Audit Requirements

(Security Enhancements for OpenEMR-MUO)

Version 1.0

By ViCarePlus Team

Prepared by

ViSolve Inc.,
Contact: 408.666.4320
EMail: vicareplus_engg@visolve.com
www.visolve.com

19th December 2009

Table of Contents

Revision History

Version	Date	Author	Reviewed By
1.0	12/19/09	ViCarePlusTeam	-

1. Audit Requirements - Brief

Requirements from “Certification Standards Committee” [http://health.state.mn.us/e-health/standards/certrecs102609.pdf]

1. Provide the capability to record and examine activity in information systems that contain or use electronic protected health information.

2. Provide the capability to use the ATNA profile to communicate audit messages between Secure Nodes and to establish Audit Repository nodes to collect audit information.

Note: The same is mentioned by the CCHIT - EHR ARRA 2011 Preliminary Certification as part of the Security Criteria related to Audit [http://www.cchit.org/sites/all/files/Preliminary%20ARRA%202011%20Security%20Criteria%20200910 01_0.pdf]

2. Auditing Requirements - Detail

Sources Referred:
1. Documents specified in the above section
2. CCHIT Ambulatory Requirements for Audit control
[**http://www.cchit.org/sites/all/files/CCHIT%20Certified%202011%20Ambulatory%20EHR%20Criteria%2020091006.pdf**]

2.1 Auditing EHR

Note: [The following requirements are taken from CCHIT Ambulatory Requirements

2.1.1. Configurable audit events

Inclusion or exclusion of auditable events based on organizational policy & operating requirements/limits.

2.1.2 Events to be audited *[from the Appendix of CCHIT Ambulatory Requirements for Audit Control]*

- start/stop
- user login/logout
- session timeout+F10
- account lockout
- patient record created/viewed/updated/deleted
- scheduling
- query
- order
- node-authentication failure
- signature created/validated
- PHI export (e.g. print)
- PHI import
- security administration events
- backup and restore

2.1.3 Information to be logged

- date and time of the event;
- the component of the system (e.g. software component, hardware component) where the event ccurred;
- type of event (including: data description and patient identifier when relevant);
- subject identity (e.g. user identity); and
- the outcome (success or failure) of the event.

2.1.4 Option for flexible time stamps

2.1.5 Audit – Access Control

- Allowing only certain users to read the audit records
- Protecting the audit records from unauthorized deletion
- Preventing modifications to the audit records

2.2. Communicate Audit messages between secure nodes

ATNA Format: Rfc-3881 defines an XML schema for reporting events that are relevant to security and privacy auditing.

Two audit message formats

- IHE Radiology interim format, for backward compatibility with radiology
- IETF/DICOM/HL7/ASTM format, for future growth
  - DICOM Supplement 95
  - IETF Draft for Common Audit Message
  - ASTM E.214
  - HL7 Audit Informative documents

Both formats are XML encoded messages, permitting extensions using XML standard extension mechanisms

ATNA Transfer Protocol: The Audit Trail and Node Authentication Integration Profile specifies the use of Reliable Syslog Cooked Profile (RFC-3195, Section 4) as the mechanism for logging audit record messages to the central audit record repository

2.3. Establish Audit repository nodes to collect audit information

<<To be explored>>

2.4. Time Synchronization using NTP/SNTP

Synchronizing with Time Server using NTP. (SNTP is optional)

3. Audit & ATNA – Actual Tasks

3.1 Creating a "Secure Node"

A Secure Node is one which has the following features incorporated

1. User Authentication – requires only local user authentication

2. Connection Authentication
   Use of bi-directional certificate based node authentication for connections to and from node.The DICOM, HL7, and HTTP protocols all have certificate-based authentication mechanisms defined.

