Integrating the Healthcare Enterprise

IHE IT Infrastructure
Technical Framework Supplement

Add RESTful Query to ATNA

Rev. 2.1 – Trial Implementation

Date: August 5, 2016
Author: IHE ITI Technical Committee
Email: iti@ihe.net

Please verify you have the most recent version of this document. See here for Trial Implementation and Final Text versions and here for Public Comment versions.

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework V13.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

This supplement is published on August 5, 2016 for trial implementation and may be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure Technical Framework. Comments are invited and may be submitted at http://www.ihe.net/ITI_Public_Comments.

This supplement describes changes to the existing technical framework documents.

"Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume.

Amend Section X.X by the following:

Where the amendment adds text, make the added text **bold underline**. Where the amendment removes text, make the removed text **~~bold strikethrough~~**. When entire new sections are added, introduce with editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.

General information about IHE can be found at: http://ihe.net.

Information about the IHE IT Infrastructure domain can be found at: http://ihe.net/IHE_Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at: http://ihe.net/IHE_Process and http://ihe.net/Profiles.

The current version of the IHE IT Infrastructure Technical Framework can be found at: http://ihe.net/Technical_Frameworks.

CONTENTS

Introduction to this Supplement

Event logging is a system facility that is used by healthcare applications and other applications.

This supplement updates the Audit Trail and Node Authentication (ATNA) Profile. ATNA defines a standardized way to create and send audit records; however, it does not identify a standardized way to retrieve audit records collected by an Audit Record Repository.

This supplement adds Retrieve capabilities to the Audit Record Repository (ARR). This profile defines a new actor, the Audit Consumer, and two new transactions:

1. [ITI-81] Retrieve ATNA Audit Event is a transaction that allows an Audit Consumer to retrieve ATNA Audit Events stored within a target Audit Record Repository. This transaction is based on a FHIR®[1] RESTful search operation on AuditEvent resources.
2. [ITI-82] Retrieve Syslog Event is a transaction that allows an Audit Consumer to search syslog messages stored in an Audit Record Repository. This transaction is defined as a RESTful operation. The search parameters are based on syslog metadata.

Note that ATNA Audit Events are syslog events, so the transaction [ITI-82] Retrieve Syslog Event enables search of ATNA events based on syslog metadata values.

Open Issues and Questions

1. Readers are asked to evaluate to what extent filters should be specified and required within the Filter and Forward Option. Do they seem to be applicable to any implementation that claims this option?
2. There is the possibility to extend this filter capability requirement aligning the type of mandatory filters with mandatory query parameter defined for Audit Record Query transaction (see Section 9.3.2).
3. Only a JSON return format is specified for Retrieve Syslog Messages [ITI-82]. It delivers a slightly parsed form of the syslog message that makes JSON attributes in a structure that corresponds to the structure define by syslog. Should other forms be supported? Should the unparsed syslog message be returned?
4. Should there be retrieve methods to get “most recent N events”? This would be a non-deterministic and constantly varying response in most cases.
5. Should a server information query be specified? There are various RFCs from the IETF that specify aspects of server information.
6. Should support of the “/.well-known/” path RFC5785 be required or described in transactions ITI-81 and ITI-82? (This can be an alternative to more complete server

[1] FHIR is the registered trademark of Health Level Seven International.

information.) For example, PACS servers providing restful access to DICOM®[2] objects may respond to "/.well-known/DICOM" in addition to a fully specified URL path.

7. Should the server be required to error for lack of a time period in ITI-81 and ITI-82 or should this be weakened to "should" or "recommend" or "may"?
8. Transaction ITI-81 is based on a FHIR query operation. Not all the search parameters defined in this transaction are actually standard FHIR search parameters. A CP to FHIR is submitted to add "outcome" and "role" as standard search parameters (CP #9919 http://gforge.hl7.org/gf/project/fhir/DSTU2/tracker/?action=TrackerItemEdit&tracker_item_id=9919).
9. The start-time and stop-time in <date> search parameters shall be in RFC 3339 format. Do we need to further constrain the format of this parameter? Is this precise enough? Doesn't it allow for date and month only? For 6 digit fractions of seconds? Or for date-time with timezones? How is matching done then (e.g., Z vs +00:00)? Right now we leverage on FHIR matching criteria.
10. Tech cmte has documented the query to patient.identifier, starting from a search parameter of type "reference". Does this reflect the FHIR requirements in the correct way?

Closed Issues

1. This supplement is being written as additions to the ITI TF-1:9, ATNA, which was written to an older outline template. Rather than redocument ATNA entirely, these section are added using that outline, not the new template. The new sections all fit appropriately into either outline.

   The Report Audit Event Transaction [ITI-20] is completely rewritten to the current template outline. It was old and written to a very different outline than the current template structure. Merging in the options and their effect on this transaction became very confusing.
   The Node Authentication Transaction [ITI-19] is not affected by this supplement.
2. What audit event log sources should be defined to be supported by the query transaction? The table below is a partial list of event sources. This list is the combination of event sources supported by a variety of event management software.

   Decision: this version will only mandate support for the IHE ATNA formats and the generic SYSLOG format. The many other formats and transports can be added later as options or by vendors as product options.
   Examination of a variety of event reporting and logging products resulted in the following list of sources. After discussion and given scope concerns, no additional sources or encodings will be described.

[2] DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

Partial List of event sources/codecs considered

Name of source	Decision
IHE ATNA	Support
Collectd	No (perhaps future)
Elasticsearch	No (perhaps future)
Eventlog	No (perhaps future)
Imap	No (perhaps future)
Log4j	No (perhaps future)
Lumberjack	No (perhaps future)
S3	No (perhaps future)
Snmp	No (perhaps future)
Syslog	Support
Twitter firehose	No (perhaps future)
Xmpp	No (perhaps future)
Zeromq	No (perhaps future)
Edn	No (perhaps future)
Fluent	No (perhaps future)
Json	No (perhaps future)
Spool	No (perhaps future)
FHIR	No (perhaps future)

3. Event transports were selected as part of the planning decision for this work item. Technical evaluation found no issues with it.

Name of source	Short Description	Issues
IHE ATNA	Covered in this supplement	None
Syslog	Covered in this supplement	None

4. Candidate Query “standards”

   A variety of existing event management products and standards were examined. Most of the existing system use product specific plug-ins, direct database access, or other methods for providing query access.
   After review, four candidates were considered worth further evaluation.

Name of source	Short Description	Decision
DCM4CHE	Open Source implementation of PACS archive including ARR as well as much else. At least 5,000 operational downloads, but most probably not for ARR use.	Evaluate

Name of source	Short Description	Decision
Tiani Spirit EHR (awaiting formal name)	EU Public specification. Implementation underway.	Evaluate
Connect / Healtheway/ ?	Published specification. Need to determine license, etc., but probably suitable.	Evaluate
FHIR Security Event Report	Query of a FHIR resource	Evaluate
Plug-in style (multiple)	A variety of product specific mechanisms to write plug-ins for that product.	Reject, too product specific, subject to change at will by product vendor
Direct access to database (multiple)	A variety of product specific mechanisms that document the format and access methods for the internal database used by the product.	Reject, too product specific, subject to change at will by product vendor
Direct access to flat files (multiple)	A variety of product specific mechanisms that document the format and access methods for flat files of messages created by the product.	Reject, too product specific, subject to change at will by product vendor

The surviving four were evaluated against the ITI list of evaluation criteria. The general spreadsheet was reviewed and the following table is the result.

200 **Evaluation Criteria Results**

Criteria	DCM4CHE	Tiani Spirit EHR	Connect/Healtheway	FHIR (SecurityEvent)
Stability		Early development	Has been deprecated	DSTU
From an SDO	No	Govt specification	Govt specification	Yes
Licensing restrictions	LGPL v2		?	CC 0
Implementation Experience	Approx 5K installations			Hackathons, Connectathons
Ease of adoption	Open Source			Will be easy
RESTful/SOAP/other	RESTful	SOAP		RESTful
ATNA specific query	Yes	Yes	Yes	Kind-of
Generic SYSLOG query	No	No	No	No
Phase 1 decision	Continue evaluation	Drop	Drop	Continue evaluation
Acceptance by Intrusion Detection/ Security Analysis vendors	?	n.a.	n.a.	?

