Integrating the Healthcare Enterprise

IHE IT Infrastructure
Technical Framework Supplement

Add RESTful ATNA (Query and Feed)

HL7® FHIR® Release 4

Using Resources at FMM Level 3 and Normative

Rev. 3.4 – Trial Implementation

Date: August 4, 2023

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 V20.0. 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 4, 2023 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 IHE.net.

Information about the IHE IT Infrastructure domain can be found at IHE Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at Profiles and IHE Process.

The current version of the IHE IT Infrastructure Technical Framework can be found at https://profiles.ihe.net/ITI/index.html.

CONTENTS

Introduction to this Supplement

Whenever possible, IHE profiles are based on established and stable underlying standards. However, if an IHE domain determines that an emerging standard has high likelihood of industry adoption, and the standard offers significant benefits for the use cases it is attempting to address, the domain may develop IHE profiles based on such a standard. During Trial Implementation, the IHE domain will update and republish the IHE profile as the underlying standard evolves.

Product implementations and site deployments may need to be updated in order for them to remain interoperable and conformant with an updated IHE profile.

This Technical Framework Supplement incorporates content from Release 4 of the HL7® FHIR® standard. HL7 describes FHIR Change Management and Versioning at https://www.hl7.org/fhir/versions.html.

HL7 provides a rating of the maturity of FHIR content based on the FHIR Maturity Model (FMM): level 0 (draft) through N (Normative). See http://hl7.org/fhir/versions.html#maturity.

The FMM levels for FHIR content used in this supplement are:

FHIR Resource Name	FMM Level
Bundle	N
AuditEvent	3
OperationOutcome	N

This supplement extends the functionalities of the ATNA Profile by introducing RESTful operations that could be used to submit and retrieve audit records. This allows light weight applications to easily manage the creation and the access audit information. This supplement is based on FHIR protocol and uses FHIR AuditEvent Resources in order to exchange audit records content. This supplement also defines a query transaction that enables access to raw syslog messages.

Open Issues and Questions

1. Should there be retrieve methods to get “most recent N events”? This would be a non-deterministic and constantly varying response in most cases.
2. For ITI-82, the start-time and stop-time in <date> search parameters shall be in RFC3339 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)?

3. The DICOM element ParticipantObjectIdentification.ParticipantObjectDescription it is defined as a complex type but FHIR AuditEvent.entity.description it is a string element. How should we handle this mapping?
   Decision: The guideline is to not use this element since in R5 it will not be present anymore (see https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=20888) because `ParticipantObjectDescription` is simply a grouper element and thus cannot hold any value.

4. In https://www.hl7.org/fhir/R4/auditevent-mappings.html#dicom the EventDateTime it is mapped in AuditEvent.period but should be mapped in AuditEvent.recorded. How should we handle this?
   Decision: In future release of FHIR, R5, this issue will be resolved (see https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_id=677&tracker_item_id=20837). In the meantime, in Table 3.81.4.2.2.1-1 there is the mapping to be used.

5. AuditEvent resource does not address the PRI syslog data field. How should we handle this?
   Decision: In future release of FHIR, R5, this issue will be resolved (see https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=18088&start=11600)

Closed Issues

1. How can we address integration statement for new actors that supports [ITI-20]?

   Decision: A set of options have been added in order to declare the protocol used by Secure Node, Secure Application, Audit Record Forwarder.

2. How to deal with different protocols defined in [ITI-20]?

   Decision: The Record Audit Event [ITI-20] transaction it has been modified to support POST of single AuditEvent resources or a Bundle of them. To send a Bundle of AuditEvent it is required to use the "batch" interaction (see https://www.hl7.org/fhir/R4/http.html#transaction).

3. In https://www.hl7.org/fhir/R4/auditevent-mappings.html#dicom the ActiveParticipant.RoleIdCode it is mapped either in AuditEvent.agent.type and AuditEvent.agent.role. How should we handle the mapping?

   Decision: The guideline is to map the RoleIdCode in the agent.role element, if the code is known by the ARR as a type should be mapped in the agent.type element instead. When FHIR Release 5 will be aligned with this decision see CP #20536 https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=2

0536&start=0 update Section 3.81.4.2.2.1 Mapping between DICOM and FHIR removing the statement.

4. The mapping defined in https://www.hl7.org/fhir/R4/auditevent-mappings.html#dicom it is not sufficient in order to allow auditing through the AuditEvent Resource.

   Decision: in Section 3.81.4.2.2.1 the mapping defined by FHIR has been further constrained in order to allow interoperability between the two data models.

5. 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"?

   Decision: the server is not required to reject a request. It could do so, in accordance to the specification.

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

   Decision: the functionality is covered by the Capability Statement.

7. Only a JSON return format is specified for Retrieve Syslog Messages [ITI-82] (non FHIR transaction). 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?

   Decision: During public comment and during TI period no vendors raise issues about the format of this transaction.

8. Should a server information query be specified? There are various RFCs from the IETF that specify aspects of server information.

   Decision: now FHIR allows the definition of conformance resources. We defined them and they can be found in the IHE/fhir github repository.

9. 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 sections 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.

10. 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 the generic SYSLOG format and the FHIR AuditEvent 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.

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	Support

11. 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
FHIR	Covered in this supplement	None

12. 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
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 AuditEvent 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.

255 **Evaluation Criteria Results**

Criteria	DCM4CHE	Tiani Spirit EHR	Connect/Healtheway	FHIR (AuditEvent)
Stability		Early development	Has been deprecated	STU and Normative
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 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.

13. 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.

14. 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.

15. 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

16. 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 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.

17. 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.

18. 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)?
    Decision: This is a very important implementation decision, and IHE cannot define requirement for this.

19. 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).
    Decision: This issue was resolved with STU3 release.

20. 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?
    Decision: Starting from STU3 release it’s well understood how to use search parameters of type `reference` to navigate through resources.

21. CP-ITI-1152 asks for an enhancement of the patient.identifier search parameter to search also for audit where the patient is involved in the event as a participant.
    Decision: During the update to move this supplement to FHIR R4 the CP was included in order to have an alignment between the search parameters, defined by FHIR and the ones defined in this supplement, that can be used to search for patient involved in the event either as a user and either as a participant.

22. This Supplement provides two different tables in order to provide distinct mapping for the feed (see Table 3.20.4.2.2.1) and for the query (see 3.81.4.2.2.1) transactions.

Mapping for the query is intended to be normative. On the other side the mapping for the feed is provided for implementers that needs guidelines on how to map Audit Message info listed in TF into an AuditEvent Resource and should not be considered normative.

23. The new FHIR feed mechanism that can be used by Secure Node Secure Application ad Audit Record Forwarder enables subscription mechanisms. Should we profile this subscription mechanism?
Decision: During Public Comment no feedback were received about this issue, thus we decided to move approve the supplement for TI without addressing this issue.