3. Time Synchronization using CT (Consistent Time) profile

HITSP Profile to be used: http://wiki.hitsp.org/docs/T17/T17-2.html#_Toc234742517

3.2 Communicate Audit Messages between Secure Nodes

3.2.1 Auditing the following auditable events

S#	Audit Event	Detail
1	Actor-start-stop	*The starting or stopping of any application or actor*
2	Audit-log-used	*Reading or modification of any stored audit log*
3	Begin-storing-instances	*The storage of any persistent object, e.g. DICOM instances, is begun*
4	Health-service-event	*Other health service related auditable event*
5	Images-availability-query	*The query for instances of persistent objects.*
6	Instances-deleted	*The deletion of persistent objects.*
7	Instances-stored	*The storage of persistent objects is completed.*
8	Medication	*Medication is prescribed, delivered, etc.*
9	Mobile-machine-event	*Mobile equipment is relocated, leaves the network, rejoins the network*
10	Node-authentication-failure	*An unauthorized or improperly authenticated node attempts communication*
11	Order-record-event	*An order is created, modified, completed.*
12	Patient-care-assignment	*Patient care assignments are created, modified, deleted.*
13	Patient-care-episode	*Auditable patient care episode event that is not specified elsewhere.*
14	Patient-record-event	*Patient care records are created, modified, deleted.*
15	*PHI-export*	*Patient information is exported outside the enterprise, either on media or electronically*
16	*PHI-import*	*Patient information is imported into the enterprise, either on media or electronically*
17	*Procedure-record-event*	*The patient record is created, modified, or deleted.*

18	*Query-information*	*Any auditable query not otherwise specified.*
19	*Security-administration*	*Security alerts, configuration changes, etc.*
20	*Study-object-event*	*A study is created, modified, or deleted.*
21	*Study-used*	*A study is viewed, read, or similarly used.*

Ref: http://www.ihe.net/Participation/upload/IHE-ITI-ATNA-CT-08.ppt

3.2.2 Audit Message Format Implementation

RFC3881 - Security Audit and Access Accountability Message XML

Ref: http://www.faqs.org/rfcs/rfc3881.html

3.2.3 Configuring Audit Transport Protocol

Reliable Syslog (RFC 3195) is the preferred transport for Audit Records.

The above derived XML format needs to be transferred via Syslog protocol. Does our understanding correct?
http://publicaa.ansi.org/sites/apdl/IOLib/T15__Collect_and_Communicate_Security_Audit_Trail.pdf

4. Questions

1. What type of events to be considered for logging? 3.2.1 (Proposed by ATNA) or 2.1.2 (Proposed by CCHIT)
2. Communicate Audit messages can be achieved by implementing HITSP construct – HITSP/T15. Does our understanding correct?
3. Does creating a secure node using HITSP/T17 (http://wiki.hitsp.org/docs/T17/T17-2.html#_Toc234742517) part of this exercise?
4. Can we assume “Audit Repository Node” (which is part of HIE) is already present?

5. HITSP Standards

HITSP/T17 – Secured Communication Channel
HITSP/T15 – Collect and Communicate Security Audit Trail
(http://wiki.hitsp.org/docs/T15/T15-3.html)

References

1. **Product Certification Standards -** http://health.state.mn.us/e-health/standards/certrecs102609.pdf
2. **Audit Trail and Node Authentication -** http://www.ihe.net/Participation/upload/IHE-ITI-ATNA-CT-08.ppt
3. **RFC 3881 -** http://www.faqs.org/rfcs/rfc3881.html
4. **About ATNA -** http://www.waset.org/journals/waset/v54/v54-33.pdf

Appendix A CCHIT Ambulatory Requirements for Audit control

Reference :
http://www.cchit.org/sites/all/files/CCHIT%20Certified%202011%20Ambulatory%20EHR%20Criteria%2020091006.pdf

S#	SC 02.01	The system shall allow an authorized administrator to set the inclusion or exclusion of auditable events in SC 02.03 based on organizational policy & operating requirements/limits.
	SC 02.02	The system shall support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile
	SC 02.03	The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include those listed in the Appendix Audited Events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.
	SC 02.04	The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.
	SC 02.05	The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).
	SC 02.06	The system shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.
	SC 02.07	The system shall have the ability to format for export recorded time stamps using UTC based on ISO 8601. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time.
	SC 02.08	The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit records.