Decision:
FHIR was selected as the standard to be used to profile the Query transaction. The FHIR event report is managed as a joint effort among HL7®[3] FHIR, IHE, and DICOM. This makes coordination of the necessary resource changes fairly straightforward.
In order to use FHIR the following modification/extension/addition to the query will be needed:

- We need the same functional capabilities as DCM4CHE. The large installed base of DCM4CHE indicates that the functionality is widely needed. Adapting this functionality to use a FHIR query is a reasonable change if the functional capabilities do not need to change significantly.
- The generic Syslog query will not fit a FHIR query. This was made optional and a simple query that is similar to FHIR was defined.

The major risk item is coordinating release and preparation schedules. In order to fit HL7 publication schedule a reasonable version of the resource and query are needed by 22 March 2015. Revisions based upon public comment and TI experience can be handled during the FHIR DSTU cycle.

5. Should we define an actor and transaction for the other syslog messages that are not ATNA schema compliant? Should we mandate support for this kind of message from any secure actor? From any secure node? Or, should these filtering these messages only be mandated when originating on an ATNA compliant node, and support for other nodes be left as a product option?

   Decisions: The Filter and Forward transaction explicitly state that syslog messages not compliant with ATNA schema can be received. Those messages should be sent using the same protocol requirement defined for ATNA. This was addressed in the ITI-20 rewrite. The query for generic syslog messages was defined and is similar to FHIR in some respects. It is made optional.

6. Should Audit Record Repository always be required grouping with secure node/application or only when it does forwarding? ARR often have lots of PHI, so secure node may be generally appropriate. What about all the other syslog uses?
   Decision: Not needed the SN/SA grouping for the store/forward option. The text in the options section is sufficient. We have the need to track the Query event without using all the requirements introduced by the SN grouping, so there is no requirement to send the audit to another repository via TLS.

7. The Retrieve Syslog Message [ITI-82] only mandates support for query to return all syslog messages with timestamps within a time window. Should any other queries be mandated? **Decision:** NO

8. The query option is silent about how the Audit Record Repository determines which syslog messages are stored for later query, how long messages remain available for

[3] HL7 is the registered trademark of Health Level Seven International.

query, etc. Should there be any requirements put on this? The motivation for this is the wide range of real world situations, ranging from sites that must process tens of thousands of syslog messages per second to sites that manage a few hundred per day. Some sites deal only with major level ATNA security events. Some sites deal with syslog reports of every network connection, ping, firewall warning, etc. **Decision:** New ITI-20 makes it clear that these issues are decided during implementation and deployment.

9. Have two endpoints - one for syslog, one for ATNA? Have one and let parameters separate? Have two and permit ATNA parameters on syslog? Have two and permit syslog parameters ATNA (FHIR will generate 400 - bad request unless there is a FHIR extension defined)? **Decision:** two endpoints, one FHIR based and one for generic syslog.
10. Should Audit Record Repository always be required grouping with secure node/application or only when it does forwarding? ARR often have lots of PHI, so secure node may be generally appropriate. What about all the other syslog uses?

Considerations: The logging of the query event is clearly appropriate. However, there are requirements introduced by the ATNA Secure Node that are not applicable to our scenario where the Audit Source IS the Audit Record Repository itself: the ARR is required to send audit records via UDP or TLS. We SHOULD mandate the creation of audit records structured in accordance to ATNA structure and no other transport requirements. There is another point to take in consideration: once the ATNA query is made, an audit record is created. Should this audit be returned into the same transaction (query Response)?
Answer: This is a very important implementation decision, and IHE cannot define requirement for this.

General Introduction

Appendix A - Actor Summary Definitions

Add the following actors to the IHE Technical Frameworks General Introduction list of actors:

Actor	Definition
Audit Consumer	Query for syslog and ATNA audit records using Syslog metadata and ATNA audit record content. Subsequent processing of the query result is not defined.

Appendix B - Transaction Summary Definitions

Add the following transactions to the IHE Technical Frameworks General Introduction list of Transactions:

Transaction	Definition
Retrieve ATNA Audit Event [ITI-81]	Retrieve Audit Records. Search ATNA audit records based upon queries using ATNA audit record content.
Retrieve Syslog Event [ITI-82]	Retrieve Syslog Messages. Search syslog messages based upon using the syslog metadata.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

Glossary Term	Definition
Syslog metadata	Attributes that classify the audit record defining: severity of the event, facility, and application that sent the message. These are defined in RFC 5424.
Syslog message	Any message that complies with RFC 5424, regardless of the format of the message body. An ATNA audit log message is a specific kind of syslog message that has a specific format for the message body.
Audit Record	A syslog message that complies with the DICOM PS3.15 schema.

Volume 1 – Profiles

Editor: Update Section 9 adding the following text at the end of that section:

9 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication (ATNA) Profile specifies the foundational elements needed by all forms of secure systems: node authentication, user authentication, event logging (audit), and telecommunications encryption. It is also used to indicate that other internal security properties such as access control, configuration control, and privilege restrictions are provided.

Many other IHE profiles require or recommend grouping with ATNA actors as part of their security considerations.

The ATNA Profile also defines optional capabilities to retrieve messages stored in an Audit Record Repository (ARR) using the Audit Consumer Actors and transactions:

- **Retrieve ATNA Audit Event [ITI-81] is a transaction that enables an Audit Consumer to retrieve ATNA Audit Events stored within a target Audit Record Repository. This transaction is based on a FHIR RESTful search operation on AuditEvent resources.**
- **Retrieve Syslog Event [ITI-82] is a transaction that enables an Audit Consumer to search syslog messages stored in an Audit Record Repository. This transaction is defined as a RESTful operation. The search parameters are based on syslog metadata.**

Note that ATNA Audit Events are syslog events, so the Retrieve Syslog Event [ITI-82] transaction enables retrieval of ATNA events based on syslog metadata values.

Editor: Replace Figure 9.1-1 with the following. Note that in the figure below, the existing actors and transactions are shown in dashed lines. The figure should be updated by adding the actors and transactions in solid lines: Audit Consumer, Retrieve ATNA Audit Record, Retrieve Syslog Event.

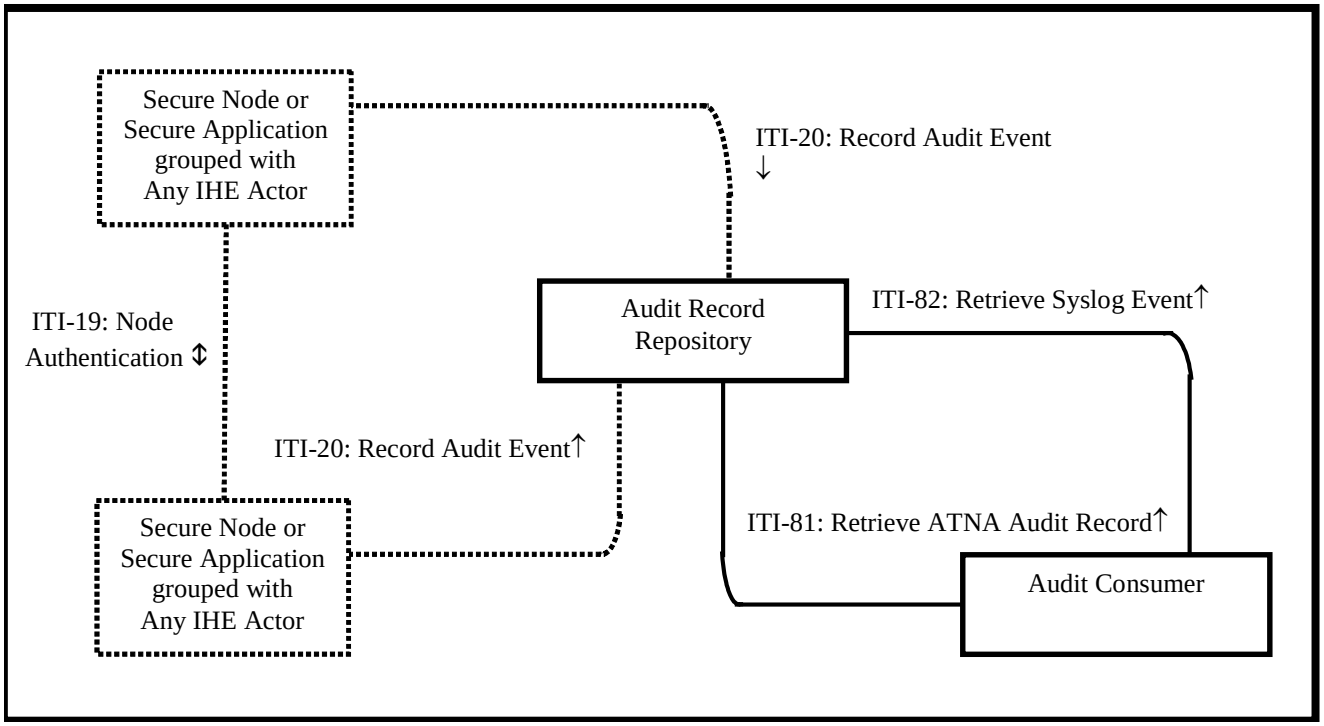


Figure 9.1-1: Audit Trail and Node Authentication Diagram

Editor: Update Section 9.1.1.3 as follows:

9.1.1.3 Audit Record Repository

The Audit Record Repository receives event audit reports and stores them. It may be part of a federated network of repositories. It is expected to have analysis and reporting capabilities, but those capabilities are not specified as part of this profile. This profile does not specify the capacity of an Audit Record Repository, because the variety of deployment needs makes it impractical to set requirements for the event report volume or capacity needed.

The Audit Repository shall support:

1. Both audit transport mechanisms specified in ITI TF-2a: 3.20.
2. Receipt of all IHE-specified audit message formats. Note that the message format is extensible to include both future IHE specifications (e.g., audit requirements for new IHE transactions) and private extensions.
3. Local security and privacy service protections and user access controls.

Optionally the Audit Record Repository supports search capabilities as defined in ITI TF-2c: 3.81 and ITI TF-2c: 3.82.

Editor: Add new Section 9.1.1.4

9.1.1.4 Audit Consumer

The Audit Consumer queries an Audit Record Repository for syslog and ATNA audit records using Syslog metadata and ATNA audit record content. Subsequent processing of the query result is not defined in this profile.

Editor: In Section 9.4, Update Table 9.4-1

Table 9.4-1: ATNA Profile - Actors and Transactions

Actors	Transactions	Optionality	Reference
Audit Record Repository	Record Audit Event [ITI-20]	R	ITI TF-2a: 3.20
	Retrieve ATNA Audit Event [ITI-81]	**O**	**ITI TF-2c: 3.81**
	Retrieve Syslog Event [ITI-82]	**O**	**ITI TF-2c: 3.82**
Audit Consumer	**Retrieve ATNA Audit Event [ITI-81]**	**O**	**ITI TF-2c: 3.81**
	Retrieve Syslog Event [ITI-82]	**O**	**ITI TF-2c: 3.82**
Secure Node	Authenticate Node [ITI-19]	R	ITI TF-2a: 3.19
	Record Audit Event [ITI-20]	R	ITI TF-2a: 3.20
Secure Application	Authenticate Node [ITI-19]	R	ITI TF-2a: 3.19
	Record Audit Event [ITI-20]	R	ITI TF-2a: 3.20

Editor: Update ITI TF-1:9.2 as shown, including the note under Table 9.2-1.

9.2 ATNA Integration Profile Options

Options that may be selected for this Integration Profile are listed in the Table 9.2-1 along with the actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 9.2-1: ATNA - Actors and Options

Actor	Option Name	Vol. & Section
Audit Record Repository	**Retrieve Audit Message**	**ITI TF-1: 9.2.3**
	Retrieve Syslog Message	**ITI TF-1: 9.2.4**
Audit Consumer	**Retrieve Audit Message (Note 1)**	**ITI TF-1: 9.2.3**
	Retrieve Syslog Message (Note 1)	**ITI TF-1: 9.2.4**
Secure Node	Radiology Audit Trail	RAD TF-1: 2.2.1; RAD TF-3: 5.1
Secure Application	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3:5.1

Note 1: The Audit Consumer shall support at least one of the two options defined.

Editor: Add new Sections 9.2.3 and 9.2.4 to ITI TF-1:9.2

9.2.3 Retrieve Audit Message Option

The Retrieve Audit Message Option enables search requests for audit records based upon message contents.

An Audit Consumer or Audit Record Repository that supports this option shall implement the Retrieve ATNA Audit Event [ITI-81] transaction.

The [ITI-81] transaction is profiled as a RESTful search from an Audit Consumer to an Audit Record Repository (ARR) using FHIR resources. The search response will reflect the contents of the data storage at the time of the search. IHE does not specify the criteria for message selection, archival, retention interval, etc. These are set by local policy and are often different for different Audit Record Repositories.

9.2.4 Retrieve Syslog Message Option

The Retrieve Syslog Message Option enables search requests for syslog messages based upon syslog metadata.

An Audit Consumer or Audit Record Repository that supports this option shall implement the Retrieve Syslog Event [ITI-82] transaction.

The [ITI-82] transaction is profiled as a RESTful search operation that searches syslog messages of any format or schema. The search request uses the syslog metadata only.

Editor: make the following changes in Table 9.3-1.

Table 9.3-1: ATNA - Required Actor Groupings

ATNA Actor	Actor to be grouped with	Reference	Content Bindings Reference
Audit Consumer	**ATNA Secure Node or Secure Application**	**ITI TF-1: 9.1**	**N/A**
Secure Node	Consistent Time / Time Client	ITI TF-1: 7.1	N/A
Secure Application	Consistent Time / Time Client	ITI TF-1: 7.1	N/A
Audit Record Repository	Consistent Time / Time Client	ITI TF-1: 7.1	N/A

Editor: Make the following changes in Section 9.4

9.4 ATNA Overview

…

Sections 9.4.2.1, 9.4.2.2, and 9.4.2.3 describe typical situations in which authorized users, unauthorized users, and unauthorized nodes attempt to gain access to protected health information (PHI).

Sections 9.4.2.4 and 9.4.2.5 describe use cases related to the retrieve capabilities of the Audit Record Repository.

Editor: Add new Sections 9.4.2.4, 9.4.2.5 and 9.4.3

9.4.2.4 Clinician Personal History of Study views process flow

A clinician wants to gather the history of studies she has accessed during her clinical activity using different devices (EHR system, WebApp, Mobile device). This information allows the clinician to:

- Discover unexpected accesses made to her devices;
- Re-evaluate clinical decisions taken;
- Consolidate on a unique device, a complete picture of complex clinical cases.

9.4.2.4.1 Clinician Personal History of Study views use-case

Dr. Luisa White usually performs her clinical activity using multiple devices. Mr. Brown is a patient who is home-monitored. Dr. White collects results of home visits using a tablet, and she monthly performs a detailed visit with Mr. Brown in her office. During home visits, Dr. White

analyzes tele-monitoring data collected by some devices (scales, blood pressure devices, etc.) and adjusts drugs therapies in accordance with those data. When Dr. White accesses Mr. Brown's data via these devices, each access is tracked as an ATNA audit event. Both document views and document creation are logged, tracking the user that performed the transaction (e.g., using an XUA identity assertion).

Monthly visit, Dr. White wants to consolidate within her EHR system the whole history of data analyzed and collected using multiple devices. This process allows Dr. White to keep track of her clinical activities and revaluate clinical decisions made in the past.

To facilitate that, the EHR system can query for audit events related to transactions performed by Dr. White during a specific period.