IHE Technical Frameworks General Introduction

The IHE Technical Framework General Introduction is shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to this document where appropriate.

9 Copyright Licenses

IHE technical documents refer to, and make use of, a number of standards developed and published by several standards development organizations. Please refer to the IHE Technical Frameworks General Introduction, Chapter 9 - Copyright Licenses for copyright license information for frequently referenced base standards. Information pertaining to the use of IHE International copyrighted materials is also available there.

10 Trademark

IHE® and the IHE logo are trademarks of the Healthcare Information Management Systems Society in the United States and trademarks of IHE Europe in the European Community. Please refer to the IHE Technical Frameworks General Introduction, Chapter 10 - Trademark for information on their use.

IHE Technical Frameworks General Introduction Appendices

The IHE Technical Framework General Introduction Appendices are components shared by all of the IHE domain technical frameworks. Each technical framework volume contains links to these documents where appropriate.

*Update the following appendices to the General Introduction as indicated below. Note that these are **not** appendices to this domain's Technical Framework (TF-1, TF-2, TF-3 or TF-4) but rather, they are appendices to the IHE Technical Frameworks General Introduction located here.*

Appendix A – Actors

*Add the following **new or modified** actors to the IHE Technical Frameworks General Introduction Appendix A:*

Actor	Definition
Audit Consumer	Queries for audit record content.

Appendix B – Transactions

*Add the following **new or modified** transactions to the IHE Technical Frameworks General Introduction Appendix B:*

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.

Appendix D – Glossary

*Add the following **new or modified glossary** terms to the IHE Technical Frameworks General Introduction Appendix D:*

Glossary Term	Definition
Audit Record	A syslog message that complies with the DICOM PS3.15 schema.
Syslog message	Any message that complies with RFC5424, 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.
Syslog metadata	Attributes that classify the audit record: defining severity of the event, facility, and application that sent the message. These are defined in RFC5424.

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 defines capabilities to both send to and retrieve messages from an Audit Record Repository (ARR):

- **The Record Audit Event [ITI-20] transaction enables a Secure Node, Secure Application or an Audit Record Forwarder to send a single or a group of Audit Records to an Audit Record Repository. This transaction supports encodings: syslog protocol over TLS, syslog protocol over UDP, or an HTTP POST of FHIR AuditEvent Resources.**
- **The Retrieve ATNA Audit Event [ITI-81] transaction enables an Audit Consumer to retrieve ATNA audit records stored within an Audit Record Repository. This transaction is based on a FHIR RESTful search operation on AuditEvent Resources.**
- **The Retrieve Syslog Event [ITI-82] transaction 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 audit events sent to the Audit Record Repository using Syslog protocol may not conform to ATNA Audit Events, so the Retrieve Syslog Event [ITI-82] transaction enables retrieval of audit records based on syslog metadata values.

Editor: Update Figure 9.1-1 as follows. 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 Event, Retrieve Syslog Event.

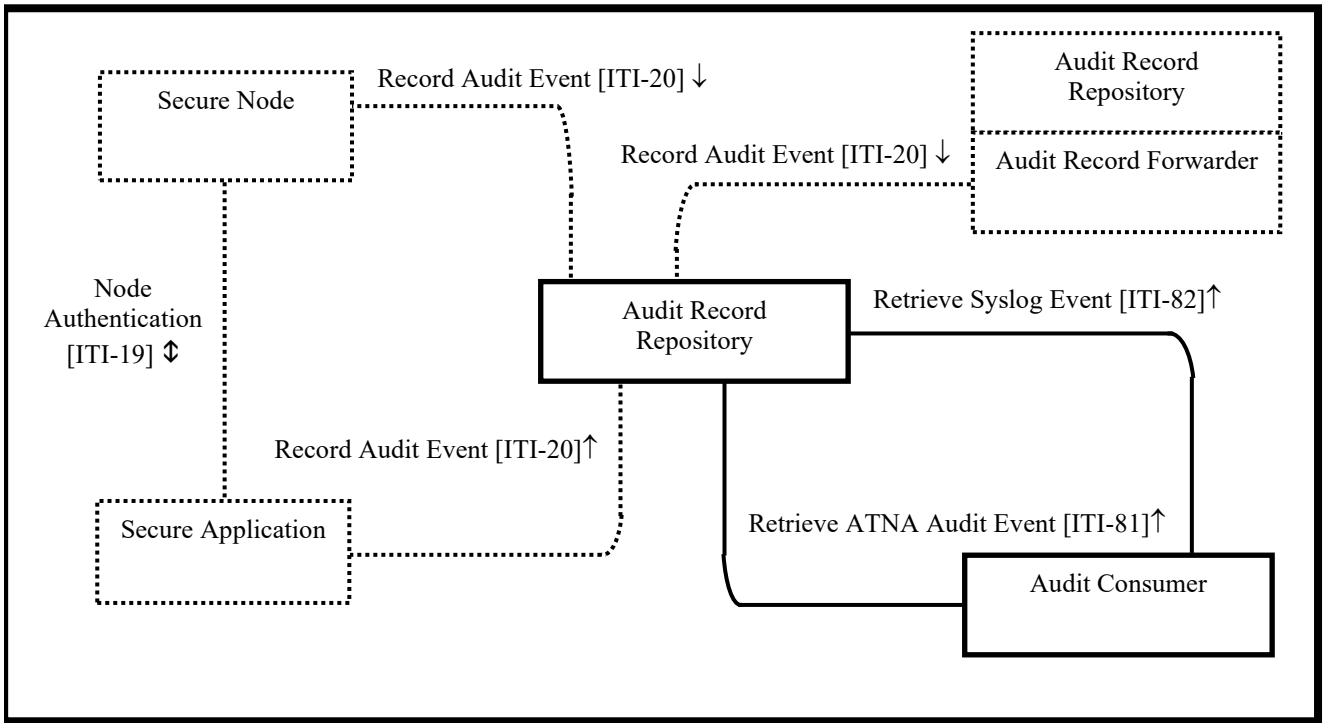


Figure 9.1-1: Audit Trail and Node Authentication Diagram

425

Editor: In Section 9.1, Update Table 9.1-1

Table 9.1-1: ATNA Profile - Actors and Transactions

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

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. At least one of the audit transport mechanisms specified in ITI TF-2: 3.20 (see Table 9.2-1).
2. Receipt of at least one of the 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.

The Audit Record Repository may ignore or process messages in non-IHE message formats. This may be for backwards compatibility or other reasons.

The Audit Record Repository be grouped with a Secure Node or Secure Application.

The Audit Record Repository may support search capabilities as defined in ITI TF-2: 3.81 and 3.82

Audit Record Repository may support search capabilities as defined in ITI TF-2: 3.81 and 3.82.

