Healthcare Audit Use Cases

# List of Audit Use Case Titles

* Consolidated and Cross-Coordinated Enterprise Audit
  + Detect Audit Event[[1]](#footnote-1)
  + Create Audit Event1
  + Submit Audit Records[[2]](#footnote-2)
  + Retrieve Audit Records2
* Audit support for disclosure reporting
  + Retrieve Disclosure Records2
* Real-time Alerts and Alarms
  + Prioritize Alarm1
  + Initiate Alarm1
* Dynamic and real-time threat detection and response
  + Verify Event Source1
  + Apply Disposition Criteria1
  + Using Audit Logs to Detect Possible attacks[[3]](#footnote-3)
  + Detection of Insider Threat3
    - Using Audit Logs to Monitor Acceptable Use
  + Suspicious Behavior of Log Source3
    - Expected host/log source not reporting
    - Unexpected events per second from log sources
* Log History of Changes
  + System retains history of create and change dates and IDs on all records (objects, procedures, vocabularies).
  + Programmer can produce a listing of changes for certain time periods and/or certain record types.
  + User with appropriate permissions can view history of changes for records.
* Archive Audit Trails1

# Format of Use Cases[[4]](#footnote-4)

## UML Diagram



## Use Case Descriptions

### Use Case AU-1: Submit Audit Record[[5]](#footnote-5)

#### Description

Invoke a function to submit a record of an auditable event.

#### Assumptions

* In order for an audit trail to effectively support one or more distributed Audit Event Sources, those Sources, and all Audit Service components must maintain consistent time from a designated authoritative time service. The accuracy requirement of the coordinated timekeeping is a policy decision.
* Appropriate security controls are in place to ensure that adequate protection of the audit event information both in transit and at rest.

#### Actors

Audit Event Source

#### Trigger Event

The use case is triggered when one or more records of auditable events are ready to be transmitted[[6]](#footnote-6).

#### Pre-conditions

* The audit event source has been configured with the endpoint address of the Audit Service(s).

#### Post-conditions

* The Audit Service has accepted the audit event record(s).

### Use Case AU-2: Retrieve Disclosure Records[[7]](#footnote-7)

#### Description

Provide a mechanism to extract information to support downstream production of accounting of disclosure reports. Return disclosure records that may subsequently be used to identify disclosure of PHI.

#### Assumptions

* Complete privacy accounting extends beyond the scope of the events captured by any electronic health system and includes handling of PHI that is not in electronic form. As a result the Audit Service may not be sole source of information required to enable the production of downstream reports.
* This capability will not have the ability to directly detect all potentially non-compliant behavior; however it can be used to support the identification of such behavior.
* We expect that the data provided by this capability will be supplemented by mechanisms that will allow identities in the record to be resolved.

#### Actors

* Audit Record Repository
* Privacy Accounting Component

#### Trigger Event

The use case is triggered by a request for disclosure information.

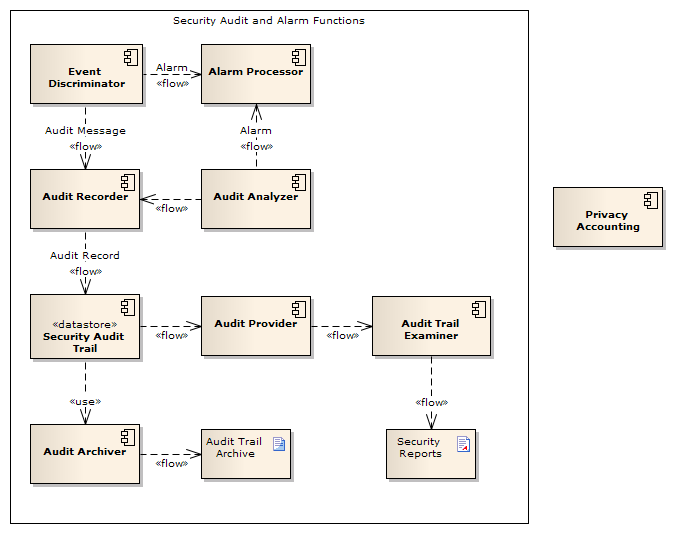
#### Pre-conditions

* The Privacy Accounting component has the appropriate authority to access the capability.

#### Post-conditions

* All available information that satisfies the request criteria has been returned to the invoking Actor.

## Work Flow Example for Security Audit and Alarm Functions[[8]](#footnote-8)



1. VHA Audit Functional Model and SRSC audit requirements. [↑](#footnote-ref-1)
2. HL7 PASS Healthcare Audit Control Services draft standard. [↑](#footnote-ref-2)
3. Derived from Top 6 *Security Incident and Event Management (SIEM) Use Cases*, http://resources.infosecinstitute.com/top-6-seim-use-cases/ [↑](#footnote-ref-3)
4. HL7 PASS Healthcare Audit Control Services draft standard. [↑](#footnote-ref-4)
5. An instance of the refinement of this use case into specifications at the Platform Specific level has been completed as DICOM Supplement 95 (ISO TS 12052), and the Record Audit Event transaction of the IHE ATNA specification (see Appendix B). These specifications are referenced in this document in the appropriate sections. [↑](#footnote-ref-5)
6. The use case is not necessarily triggered by the occurrence of an auditable event, although it can be. Generally, the Audit Event Source determines when conditions are appropriate to submit the audit event information. [↑](#footnote-ref-6)
7. See HL7 Composite Privacy Domain Analysis Model DSTU, December 9, 2009 – pg 56 – Accounting of Disclosures. [↑](#footnote-ref-7)
8. HL7 PASS Healthcare Audit Control Services draft standard. [↑](#footnote-ref-8)