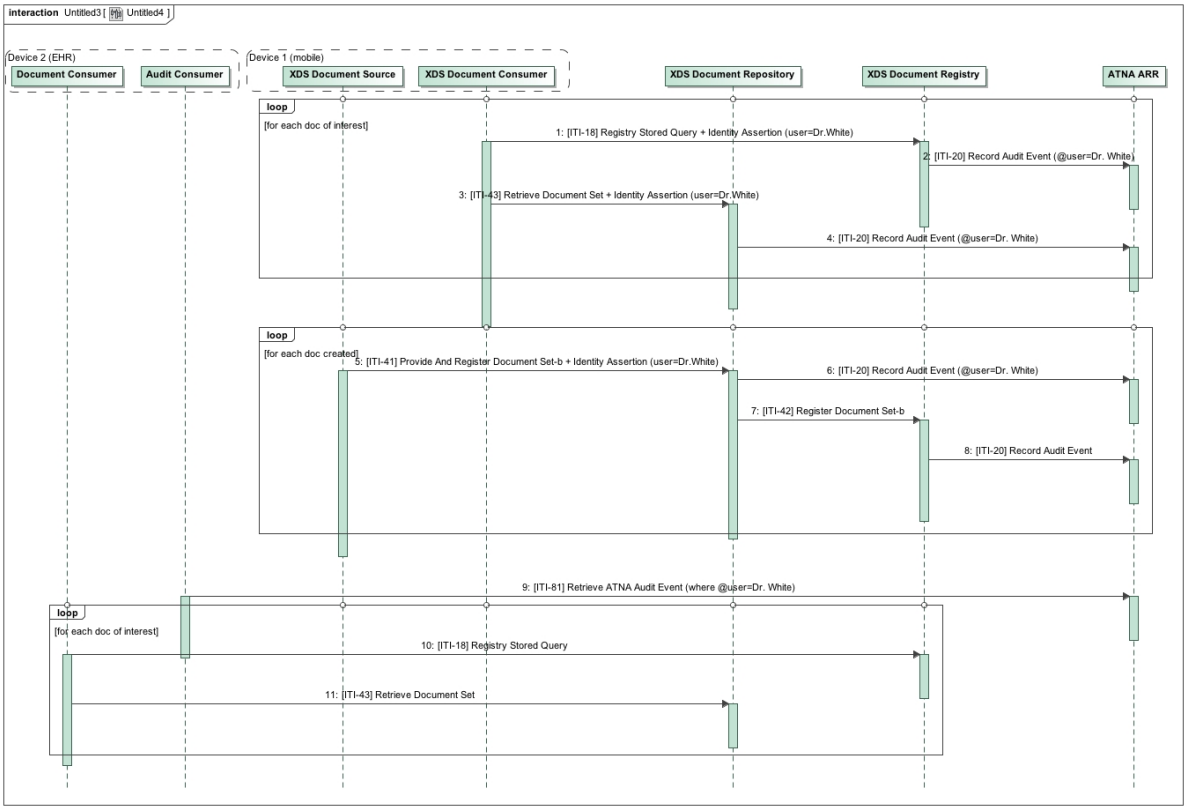


Figure 9.4.2.4.1-1: Clinician Personal History of Study views process flow

9.4.2.5 Patient access to his audit records process flow

A patient wants to discover the list of people that accessed a specific study. Using those data, the patient discovers if privacy policies were correctly applied.

9.4.2.5.1 Patient access to his audit records use case

During a hospitalization, Mr. Brown was asked to sign a consent to share documents produced during that clinical event with a research facility, so that researchers could analyze the efficiency of the applied treatment. Mr. Brown does not provide this consent because he is worried that his data could be used for marketing purposes. A nurse collects the patient's consent document, but forgets to record his decision in the HIS system.

Access to all the data collected during Mr. Brown's hospitalization, by clinicians involved in his care are tracked as "Export" or "Disclosure events for a "Treatment" purpose. An access to the data by the research facility would be tracked as "Export" or "Disclosure" events for a "Research" purpose. Mr. Brown's healthcare facility provides on-line access to health information. Mr. Brown can use a web app to access this data (shared using XDS or XCA infrastructure). The web app can also display audit information related to those documents/studies. Audit records are collected by many ATNA Audit Record Repositories, but local policies or system configurations allows the web app to identify the right Audit Record Repository system that stores relevant records. Using the document and study identifiers, the web app can query the appropriate ATNA Audit Record Repository.

The web app reports to Mr. Brown that his documents/studies had been disclosed or exported for both treatment and research purposes.

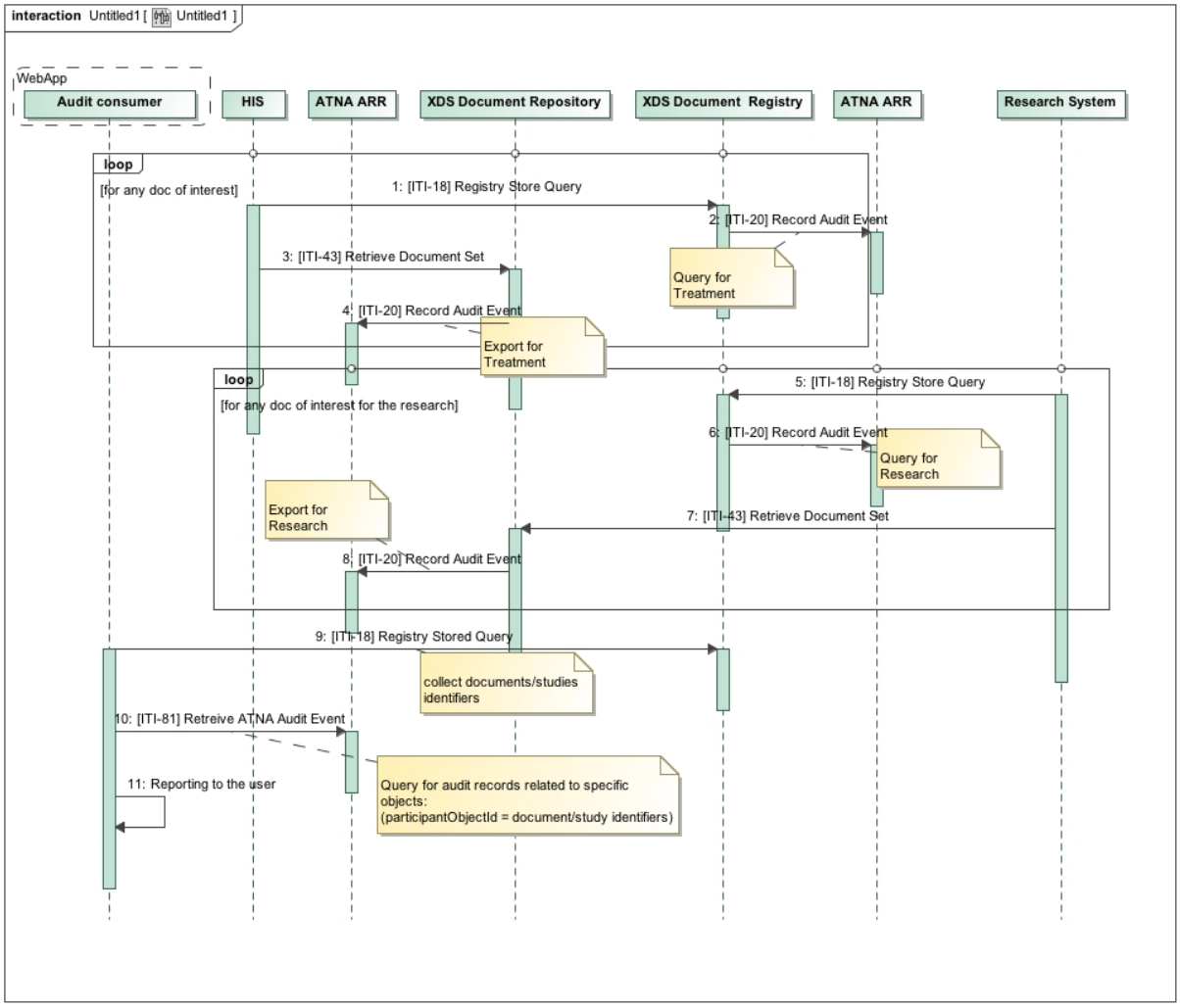


Figure 9.4.2.5-1: Patient access to his audit records Process Flow

9.4.3 Technical Approach to Query use cases

A wide variety of specific reports and analyses may be needed. It is assumed there will be a reporting and analysis system with extensive database and programmability features. The interoperability need is to search suitable subsets of the records held by the ARR, and to combine and analyze those records to determine a final result.

Rather than support a highly complex query capability, ATNA defines simple search transactions that can be combined to fit real-world needs.