*Editor: Add **new** Section 9.1.1.5*

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

9.2 ATNA Actor 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.

Note: The "ATX" prefix in option names below marks alternatives for audit transport protocol, and the "STX" prefix marks alternatives for secure transport protocol, as defined in the Record Audit Event [ITI-20] transaction.

Table 9.2-1: ATNA – Actors and Options

Actor	Option Name	Vol. & Section
Audit Record Repository (Note 4)	**Retrieve Audit Message**	**ITI TF-1: 9.2.3**
	Retrieve Syslog Message	**ITI TF-1: 9.2.4**
	ATX: FHIR Feed	**ITI TF-1: 9.2.7.1**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Audit Consumer	**Retrieve Audit Message (Note 5)**	**ITI TF-1: 9.2.3**
	Retrieve Syslog Message (Note 5)	**ITI TF-1: 9.2.4**
Audit Record Forwarder (Note 4)	**ATX: FHIR Feed**	**ITI TF-1: 9.2.7.1**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Secure Node (Note 1) (Note 4)	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	…	…
	ATX: FHIR Feed	**ITI TF-1: 9.2.7.1**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3
Secure Application (Note 1) (Note 4)	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	…	…
	ATX: FHIR Feed	**ITI TF-1: 9.2.7.1**
	ATX: TLS Syslog	ITI TF-1: 9.2.7.2
	ATX: UDP Syslog	ITI TF-1: 9.2.7.3

…

Note 4: This actor shall support at least one of the "ATX" Options. If a product's IHE Integration Statement does not declare one of these options, the reader should assume that the product supports the TLS or UDP Syslog Option.

Note 5: 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 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 a RESTful search operation that searches syslog messages of any format or schema. The search request uses the syslog metadata only.

*Editor: Add **new** Section 9.2.7.1 as follows.*

9.2.7 Audit Transport (ATX) Options

At least one of these options shall be supported. Many can be declared, for which the product must then be configurable to enable each of the supported Audit Transport Options.

9.2.7.1 ATX: FHIR Feed Option

The ATX: FHIR Feed Option enables sending ATNA audit records using RESTful capabilities and FHIR resources.

An Audit Record Repository that supports this option shall implement the two RESTful interactions defined in the Record Audit Event [ITI-20] transaction. See ITI TF-2: 3.20.4.2 (Send Audit Resource) and 3.20.4.4 (Send Audit Bundle).

A Secure Node, Secure Application or Audit Record Forwarder that supports this option shall at least support one of the two RESTful interactions defined in the Record Audit Event [ITI-20] transaction. See ITI TF-2: 3.20.4.2 (Send Audit Resource) and 3.20.4.4 (Send Audit Bundle).

9.2.7.2 ATX: TLS Syslog Option

…

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 Record Repository	Consistent Time / Time Client	ITI TF-1: 7	N/A
	ATNA / Secure Node or Secure Application	ITI TF-1: 9	N/A
Audit Consumer	**ATNA / Secure Node or Secure Application**	**ITI TF-1: 9**	**N/A**
…			

Editor: Make the following changes in Section 9.4.2:

9.4.2 Use Cases

…

~~In the following paragraphs~~ Sections 9.4.2.1, 9.4.2.2, and 9.4.2.3 describe three typical process flows **~~are described~~** for 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.

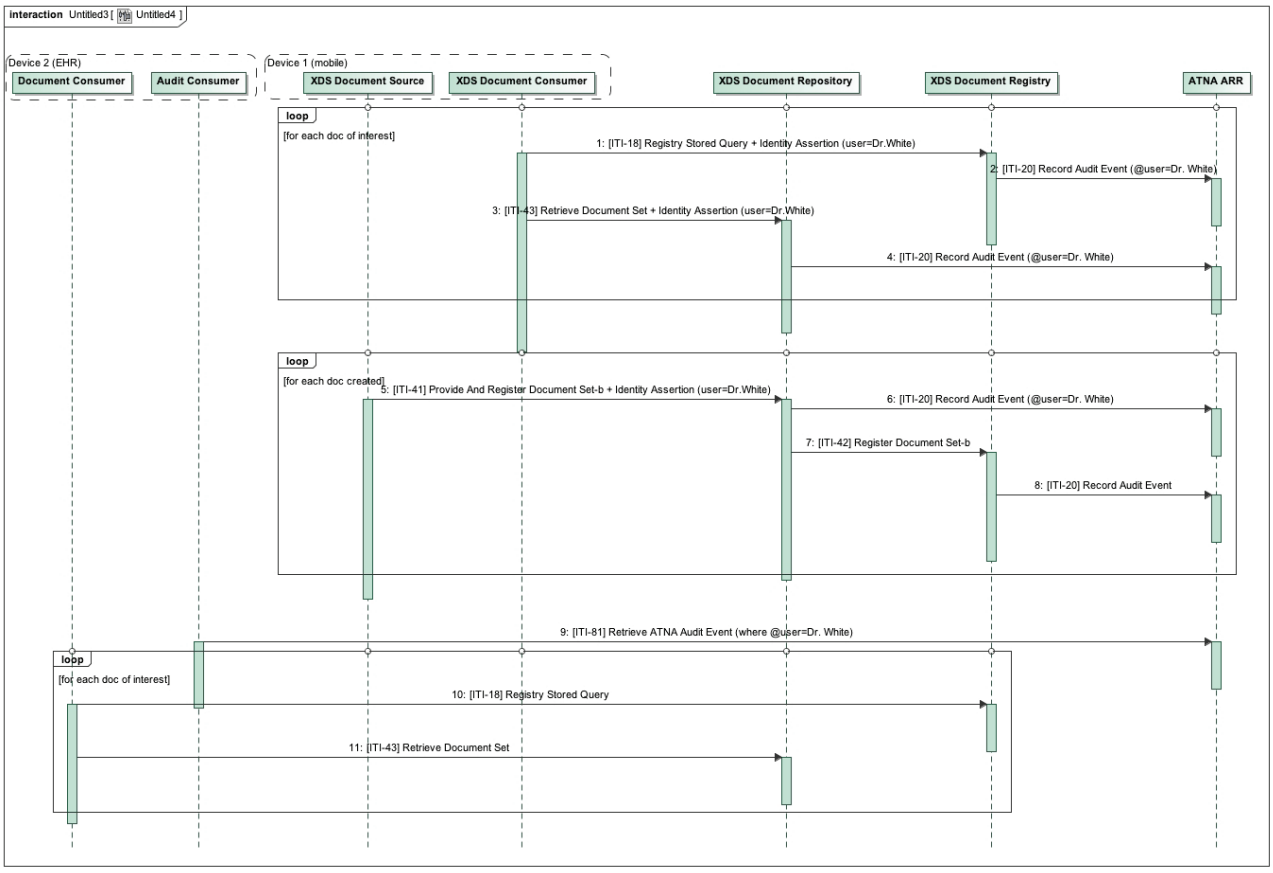


Figure 9.4.2.4.1-1: Clinician Personal History of Study views process flow

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.

