or terminating point of information or signal flow in a telecommunications network. This interface is equivalent to the Secure Node in the IHE-ITI-TF ATNA Transaction)</td>
<td>IHE ITI-TF-2</td>
<td>R</td>
</tr>
</tbody>
</table>

---

1 It is anticipated that the Internet Engineering Task Force will publish a syslog-protocol that will provide a more robust alternative to BSD syslog.

2 Optionality = “R” for Required, “R2” for Required if Known or “O” for Optional, or “C” for Conditional. Repeatable = “Y” for Yes, “N” for No.
2.1.3 INTERFACE INTERACTIONS

Figure 2-1 Interface 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 and enable selective reporting to investigate user activity, etc.

2.1.4 PRE-CONDITIONS

Table 2-3 Pre-conditions

<table>
<thead>
<tr>
<th>Pre-condition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A policy defining what is to be audited exists</td>
<td></td>
</tr>
<tr>
<td>Audit Record Repository is active and designated as the destination for recorded audit events</td>
<td></td>
</tr>
<tr>
<td>Audit Record Source is initialized to the audit policy</td>
<td></td>
</tr>
<tr>
<td>Consistent Time construct is a pre-requisite for this Transaction</td>
<td></td>
</tr>
<tr>
<td>Identities are managed</td>
<td></td>
</tr>
<tr>
<td>Policy defining the protection of the log and audit exists and is being enforced</td>
<td></td>
</tr>
</tbody>
</table>
2.1.4.1 PROCESS TRIGGERS

Table 2-4 Process Triggers

<table>
<thead>
<tr>
<th>Process Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>An action requiring logging occurs</td>
</tr>
<tr>
<td>Audit records are created (trigger for communicated)</td>
</tr>
<tr>
<td>Audit records are received (triggers for reports/alarms/alerts)</td>
</tr>
</tbody>
</table>

Various Transaction triggers are described in Table 3.20.6-1 of IHE ITI-TF-2. 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 policies that can be supported by a log standard.

2.1.5 POST-CONDITIONS

Table 2-5 Post-conditions

<table>
<thead>
<tr>
<th>Post-condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit record is created, communicated, stored, and analyzed</td>
</tr>
<tr>
<td>Subsequent action initiated per policy, e.g., reports and other automated actions</td>
</tr>
</tbody>
</table>

2.1.5.1 REQUIRED OUTPUT

Table 2-6 Required Outputs

<table>
<thead>
<tr>
<th>Required Output</th>
<th>Format/Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit record</td>
<td>Defined in Section 3.20.7.1 of IHE-ITI-TF-2</td>
</tr>
<tr>
<td>Security audit alarms</td>
<td>Defined in ISO 10164-7</td>
</tr>
<tr>
<td>Security report</td>
<td>Defined in ASTM E2147-01</td>
</tr>
</tbody>
</table>

2.1.6 DATA FLOWS

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

2.2 LIST OF HITSP CONSTRUCTS

Table 2-7 List of HITSP Constructs

<table>
<thead>
<tr>
<th>Construct Name</th>
<th>Description</th>
<th>Event/Action Code</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable HITSP constructs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2.1 CONSTRUCT DEPENDENCIES

Table 2-8 Construct Dependencies

<table>
<thead>
<tr>
<th>Construct</th>
<th>Depends On (Name of Component that it depends on)</th>
<th>Dependency Type (Pre-condition, post-condition, general)</th>
<th>Purpose (Reason for this dependency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable dependencies</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

Table 2-9 Additional Constraints on Required Constructs

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Construct</th>
<th>Constraint</th>
<th>Constraint Type (Pre-condition, post-condition, general)</th>
<th>Purpose (Reason for this constraint)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable dependencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-10 Regulatory Guidance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No applicable regulatory guidance</td>
<td></td>
</tr>
</tbody>
</table>

2.3.2 SELECTED STANDARDS

Table 2-11 Selected Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication (ATNA) Integration Profile</td>
<td>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 interface specific requirements. The latest version of the IHE Technical Framework is available at <a href="http://www.ihe.net">www.ihe.net</a></td>
</tr>
</tbody>
</table>

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-12 Informative Reference Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASTM International Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems: # E2147-01</td>
<td>E2147-01 &quot;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).&quot; For more information visit <a href="http://www.astm.org">www.astm.org</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>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 <a href="http://www.iso.org">www.iso.org</a></td>
</tr>
</tbody>
</table>
3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.
4.0 DOCUMENT UPDATES

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

4.1 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

4.2 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.

4.3 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:


4.4 AUGUST 27, 2008

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

4.5 DECEMBER 10, 2008

Minor editorial changes were made to this construct.

Minor editorial updates for standards version change to IHE ITI-TF Revision 5. Also updated quoted text from underlying standard that has been modified with the updated standard.

4.6 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

4.7 JUNE 26, 2009

Per public comment issue ID 7067, the SPI committee deleted last line of Table 2-3, so that Secure Node is no longer a required pre-condition.

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

---

HITSP Collect and Communicate Security Audit Trail Transaction
Released for Implementation
20090708 V1.4
4.8 JULY 8, 2009

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