The ATNA Retrieve Audit Event transaction support searches based on:

- **Patient identifier**: this search parameter allows discovering all of the events that occurred related to a specific patient;

- **User identifier**: this search parameter allows discovering all of the actions performed by a specific user
- **Object identifier**: this search parameter allows discovering each event that occurred related to a specific object (like study, reports, image, etc.).
- **Time frame**: this search parameter allows discovering all of the events that occurred during a specific time frame.
- **Event type**: this search parameter allows discovering all of the occurrences of a specific event (like Data Export, Data Import, Query, Authentication, etc.).
- **Application identifier**: this search parameter allows discovering all of the events recorded by a specific application or system.
- **Event Outcome Indicator**: this search parameter allows discovering all of the events characterized by a specific outcome (Success, Failure, etc.) of the related event.

For additional analysis beyond that which is fulfilled by the above parameters, the Audit Consumer can perform a search for records from the time frame expected, and then perform a more detailed analysis on those records, locally.

Further details about message semantics are defined in Section ITI TF-2c: 3.81.

Editor: Make the following changes in Section 9.5

9.5 ATNA Security Considerations

Some basic concepts are described in ~~**See**~~ Section 9.4.

In addition to those concepts, ATNA defines transactions for the Audit Record Repository that enables sharing of sensitive information related to patients and systems.

Audit Record Repositories have been considered in many implementations and projects as a "black-box" able to store relevant information for security and monitoring purposes. Those systems have not historically been designed to provide external access to stored records. Security Officers and System Architects should consider this, and analyze the risks of disclosing data stored in the Audit Record Repository. The Retrieve ATNA Audit Event [ITI-81] and Retrieve Syslog Event [ITI-82] transactions define how to search two categories of audit records:

- **messages related to IHE transactions or compliant with DICOM Audit Message Schema (DICOM PS3.15 Section A.5) http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html**
- **other syslog messages compliant with RFC 5424.**

Security analysis should include consideration of the content of the other syslog messages. The content of those messages is not profiled by IHE or DICOM, and may include PHI or other sensitive information.

Accordingly, access control mechanisms on the ATNA actors and queries are strongly recommended. The Internet User Authentication (IUA) Profile should be considered for the authorization controls. The ATNA Audit Record Repository can be grouped with an IUA Resource Server to enforce policies and authorization decisions. The Audit Consumer can be grouped with an IUA Authorization Client to provide authorization information to the ATNA Audit Record Repository. Access controls should appropriately restrict access to audit records.

The Retrieve ATNA Audit Event and Retrieve Syslog Event transactions may involve the disclosure of sensitive information. The logging of these retrieval transactions as a query event is appropriate. However, the ATNA Profile does not mandate the grouping of the Audit Record Repository with a Secure Node because that grouping introduces requirements that are not applicable to this scenario. In particular, it is reasonable that an audit record generated by the Audit Record Repository is directly stored within the ARR database rather than being sent to another system using Syslog over TLS protocol. Also, mandating a grouping of the Audit Record Repository with a Secure Node could lead to audit record feedback loops. The Record Audit Event [IT-20] already includes some audit requirements for the ATNA Audit Record Repository, such as reporting accesses to the ARR.

Volume 2c – Transactions

Editor: Add new Section 3.81 Retrieve ATNA Audit Event and 3.82 Retrieve Syslog Event to Volume 2c

3.81 Retrieve ATNA Audit Event [ITI-81]

This transaction supports the retrieval of ATNA audit record from the Audit Record Repository in accordance with a set of search parameters that determine the retrieved event reports. This transaction enables an Audit Consumer to search audit events that an Audit Record Repository created via transaction [ITI-20] Record Audit Event.

This transaction is a profiling of a standard FHIR search of the AuditEvent resource.

3.81.1 Scope

The Retrieve ATNA Audit Event transaction is used to search ATNA events recorded in an ATNA Audit Record Repository. The result of this retrieval is a FHIR bundle of AuditEvent resources that match with a set of search parameters.

3.81.2 Actor Roles

Table 3.81.2-1: Actor Roles

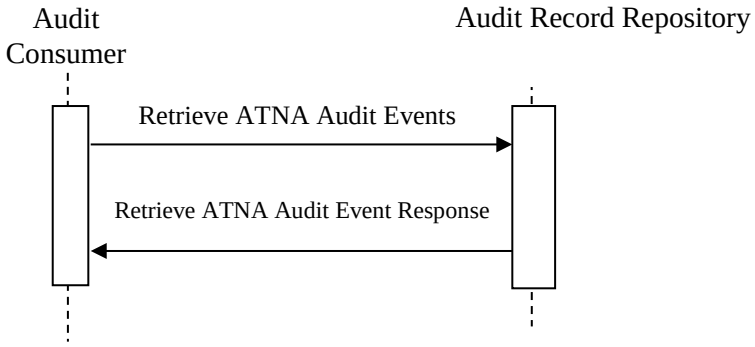
Actor:	Audit Record Repository
Role:	Provides storage for ATNA audit events, and responds to queries for a portion of the stored records.
Actor:	Audit Consumer
Role:	Queries for ATNA audit records.

3.81.3 Referenced Standards

RFC 2616	IETF Hypertext Transfer Protocol –HTTP/1.1
RFC 4627	The application/json Media Type for JavaScript Object Notation (JSON)
RFC 6585	IETF Additional HTTP Status Codes
RFC 5424	The Syslog Protocol
RFC 3339	Date and Time on the Internet: Timestamps

HL7 FHIR Standard DSTU2 (v1.0.2) http://hl7.org/fhir/DSTU2/index.html

3.81.4 Interaction Diagram



3.81.4.1 Retrieve ATNA Audit Events Message

This is an HTTP GET parameterized search from an Audit Consumer to an Audit Record Repository. The Audit Record Repository has stored ATNA audit records received via [ITI-20] Record Audit Event transactions. Those messages, which are stored within a data-store, can be retrieved in accordance with specific search parameters.

3.81.4.1.1 Trigger Events

The Audit Consumer sends a Retrieve ATNA Audit Events message when it needs ATNA audit records to process or analyze.

3.81.4.1.2 Message Semantics

The Retrieve ATNA Audit Event message shall be an HTTP GET request sent to the Audit Record Repository. This message is a FHIR search (see FHIR Section 2.1.1) on AuditEvent Resources (see FHIR Section 6.5). This "search" target is formatted as:

<scheme>://<authority>/<path>/AuditEvent?date=ge[start-time]&date=le[stop-time]&<query>

where:

- **<scheme>** shall be either http or https. The use of http or https is a policy decision, but https is usually appropriate due to confidentiality of ATNA audit record content;
- **<authority>** shall be represented as a host (either IP address or DNS name) followed optionally by a colon and port number.

- The Audit Record Repository may use **<path>** to segregate the HTTP search service for AuditEvent implementation from other REST-based services.
- The **date** search parameter is required. See Section 3.81.4.1.2.1.
- **"&"** is a conditional parameter that shall be present if the **<query>** parameter is present.
- **<query>**, if present, represents a series of encoded name-value pairs representing filters for the search. See Section 3.81.4.1.2.2.

3.81.4.1.2.1 Date Search Parameters

The two **date** parameters are recommended in every search by the Audit Consumer and shall be supported by the Audit Record Repository in order to avoid overload of matching AuditEvent resources in the Response message. One or two date parameters shall be present. These parameters allow the Audit Consumer to specify the time frame of creation of audit records of interest and enable the Audit Consumer to constrain the number of audit records returned. The lower and upper bound times shall be in RFC 3339 format.

Note: RFC 3339 format is the format mandated by Syslog for time stamps and is a sub-set of the XML date-time data format used by FHIR.

For example, to search AuditEvent resources created during the whole day of January 5, 2013:

```
http://example.com/ARRservice/AuditEvent?date=ge2013-01-05&date=le2013-01-05
```

The Audit Record Repository shall apply matching criteria to AuditEvent resources characterized by AuditEvent.event.dateTime field valued within the time frame specified in the Request message.

The Audit Record Repository shall apply other date matching criteria following rules defined by FHIR Section 2.1.1 (http://hl7.org/fhir/DSTU2/search.html).