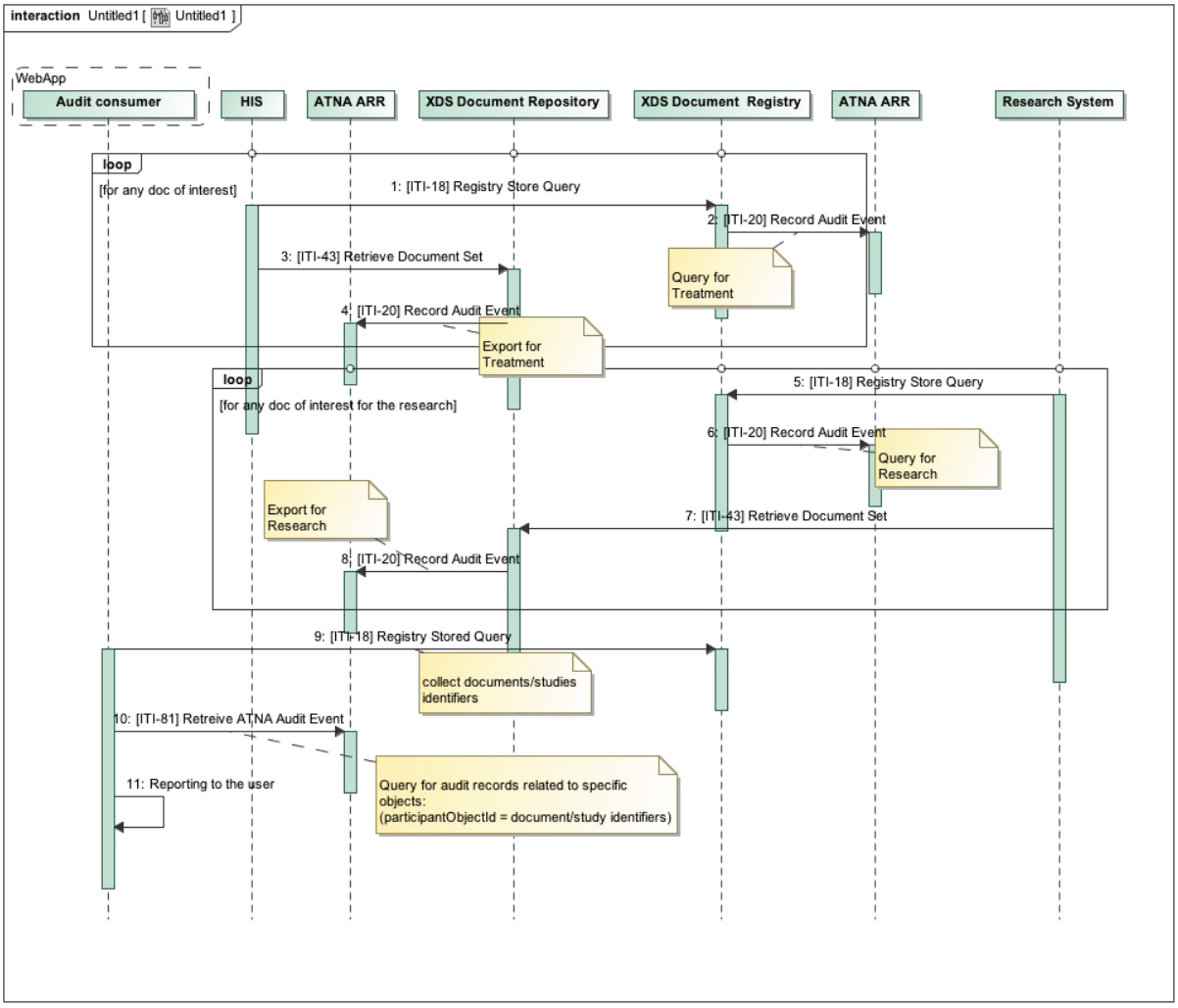


Figure 9.4.2.5-1: Patient access to his audit records Process Flow

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 Audit Record Repository, 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 Retrieve ATNA Audit Event [ITI-81] 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 (e.g., 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 (e.g., 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 (e.g., 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-2: 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.

ATNA defines transactions for the Audit Record Repository that enable sharing of sensitive information related to patients and systems.

In many implementations and projects, Audit Record Repository have been considered 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 RFC5424.**

Security analysis should consider 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 Authorization (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 [ITI-81] and Retrieve Syslog Event [ITI-82] transactions may involve the disclosure of sensitive information. Logging these retrieval transactions as a query event is appropriate (see ITI TF-2: 3.81.5.1 and 3.82.5.1). 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 in this case. In particular, it is reasonable that an audit record generated by the Audit Record Repository is directly stored within the Audit Record Repository 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 [ITI-20] transaction includes some audit requirements for the ATNA Audit Record Repository, such as reporting accesses to the Audit Record Repository; see ITI TF-2: 3.20.8 "Disclosures audit message".

Additional Security Considerations are described in ITI TF-2: Appendix Z.8.

Volume 2 – Transactions

Editor: update Section 3.20.3 as follows

3.20 Record Audit Event [ITI-20]

…

3.20.3 Referenced Standards

RFC5424	The Syslog Protocol.
RFC5425	Transmission of Syslog Messages over TLS
RFC5426	Transmission of Syslog Messages over UDP
RFC7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
DICOM	DICOM PS3.15 Annex A.5 http://medical.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.html
ASTM E2147-01	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
NIST SP 800-92	Guide to Computer Security Log Management.
W3C XML 1.0	Extensible Markup Language (XML) 1.0
HL7 FHIR	**Release 4** **http://hl7.org/fhir/R4/index.html**
RFC4627	**The application/json Media Type for JavaScript Object Notation (JSON)**

Editor: update Section 3.20.4 adding the new text and interaction diagram that shows the two new RESTful interactions