3.81.4.1.2.2 Additional ATNA Search Parameters

The search parameters in this section may be supported by the Audit Consumer and shall be supported by the Audit Record Repository. These parameters can be used by the Audit Consumer to refine search requests. Refer to Section 3.81.4.2.2 for the mapping between FHIR AuditEvent resource and DICOM standard.

The Audit Consumer shall encode all search parameters per RFC 3986 "percent" encoding rules. Although FHIR allows unconstrained use of AND OR operators to make queries of unlimited complexity, this transaction constrains the queries allowed. Multiple search parameters shall only be combined using AND "&" operators. The OR "," operator shall be used only within a single search parameter that has multiple values.

Additional search parameters are listed below:

- **address** is a parameter of `string` type. This parameter specifies the identifier of the network access point (NetworkAccessPointID) of the user device that creates the audit record (This could be a device id, IP address, or some other identifier associated with a device).

  The value of this parameter shall contain the substring to match.

  For example:
  `http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&address=192.168.0.1`

  The Audit Record Repository shall match this parameter with the AuditEvent.participant.network.address.

- **patient.identifier** is a parameter of `token` type. This parameter specifies the identifier of the patient involved in the event as a participant. The value of this parameter can contain the namespace URI (that represents the assigning authority for the identifier) and the identifier.

  For example:
  http://`example.com`/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&patient.identifier=urn:oid:1.2.3.4|5678

  The Audit Record Repository shall match this parameter only with the AuditEvent.participant.identifier field that represent the patient. The Audit Record Repository shall not match this parameter with other fields in the AuditEvent Resource.. (The patient identifier can be used in other audit event fields; the objective of this constraint is to force the repository to respond only with audit records for which the identifier specified in the query plays the role of the patient identifier, and not with all the audit records that involve this identifier in other roles).

- **identity** is a parameter of `token` type. This parameter specifies unique identifier for the object. The parameter value should be identified in accordance to the object type;

  For example:
  - `?identity=urn:oid:1.2.3.4.5|123-203-FJ`
  - `?identity=|123-203-FJ.`

  The Audit Record Repository shall match this parameter with the AuditEvent.object.identifier field that is of type identifier (ParticipantObjectID in DICOM schema).

- **object-type** is a parameter of `token` type. This parameter specifies the type of the object (e.g., Person, System Object, etc.). The parameter value shall contain the namespace URI `http://hl7.org/fhir/DSTU2/valueset-object-type.html` defined by FHIR and a coded value. See http://hl7.org/fhir/DSTU2/valueset-object-type.html for available codes.

The Audit Record Repository shall match this parameter with the AuditEvent.object.type field that is of code type.

- **role** is a parameter of `token` type. This parameter specifies the role played by the object (e.g., Report, Location, Query, etc.). The parameter value shall contain the namespace URI `http://hl7.org/fhir/DSTU2/object-role` defined by FHIR and a coded value. See http://hl7.org/fhir/DSTU2/object-role for available codes.

  For example, to search all the audit records related to the document object (Report="3") with the unique id 12345^1.2.3.4.5 a fully specified request would be:

  ```
  http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&role=http://hl7.org/fhir/DSTU2/object-role|3&identity=urn:oid:1.2.3.4.5|12345
  ```

  The Audit Record Repository shall match this parameter with the AuditEvent.object.role field

- **source** is a parameter of `token` type. This parameter identifies the source of the audit event (DICOM AuditSourceID).

  For example, to search AuditEvent resources produced by the audit source application characterized by unique ID: 1234:

  ```
  http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&source=1234
  ```

  The Audit Record Repository shall match this parameter with the AuditEvent.source.identifier field.

- **type** is a parameter of `token` type. This parameter represents the identifier of the specific type of event audited. The parameter value shall contain the namespace URI `http://nema.org/dicom/dicm` and a coded value. Codes available are defined by DICOM and IHE (see ITI TF-1: Table 3.20.6-1: Audit Record trigger events)

  For example, to search AuditEvent resources related to PHI Export Events:

  ```
  http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&type=http://nema.org/dicom/dicm|110106
  ```

  The Audit Record Repository shall match this parameter with the AuditEvent.event.type field (DICOM EventID).

- **user** is a parameter of `token` type. This parameter identifies the user that participated in the event that originates the audit record.

  For example, to search AuditEvent resources related to the user "admin":

  ```
  http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&user=admin
  ```


The Audit Record Repository shall match this parameter with the AuditEvent.participant.userId field.

- **subtype** is parameter of `token` type. This parameter identifies the specific IHE transaction that originates the audit record. The parameter value shall contain the namespace URI `urn:ihe:event-type-code`. Each IHE transaction specifies an associated audit record that defines a specific code identifying the transaction itself, and assigns this code to the EventTypeCode element within the [ITI-20] audit record.

For example, to search AuditEvents resources related to Retrieve Document Set [ITI-43] transactions:

```
http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&subtype=urn:ihe:event-type-code|ITI-43
```

The Audit Record Repository shall match this parameter with the AuditEvent.event.subtype field (DICOM EventTypeCode).

- **outcome** is a parameter of `token` type. This parameter represents whether the event succeeded or failed. The parameter value shall contain the namespace URI `http://hl7.org/fhir/DSTU2/audit-event-outcome` and a code taken from the related value set. Codes available can be found at http://hl7.org/fhir/DSTU2/audit-event-outcome.

To search AuditEvents resources related to failed events:

```
http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&outcome=http://hl7.org/fhir/DSTU2/audit-event-outcome|4,8,12
```

The Audit Record Repository shall match this parameter with the AuditEvent.event.outcome field (DICOM EventOutcomeIndicator).

The FHIR standard provides additional search parameters. This transaction does not define specific behavior on those parameters (such as _sort, _include, etc.). See Section “2.1.1 Search” in FHIR standard for details about available parameters.

3.81.4.1.2.3 Populating Expected Response Format

The FHIR standard provides encodings for responses as either XML or JSON. The Audit Record Repository shall support both message encodings. The Audit Consumer shall support one and may optionally support both encodings. The Audit Consumer may indicate the desired response format using the HTTP “Accept” header or may provide a `_format` parameter carrying at least one of the values in Table 3.81.4.1.2.3-1. Multiple values in the accept header or `_format` parameter indicate the Audit Consumer is capable of processing responses in either response

encoding. If the `_format` parameter is used, it has to convey one of the values provided by the HTTP "Accept" header. For Desired Response Encoding see ITI TF-2x: Z.6.

3.81.4.1.3 Expected Actions

The Audit Record Repository (ARR) maintains a database of security events. The Audit Record Repository shall return all the security events stored in that database that match the query parameters, and which the requester is authorized to view (see ITI TF-1: 9.9 for further details). The Audit Record Repository retains data in accordance to local policies and some data may be deleted.

When performing matching based on the search parameters, the Audit Record Repository shall:

- Select all audit records that have a time interval specified in the request URL.
- If search parameters other than those defined in Section 3.81.4.1.2.2 (e.g., `_sort`, `_include` FHIR search result parameters) are specified in the request URL, then
  1. If the Audit Record Repository does not support the parameter, it shall be ignored;
  2. If the Audit Record Repository supports the parameter, the matching or other behavior shall comply with the matching rules for its datatype in FHIR.

The Audit Record Repository shall return matching resources using the Retrieve ATNA Audit Event Response Message. See Section 3.81.4.2.

3.81.4.2 Retrieve ATNA Audit Event Response Message

The Audit Record Repository sends the Retrieve ATNA Audit Event Response message in response to a query from an Audit Consumer

3.81.4.2.1 Trigger Events

The Audit Record Repository creates this message when it receives and processes a Retrieve ATNA Audit Event message.

3.81.4.2.2 Message Semantics

When the search request is successfully processed, the Audit Record Repository shall return the AuditEvent resources that match the search parameters inside a FHIR Bundle resource. See ITI TF-2x: Z.1 in for further details. Additional resources, like `Patient`, may be contained in the response Bundle.

The "Content-Length" entity-header field shall be returned, unless this is prohibited by the rules in RFC 2616 Section 4.4, or subsequent versions of the HTTP specification.

Note: RFC 2616 specifies that this field *should* be returned. This transaction strengthens that requirement.

The "Content-Type" of the response will depend upon the requested response format indicated by Audit Consumer via the `_format` parameter.