3.20.4 Messages

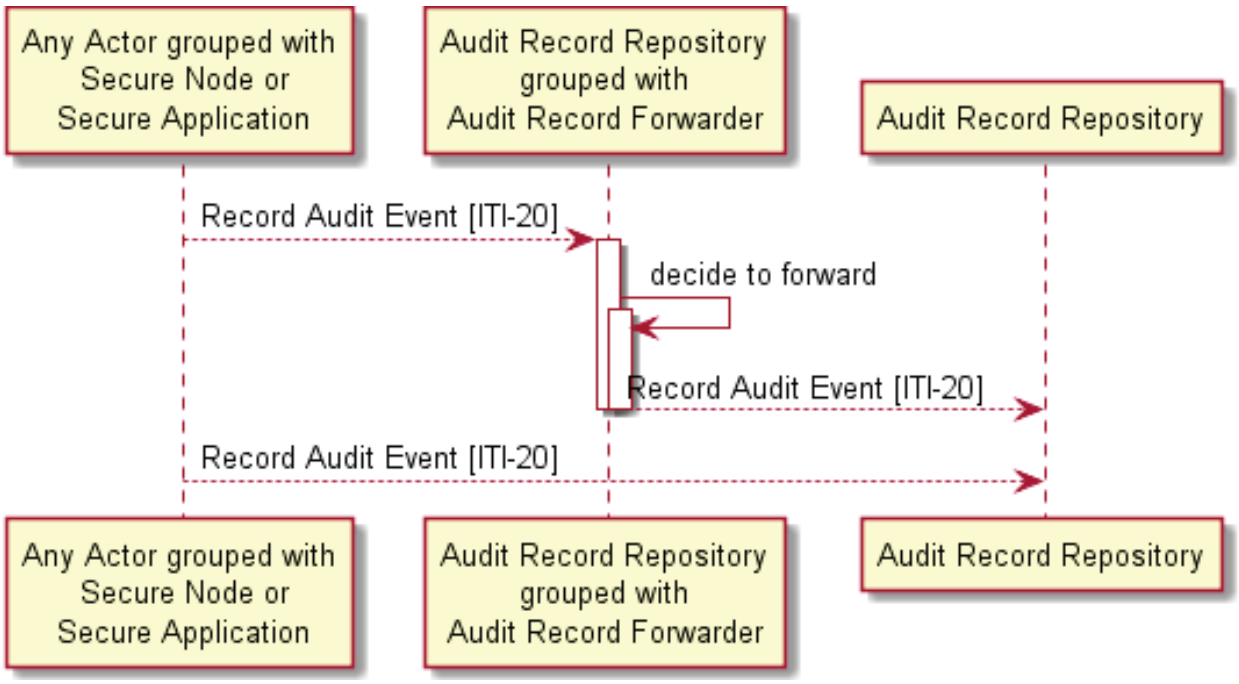


Figure 3.20.4-1: Interaction Diagram

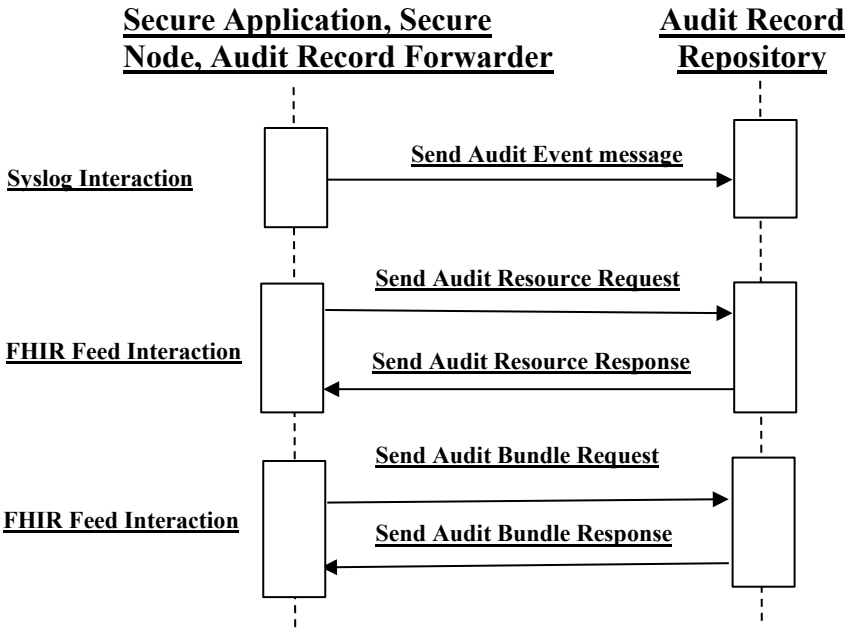
Note 1: Any actor initiating [ITI-20] may send to more than one Audit Record Repository.

Note 2: The Audit Repository that receives an [ITI-20] transaction may or may not be grouped with an Audit Record Forwarder. This diagram does not show a chain of forwarding between actors.

Transaction [ITI-20] defines three different interactions that can be used for auditing:

1. **The "Send Audit Event Message - Syslog Interaction" is used for auditing using Syslog protocol (see Section 3.20.4.1)**
2. **The "Send Audit Resource Request Message - FHIR Feed Interaction" is used for auditing a single FHIR AuditEvent Resource using RESTful protocol (see Section 3.20.4.2)**
3. **The "Send Audit Bundle Request Message - FHIR Feed Interaction" is used for auditing a bundle of FHIR AuditEvent Resources using RESTful protocol (see Section 3.20.4.4)**

The diagram below shows the three interactions that this transaction supports:



*Editor: add **new** Sections: 3.40.4.2, 3.40.4.3, 3.40.4.4, 3.40.4.5, and subsections under Section 3.20.4 (following Section 3.20.4.1.3 Expected Actions)*

3.20.4 Messages

…

3.20.4.2 Send Audit Resource Request Message – FHIR Feed Interaction

An actor that is grouped with Secure Node or Secure Application, or an Audit Record Forwarder, detects an event that should be reported and uses the Send Audit Resource Request message to send a report about the event to an Audit Record Repository.

A Secure Node, Secure Application or Audit Record Forwarder, that supports the ATX: FHIR Feed Option, uses this message to post a single AuditEvent Resource to the Audit Record Repository using a FHIR create interaction (see https://www.hl7.org/fhir/R4/http.html#create).

3.20.4.2.1 Trigger Events

This message is sent when an actor that is grouped with Secure Node or Secure Application or an Audit Record Forwarder needs to post a single AuditEvent Resource to the Audit Record Repository.

There are two trigger events:

1. A Secure Node or Secure Application detects an event that should be reported to the Audit Record Repository. This transaction does not specify all of the policies or reasons

for reporting events. They may be specified in other IHE profiles, they may be specified by local law or regulation, or they may be specified by local policy.

2. An Audit Record Forwarder determines that a received AuditEvent Resource should be sent to another Audit Record Repository. This transaction does not specify what rules or policies determine whether an AuditEvent Resource should be forwarded.

An actor in any IHE profile, when grouped with a Secure Node or Secure Application, shall be able to report the events defined in Table 3.20.4.1.1.1-1. Additional reportable events are often identified for specific events in other IHE profiles, and are documented in that profile or transaction.

3.20.4.2.2 Message Semantics

A Secure Node, Secure Application or Audit Record Forwarder shall issue an HTTP request according to requirements defined in the FHIR specification for "create" interaction (http://hl7.org/fhir/R4/http.html#create). The message uses an HTTP POST method to send a FHIR AuditEvent Resource.

The Secure Node, Secure Application or Audit Record Forwarder shall submit the FHIR AuditEvent Resource in either XML format or JSON format. Values for mime-type of the request message are defined in the ITI TF-2: Appendix Z.6.

An AuditEvent Resource that reflect Audit Message definition defined in IHE Technical Framework shall conform to the requirements defined in Section 3.20.4.2.2.1.

3.20.4.2.2.1 Mapping between DICOM Audit Message definitions and FHIR AuditEvent Resource for the FHIR Feed interactions

The mappings between IHE defined Audit Message content and FHIR AuditEvent Resource is based on FHIR Table 6.4.7.4 (http://hl7.org/fhir/R4/auditevent-mappings.html) that is further constrained in Table 3.20.4.2.2.1-1.

Table 3.20.4.2.2.1-1 is normative and contains mappings from Audit Message definitions for IHE transactions and based on DICOM standard into a FHIR AuditEvent Resource.

Table 3.20.4.2.2.1-1: DICOM Audit Message Definitions represented into an AuditEvent Resource

DICOM AuditMessage	FHIR AuditEvent Resource
EventIdentification.EventID	type
EventIdentification.EventTypeCode	subtype
EventIdentification@EventActionCode	action
EventIdentification@EventDateTime	recorded
EventIdentification@EventOutcomeIndicator	outcome
EventIdentification.EventOutcomeDescription	outcomeDesc
EventIdentification.purposeOfUse	purposeOfEvent
ActiveParticipant	agent

DICOM AuditMessage	FHIR AuditEvent Resource
ActiveParticipant.RoleIDCode	agent.type (Note 1)
ActiveParticipant.RoleIDCode	agent.role (Note 1)
ActiveParticipant@UserId	agent.who
ActiveParticipant@AlternativeUserId	agent.altId
ActiveParticipant@UserName	agent.name
ActiveParticipant@UserIsRequestor	agent.requestor
ParticipantRoleIDCode	agent.policy
ActiveParticipant.MediaIdentifier.MediaType	agent.media
ActiveParticipant@NetworkAccessPointID	agent.network.address
ActiveParticipant@NetworkAccessPointTypeCode	agent.network.type
AuditSourceIdentification	source
AuditSourceIdentification@AuditEnterpriseSiteId	source.site
AuditSourceIdentification@AuditSourceId	source.observer
AuditSourceIdentification.AuditSourcetypeCode	source.type
ParticipantObjectIdentification	entity
ParticipantObjectIdentification@ParticipantObjectID and ParticipantObjectIdentification.ParticipantObjectIDTypeCode	entity.what
ParticipantObjectIdentification@ParticipantObjectTypeCode	entity.type
ParticipantObjectIdentification@ParticipantObjectTypeCodeRole	entity.role
ParticipantObjectIdentification@ParticipantObjectDataLifeCycle	entity.lifecycle
ParticipantObjectIdentification@ParticipantObjectSensitivity	entity.securityLabel
ParticipantObjectIdentification.ParticipantObjectName	entity.name (Note 2)
ParticipantObjectIdentification.ParticipantObjectQuery	entity.query (Note 2)
ParticipantObjectIdentification.ParticipantObjectDetail	entity.detail
ParticipantObjectIdentification.ParticipantObjectDetail@type	entity.detail.type
ParticipantObjectIdentification.ParticipantObjectDetail@value	entity.detail.ValueBase64Binary

Note 1: If the Audit Record Repository knows the ActiveParticipant.RoleIDCode as a type, it should be mapped to `agent.type`. Otherwise the default mapping is to `agent.role`.

Note 2: Only one element between `entity.name` and `entity.query` shall be used in the AuditEvent Resource

3.20.4.2.3 Expected Actions

The Audit Record Repository shall support all the mime-types defined in ITI TF-2: Appendix Z.6.

On receipt of the Send Audit Resource Request message, the Audit Record Repository shall validate the Resources and respond with one of the HTTP codes defined in Section 3.20.4.3.2 Message Semantics.

For the Resource received, the Audit Record Repository may:

- discard the Resource as irrelevant

- retain the Resource in an internal data store
- perform other processing on the Resource

The Audit Record Repository may apply a variety of data retention rules to the data store. This transaction does not specify data retention rules. These usually depend upon the purposes assigned to a specific Audit Record Repository.

If needed, an Audit Record Repository that needs to store a received AuditEvent Resource as a DICOM Audit Message can do the transformation from the FHIR Resource to a DICOM message according to the requirements defined in Table 3.20.4.2.2.1-1.

The Audit Record Repository shall store any resources that were not discarded and make them available for further search via the Retrieve ATNA Audit Event [ITI-81] transaction. These events shall not be available for further search via Retrieve Syslog Events [ITI-82] transaction.

When the Audit Record Repository is grouped with an Audit Record Forwarder, the Audit Record Forwarder shall:

- apply filtering rules to all AuditEvent Resources received by the Audit Record Repository, and
- forward all AuditEvent Resources that match filters to their configured destinations.

If needed, an Audit Record Forwarder that will forward a received AuditEvent Resource using the Audit Event message (DICOM audit event via syslog protocol) can do the transformation from the FHIR Resource to a DICOM message according to the requirements defined in Table 3.20.4.2.2.1-1.

3.20.4.3 Send Audit Resource Response

The Audit Record Repository responds to the Secure Node, Secure Application or Audit Record Forwarder using a Send Audit Resource Response message in order to inform the client about the result of the operation.

3.20.4.3.1 Trigger Events

When the Audit Record Repository has finished storing the AuditEvent Resource received, it sends this message back to the client acknowledging the result of the request.

3.20.4.3.2 Message Semantics

The Audit Record Repository returns an HTTP Status code appropriate to the processing, conforming to specification requirements as specified in https://www.hl7.org/fhir/R4/http.html#create.

If the outcome is a success, the http status code of the response shall be a 2xx code.

If the outcome is a failure, the Audit Record Repository shall be capable of returning status codes according to what is defined in https://www.hl7.org/fhir/R4/http.html#create.

The Audit Record Repository can return other status codes 4xx or 5xx in accordance to internal business rules that are out of scope for this transaction.

3.20.4.3.3 Expected Actions

The Audit Record Repository could return failures. For this reason, it is up to the client to decide what to do with failures that have been returned by the Audit Record Repository.

3.20.4.4 Send Audit Bundle Request Message – FHIR Feed Interaction

A Secure Node, Secure Application or Audit Record Forwarder that supports the ATX: FHIR Feed Option uses this message to post a Bundle of AuditEvent Resources to the Audit Record Repository using a FHIR batch interaction (see https://www.hl7.org/fhir/R4/http.html#transaction).