Table 3.81.4.2.2-1: Response Type related to Requested format

_format parameter value	Bundle Format	Content-Type
application/json+fhir	FHIR JSON Bundle	application/json+fhir; charset=UTF-8
application/xml+fhir	FHIR XML Bundle	application/xml+fhir; charset=UTF-8

If the "`date`" search parameter is missing (see Section 3.81.4.1.2.1), the Audit Record Repository may return HTTP response code 400 - Bad Request.

If the specified search parameters do not result in any matching audit record, the Audit Record Repository shall return HTTP response of success 200, with an empty FHIR bundle.

If the requested data size is considered excessive by the Audit Record Repository, it may respond with HTTP 206 Partial Content. If the response is 206 Partial Content, then the response body may contain a subset of the messages that match the search request.

Other HTTP response codes may be returned by the Audit Record Repository, indicating conditions outside of the scope of this transaction, for example, 401 – Authentication Failed might be returned if Audit Record Repository is grouped with the Kerberized Server in the EUA Profile. See ITI TF-2x: Z.7 for further details.

The Audit Record Repository should complement the returned error code with a human readable description of the error condition.

Audit Record Repository may return HTTP redirect responses (responses with values of 301, 302, 303, or 307) in response to a request. Audit Consumers must follow redirects, but if a loop is detected, it may report an error.

The mapping rules between AuditEvent FHIR resources and DICOM audit message format is defined and maintained in FHIR Table 6.5.7.2, http://hl7.org/fhir/DSTU2/auditevent-mappings.html. The AuditEvent resource shall encode all the data within the DICOM format of the syslog Audit record.

3.81.4.2.2.1 FHIR Bundle of Audit Events Messages

When the search is successful, the body of the Response message shall contain a FHIR Bundle of AuditEvent FHIR resources.

Example XML format:


```
<Bundle>
    <type>searchset</type>
    <total>3</total>
  <link>
       <relation value=”self”/>
       <url value=” http://example.com/ARRservice/AuditEvent?date=&gt;2013-01-01&date=&lt;2013-
01-02”/>
  </link>
    <entry>
        <fullUrl value="http://example.com/ARRservice/AuditEvent/23#"/>
        <resource>
            <AuditEvent>
                .....
            </AuditEvent>
        <resource>
    </entry>
    <entry>
        <fullUrl value="http://example.com/ARRservice/AuditEvent/564#"/>
        <resource>
            <AuditEvent>
                .....
            </AuditEvent>
        <resource>
    </entry>
    <entry>
        <fullUrl value="http://example.com/ARRservice/AuditEvent/3446#"/>
        <resource>
            <AuditEvent>
                .....
            </AuditEvent>
        <resource>
    </entry>
</Bundle>
```

3.81.4.2.3 Expected Actions

The Audit Consumer may further analyze the data received within the FHIR Bundle of AuditEvent resources.

The Audit Record Repository shall create and store locally an audit event structured in accordance to requirements defined in DICOM PS3.15 Section A.5.3.2 “Audit Log Used”.

3.81.5 Security Considerations

See the general Security Considerations in ITI TF-1:9.5.

3.81.5.1 Security Audit Considerations

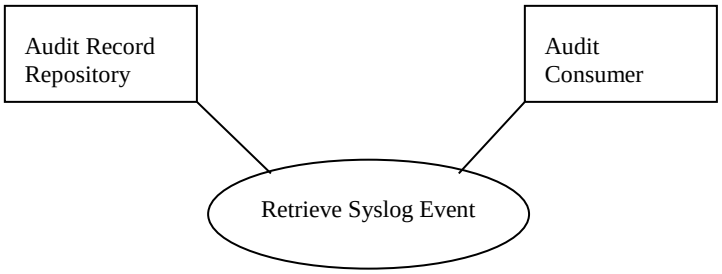
This transaction does not require the Audit Record Repository to be able to send audit records using [ITI-20] Record Audit Event transaction. However, it shall create and store locally an audit event structured in accordance to requirements defined in DICOM PS3.15 Section A.5.3.2 “Audit Log Used”. DICOM PS3.15 defines a specific structure for an audit record that may be created when an Audit Log is used. See http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.3.2.html DICOM PS3.15 Section A.5.3.2 “Audit Log Used” for further details.

3.82 Retrieve Syslog Event

This transaction supports the retrieval of syslog messages from the Audit Record Repository subject to parameters that limit the retrieval.

3.82.1 Scope

The Retrieve Syslog Event transaction is used to search events recorded.



3.82.2 Use-case Roles

Actor: Audit Record Repository

Role: Provides storage for syslog messages, and responds to queries for a portion of the stored messages.

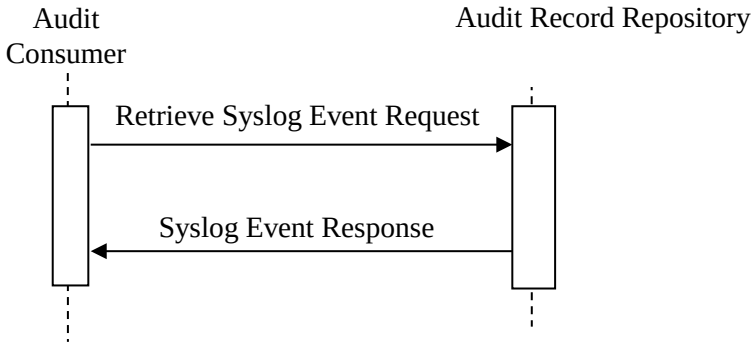
Actor: Audit Consumer

Role: Queries for audit records.

3.82.3 Referenced Standard

RFC 2616	IETF Hypertext Transfer Protocol –HTTP/1.1
RFC 4627	The application/json Media Type for JavaScript Object Notation (JSON)
RFC 6585	IETF Additional HTTP Status Codes
RFC 5424	The Syslog Protocol
RFC 3339	Date and Time on the Internet: Timestamps

3.82.4 Interaction Diagram



3.82.4.1 Retrieve Syslog Event Request Message

This message shall be an HTTP GET parameterized search from an Audit Consumer to an Audit Record Repository. The Audit Record Repository maintains a database of received syslog messages. This database may be a subset of all messages received and it may include messages that do not adhere to the IHE Audit Trail format defined in the [ITI-20] transaction. See ITI TF-2a: 3.20.7 Audit Message Format.. The Audit Record Repository may have selection criteria for what kinds of messages are kept for later search, how long different kinds of messages are kept, etc.

3.82.4.1.1 Trigger Events

This message is sent when the Audit Consumer needs syslog messages to process.

3.82.4.1.2 Message Semantics

The Retrieve Syslog Event Request message is an HTTP GET request sent by the Audit Consumer to the Retrieve Syslog Event URL on the Audit Record Repository. The "search" target is formatted as:

<scheme>://<authority>/<path>/syslogsearch?date=le[start-time]&date=ge[stop-time]&<query>

Where:

- **<scheme>** shall be either http or https. The use of http or https is a policy decision, but https is usually appropriate due to confidentiality of syslog message content;
- **<authority>** shall be represented as a host (either IP address or DNS name) followed optionally by a colon and port number.
- The Audit Record Repository may use **<path>** to segregate the search.

- "**syslogsearch**" is a required part of the URL that allows the Audit Consumer to ask for syslog messages stored in the Audit Record Repository.
- A **date** search parameters are required. It is suggested to use two date parameters in order to search for a limited time window. See Section 3.82.4.1.2.1.
- **"&"** is a conditional parameter that shall be present if the <query> parameter is present.
- **<query>,** if present, represents additional search parameters. See Section 3.82.4.1.2.2 Additional Search Parameters.

The Audit Consumer may indicate the preferred format of the response in the HTTP "Accept" header.

3.82.4.1.2.1 Date Search Parameters

One or two **date** parameter shall be present in every search by the Audit Consumer and shall be supported by the Audit Record Repository. Using two parameters allows the Audit Consumer to specify the time frame of creation of syslog messages of interest and enable the Audit Consumer to constrain the number of syslog messages returned. The lower and upper bound for time shall be in RFC 3339 format.

Note: RFC 3339 format is the format mandated by Syslog for time stamps and is a sub-set of the XML date-time data format.