3.20.4.4.1 Trigger Events

This message is sent when an Audit Record Forwarder or an actor that is grouped with Secure Node or Secure Application needs to send multiple events that has been audited to the Audit Record Repository.

There are two trigger events:

1. A Secure Node or Secure Application detects at least one event that should be reported to the Audit Record Repository. This transaction does not specify all of the policies or reasons for reporting events. They may be specified in other IHE profiles, they may be specified by local law or regulation, or they may be specified by local policy.
2. An Audit Record Forwarder determines that at least one received AuditEvent Resource should be sent to another Audit Record Repository. This transaction does not specify what rules or policies determine whether an AuditEvent Resource should be forwarded.

An actor in any IHE profile, when grouped with a Secure Node or Secure Application, shall be able to report the events defined in Table 3.20.4.1.1.1-1. Additional reportable events are often identified for specific events in other IHE profiles, and are documented in that profile or transaction.

3.20.4.4.2 Message Semantics

An Audit Record Forwarder or an actor that is grouped with Secure Node or Secure Application shall issue an HTTP request according to requirements defined in the FHIR specification for "batch" interaction (see https://www.hl7.org/fhir/R4/http.html#transaction).

The Audit Record Repository and the client shall both support the "batch" interaction.

The message uses an HTTP POST method to submit a FHIR Bundle Resource. The client shall post FHIR resources in either XML format or JSON format. Values for mime-type of the request message are defined in the ITI TF-2: Appendix Z.6.

The FHIR Bundle Resource shall contain at least one FHIR AuditEvent Resource (https://www.hl7.org/fhir/R4/auditevent.html).

The element `Bundle.entry.request.method` shall be POST.

AuditEvent Resources included in the Bundle that reflect Audit Message definitions defined in IHE Technical Framework shall conform to the requirements defined in Section 3.20.4.2.2.1.

Table 3.20.4.4.2-1: Bundle Resource Constraints

Element & Cardinality	Constraints
`type` `[1..1]`	Shall be: `batch`
`entry` `[1..*]`	Shall contain at least one AuditEvent Resource.
`entry.request.method`	Shall be: `POST`

3.20.4.4.3 Expected Actions

The Audit Record Repository shall support all the mime-types defined in ITI TF-2: Appendix Z.6.

On receipt of the Send Audit Bundle Resource Request, the Audit Record Repository shall validate Resources included in it and respond with one of the HTTP codes defined in Section 3.20.4.5.2 Message Semantics.

For each Resource received in the Bundle, the Audit Record Repository may:

- Discard the Resource as irrelevant.
- Retain the Resource in an internal data store.
- Perform other processing on the Resource.

The Audit Record Repository may apply a variety of data retention rules to the data store. This transaction does not specify data retention rules. These are usually dependent upon the purposes assigned to a specific Audit Record Repository.

If needed, an Audit Record Repository that needs to store a received AuditEvent Resource as a DICOM Audit Message can do the transformation from the FHIR Resource to a DICOM message according to the requirements defined in Table 3.20.4.2.2.1-1.

The Audit Record Repository shall store any resources that were not discarded and make them available for further search via the Retrieve ATNA Audit Event [ITI-81] transaction. These events shall not be available for further search via Retrieve Syslog Events [ITI-82] transaction.

When the Audit Record Repository is grouped with an Audit Record Forwarder, the Audit Record Forwarder shall:

- Apply filtering rules to all AuditEvent Resources received by the Audit Record Repository, and
- Forward all AuditEvent Resources that match filters to their configured destinations.

If needed, an Audit Record Forwarder that needs to forward a received AuditEvent Resource using the Audit Event message can do the transformation from the FHIR Resource to a DICOM message according to the requirements defined in Table 3.20.4.2.2.1-1.

3.20.4.5 Send Audit Bundle Response

The Audit Record Repository sends a Send Audit Bundle Response message in response to a Send Audit Bundle Request.

3.20.4.5.1 Trigger Events

When the Audit Record Repository has finished storing the AuditEvent Resources received in the Bundle Resource, it sends back this message to the client acknowledging the result of the request.

3.20.4.5.2 Message Semantics

The Audit Record Repository returns an HTTP Status code appropriate to the processing, conforming to specification requirements as specified in https://www.hl7.org/fhir/R4/http.html#transaction-response.

When the Audit Record Repository has processed the request shall return an HTTP response with an overall status code.

To allow the client to know the outcome of the transaction, and the identities assigned to the resources by the Audit Record Repository, the Audit Record Repository shall return a Bundle, with type set to `batch-response`. Each entry element shall contain a response element with an HTTP Status Code which details the outcome of processing of the request entry.

If no “Prefer” header is specified in the request the server should respond as if it is set to `return=minimal`; see https://www.hl7.org/fhir/R4/http.html#ops.

If the outcome of the entry is a success, the http status code of the response shall be a 2xx code.

If the outcome of the entry is a failure, the Audit Record Repository shall be capable of returning status codes according to what is defined in https://www.hl7.org/fhir/R4/http.html#create.

The Audit Record Repository can return other status codes 4xx or 5xx in accordance to internal business rules that are out of scope for this transaction.

3.20.4.5.3 Expected Actions

The Audit Record Repository could return a partial success for the Bundle where some resources succeeded and other not. For this reason, it is up to the client to decide what to do with failures that have been returned by the Audit Record Repository.

Editor: Update Section 3.20.5 as follows

3.20.5 Security Considerations

The use of the TLS **or HTTPS** transport mechanism is recommended because the audit event messages often contain PHI or other sensitive information. See Section 3.20.4.1.2.1.

The use of the TLS transport mechanism is not always required because there are other means of protection that may be more appropriate in some situations. The decision to use the UDP transport mechanism should be based upon a security and privacy risk analysis.

The data store within the Audit Record Repository may contain sensitive information, and the Audit Record Repository analysis facilities may allow sensitive queries. It will be a high value target for malicious actors, and should be protected accordingly.

The Audit Record Repository is required to generate audit event messages for various kinds of use of the data store and configuration changes. This is specified in Section 3.20.4.1.1.

If the AuditEvent Message Option is supported on the Audit Record Repository, update, delete and patch interaction of AuditEvent Resources should be managed by local policies.

*Editor: Add **new** Sections 3.81 Retrieve ATNA Audit Event and 3.82 Retrieve Syslog Event to Volume 2.*

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 the Record Audit Event [ITI-20] transaction.