To search syslog messages created during the whole day of January 5, 2013, the search URL is:

```
http://example.com/ARRservice/syslogsearch?date=ge2013-01-05&date=le2013-01-05
```

This parameter matches with the time of the syslog message creation.

3.82.4.1.2.2 Additional Search Parameters

The search parameters in this section may be supported by the Audit Consumer and shall be supported by the Audit Record Repository. These parameters can be used by the Audit Consumer to refine search requests.

The Audit Consumer may include additional search parameters. These search parameters shall be encoded in accordance with RFC 3986 for encoding GET queries.

The search string is encoded as a list of search parameter/value pairs, using the parameter names in column 2 of Table 3.82.4.1.2.2-1 to indicate the syslog message element being matched. There is a search parameter assigned for each syslog metadata element. In all cases:

- The search values shall be encoded as strings.
- The Syslog message is considered to match if the value string is a sub-string found in the specified message element.

Table 3.82.4.1.2.2-1: Retrieve Syslog Event search parameters mapping with syslog metadata

Syslog RFC 5424 element	Retrieve Syslog Event Search Parameter
PRI	pri
VERSION	version
HOSTNAME	hostname
APP-NAME	app-name
PROCID	procid
MSG-ID	msg-id
MSG	msg

HTTP allows for multiple instances of a parameter to be requested with different values. Multiple values of the same parameter name shall be treated as an OR relationship for string matches. The Audit Consumer may combine different search parameters. The matching of different search parameters is combined with an AND relationship. Some examples of how this works are:

- To search for "hostname=Frodo" and "hostname=Bilbo" will return the combination of all event reports from either host Frodo or Bilbo during the time interval:

```
http://example.com/ARRservice/syslogsearch?date=ge2013-01-01&date=le2013-01-02&hostname=Frodo&hostname=Bilbo
```

- To search for "hostname=Frodo" and "proc-id=system" it means all events from the host "Frodo" with proc-id of "system" during the time interval:

```
http://example.com/ARRservice/AuditEvent?date=ge2013-01-01&date=le2013-01-02&hostname=Frodo&proc-id=system
```

- To search for "hostname=Frodo", "hostname=Bilbo", and "proc-id=system" will return the combination of all event reports from either host Frodo or Bilbo that have the proc-id of "system" during the time interval:

```
http://example.com/ARRservice/syslogsearch?date=ge2013-01-01&date=le2013-01-02&hostname=Frodo&hostname=Bilbo
```

This form of search is not a substitute for additional processing by the Audit Consumer. The Audit Record Repository can return a large quantity of syslog messages. The Audit Consumer may need to perform further processing to select the information needed for a report.

The Audit Record Repository shall document in its IHE Integration Statement any additional parameters supported.

3.82.4.1.3 Expected Actions

The Audit Record Repository (ARR) maintains a database of syslog messages. The Audit Record Repository shall return all the syslog messages stored in that database that match the query

parameters, and which the requester is authorized to view (see ITI TF-1: 9.9 for further details). The Audit Record Repository retains data in accordance to local policies and some data may be deleted.

The Audit Record Repository shall respond with a Syslog Event Response message described in Section 3.82.4.2.

When performing matching based on the search parameters, the Audit Record Repository shall:

- Select all messages that have a time interval specified in the request URL.
- If search parameters other than those defined in Section 3.82.4.1.2.2, are specified in the request URL, then if the parameter is not supported, it shall be ignored; otherwise, if this parameter is supported, the Audit Record Repository shall apply matching criteria in accordance to that.
- select a response format following the rules of RFC 7231 section 5.3.2. The Audit Record Repository shall support JSON format (i.e., application/json). In the absence of an Accept preference, JSON shall be used.

3.82.4.2 Syslog Event Response Message

The Audit Record Repository sends the Syslog Event Response message in response to a query from an Audit Consumer

3.82.4.2.1 Trigger Events

The Audit Record Repository creates this message when it receives and processes a Retrieve Syslog Event Request message.

3.82.4.2.2 Message Semantics

The Content-Length entity-header field shall be returned, unless this is prohibited by the rules in RFC 2616 Section 4.4, or subsequent versions of the HTTP specification.

Note: RFC 2616 specifies that this field *should* be returned. This transaction strengthens that requirement.

In case of success, the Audit Record Repository shall return the syslog messages that match the search parameters, encoded as an array of messages encoded in one of the formats specified in the Accept header of the request message. The Syslog Event Response message shall carry a HTTP response status code of 200, and its body shall contain an Array of Syslog messages in the selected format.

Each syslog message shall be encoded as described in Table 3.38.4.2.2-1:

Table 3.38.4.2.2-1: Syslog Message Encoding

Syslog Metadata	JSON element	dataType
PRI	Pri	<string>
VERSION	Version	<string>
TIMESTAMP	Timestamp	see RFC 5424 (sec. 6.2.3)

Syslog Metadata	JSON element	dataType
HOSTNAME	Hostname	<string>
APP-NAME	App-name	<string>
PROCID	Procid	<string>
MSG-ID	Msg-id	<string>
MSG	Msg	<string>
STRUCTURED_DATA	Structured_data	<string>

If the date parameter is missing, the Audit Record Repository may return HTTP response code 400 - Bad Request.

If the specified parameters do not result in any matching syslog messages, the Audit Record Repository shall report a Response of Success (HTTP 200) with an empty JSON array.

If the requested data size is excessive, the Audit Record Repository may respond with HTTP 206 Partial Content. If the response is 206 Partial Content, then the response body may contain a subset of the syslog messages that match the search. This transaction does not define query result pagination mechanisms, so the Audit Consumer cannot query for remaining content in case of http 206 error received.

If the “Accept” header provided in the Request is not supported by the Audit Record Repository, it may send a 415 “Unsupported Media Type” error.

Note: Other HTTP response codes may be returned by the Audit Record Repository, indicating conditions outside of the scope of this transaction, for example, 401 – Authentication Failed might be returned if Audit Record Repository also supports the IUA Profile and is given an expired authorization token or is grouped with the EUA Profile Kerberized Server.

The Audit Record Repository should complement the returned error code with a human readable description of the error condition.

Audit Record Repository may return HTTP redirect responses (responses with values of 301, 302, 303, or 307) in response to a request. Audit Consumers must follow redirects, but if a loop is detected, it may report an error.

3.82.4.2.2.1 JSON encoded array of Syslog Messages

Example:

```
{
      {
      Pri : “string”,
      Version: “string”,
      Timestamp: “2015-03-17T00:05”
      Hostname: “string”
      App-name: “string”
      Procid: “string”
      Msg-id : “string”
```



```
        Structured-data : “string”
        Msg : “string1”
        Structured_data: “string”
        }
        {
        Pri : “string”,
        Version: “string”,
        Timestamp: “2015-03-17T00:05”
        Hostname: “string”
        App-name: “string”
        Procid: “string”
        Msg-id : “string”
        Msg : “string2”
        }
        {
        Pri : “string”,
        version: “string”,
        Timestamp: “2015-03-17T00:05”
        Hostname: “string”
        App-name: “string”
        Procid: “string”
        Msg-id : “string”
        Msg : “string3”
        }
}
```

The Audit Record Repository shall construct a JSON array of syslog messages by parsing the message elements in each matching Syslog as defined in RFC 5424 as strings identified by the element name in RFC 5424. If an element is absent from the syslog message, the Audit Record Repository shall not include this element in the JSON encoding.

3.82.4.2.3 Expected Actions

The Audit Consumer shall process the response according to the capabilities of its application. The processing is not constrained by IHE.

The Audit Record Repository shall create and store locally an audit event structured in accordance to requirements defined in DICOM PS3.15 Section A.5.3.2 “Audit Log Used”.

3.82.5 Security Considerations

See the general Security Considerations in ITI TF-1:9.8.

3.82.5.1 Security Audit Considerations

This transaction does not require the Audit Record Repository to be able to send audit records using [ITI-20] Record Audit Event transaction. However, it shall create and store locally an audit event structured in accordance to requirements defined in DICOM PS3.15 Section A.5.3.2 “Audit Log Used”. DICOM PS3.15 defines a specific structure for an audit record that may be created when an Audit Log is used. See

http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.3.2.html DICOM
1030 PS3.15 Section A.5.3.2 “Audit Log Used” for further details.