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

RFC2616	IETF Hypertext Transfer Protocol – HTTP/1.1	
RFC4627	The application/json Media Type for JavaScript Object Notation (JSON)	
RFC6585	IETF Additional HTTP Status Codes	
RFC5424	The Syslog Protocol	
RFC3339	Date and Time on the Internet: Timestamps	
HL7 FHIR	Release 4	http://hl7.org/fhir/R4/index.html

3.81.4 Messages

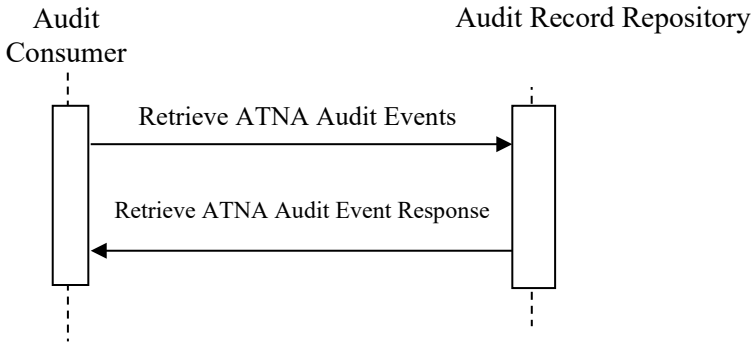


Figure 3.81.4-1: Interaction Diagram

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 Record

Audit Event [ITI-20] 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 to process or analyze ATNA audit records.

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 http://hl7.org/fhir/R4/search.html) on AuditEvent Resources (see http://hl7.org/fhir/R4/auditevent.html). 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.
- At least one `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 `date` parameter shall be used to specify an upper and/or lower bound for the search. At least one `date` parameter shall be present. 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 overloading the Audit Consumer. 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 values for the `date` search parameters shall be in RFC3339 format.

Note: RFC3339 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.recorded` 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 specification (http://hl7.org/fhir/R4/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 the FHIR AuditEvent Resource and the DICOM standard definition.

The Audit Consumer shall encode all search parameters per RFC3986 "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 **"&"** operator.
- 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.agent.network.address`.

- `agent.identifier` 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&agent.identifier=admin`

The Audit Record Repository shall match this parameter with the `AuditEvent.agent.who.identifier` field.
If a patient identifier it is used, the Audit Record Repository will return only the audit records where the patient is involved in the event as a user.

- `patient.identifier` is a parameter of `token` type. This parameter specifies the identifier of the patient involved in the event as a participant or as a user. 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 with the `AuditEvent.agent.who.identifier` and `AuditEvent.entity.what.identifier` where the reference resolve to a Patient.

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

  For example:

  - `?entity.identifier=urn:oid:1.2.3.4.5|123-203-FJ`
  - `?entity.identifier=|123-203-FJ.`

  The Audit Record Repository shall match this parameter with the `AuditEvent.entity.what.identifier` field that is of type identifier (ParticipantObjectID in DICOM schema). If a patient identifier is used the Audit Record Repository will return only audit records where the patient is involved in the event as a participant.

- `entity-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/audit-entity-type or http://hl7.org/fhir/resource-types defined by FHIR and a coded value. See http://hl7.org/fhir/R4/valueset-audit-entity-type.html for codes that shall be used.

  The Audit Record Repository shall match this parameter with the `AuditEvent.entity.type` field.

- `entity-role` is a parameter of `token` type. This parameter specifies the role played by the entity (e.g., Report, Location, Query, etc.). The parameter value shall contain the namespace URI http://hl7.org/fhir/object-role defined by FHIR and a coded value. See http://hl7.org/fhir/R4/object-role for codes that shall be used.

For example, to search all the audit records related to the document entity (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&entity-role=http://hl7.org/fhir/object-role|3&entity-id=urn:oid:1.2.3.4.5|12345
```

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

- `source.identifier` 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.observer.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://dicom.nema.org/resources/ontology/DCM` and a coded value. Codes available are defined by DICOM and IHE (see ITI TF-1: Table 3.20.4.1.1.1-1: 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://dicom.nema.org/resources/ontology/DCM|110106
```

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

- `subtype` is parameter of `token` type. This parameter identifies the specific IHE transaction that originates the audit record. The parameter value can contain the namespace URI `urn:ihe:event-type-code` to search for audit messages triggered by IHE transactions with the defined audit message. Each IHE transaction that defines an ATNA messages, specifies a code identifying the transaction itself, and assigns this code to the EventTypeCode element within the [ITI-20] audit record.

  For example, to search AuditEvent 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.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/audit-event-outcome and a code taken from the related value set. See http://hl7.org/fhir/R4/valueset-audit-event-outcome.html.

To search AuditEvent Resources related to failed events:

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

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

The HL7® FHIR® standard provides additional search parameters. This transaction does not define specific behavior on those parameters (such as `_sort`, `_include`, etc.). See http://hl7.org/fhir/R4/search.html for details about available parameters.

3.81.4.1.2.3 Populating Expected Response Format

The HL7® 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. For Desired Response Encoding and format negotiation see ITI TF-2: Appendix Z.6.

3.81.4.1.3 Expected Actions

The Audit Record Repository (ARR) maintains a database of audit events. The Audit Record Repository retains data according to local policies, and some data may be deleted.

The Audit Record Repository shall return all the audit events stored in its database that match the query parameters, and which the requester is authorized to view (see ITI TF-1: 9.4 for further details).

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
  - If the Audit Record Repository does not support the parameter, it shall be ignored;
  - 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 Audit Record Repository successfully processes the search request, it shall return the matching AuditEvent Resources inside a FHIR Bundle Resource.

The "Content-Type" of the response will depend upon the response format negotiation described in ITI TF-2: Appendix Z.6.

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 choose to return the results in a series of pages (see https://www.hl7.org/fhir/R4/http.html#paging).

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-2: Appendix Z.7 "Guidance on Access Denied Results".

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.

3.81.4.2.2.1 Mapping between FHIR and DICOM for query interaction

The mapping rules between FHIR AuditEvent Resources and DICOM AuditMessage format is based on FHIR Table 6.4.7.4 (http://hl7.org/fhir/R4/auditevent-mappings.html) that is further constrained in Table 3.81.4.2.2.1-1.

Table 3.81.4.2.2.1-1 is normative and defined a strict alignment between the AuditEvent Resource and the DICOM AuditMessage. However, Table 3.81.4.2.2.1-1 does not aim to resolve

the dissonance between the FHIR AuditEvent Resource and the DICOM AuditMessage, but rather it ensures interoperability between these two data models.

1125 The Audit Record Repository shall encode all the data within the DICOM format of the AuditMessage into the AuditEvent Resource(s) sent in the Retrieve ATNA Audit Event Response message.

Table 3.81.4.2.2.1-1: DICOM Tag Mapping for query interaction

AuditEvent Resource	AuditMessage
type	EventIdentification.EventID
subtype	EventIdentification.EventTypeCode
action	EventIdentification@EventActionCode
period	NOT PRESENT
recorded	EventIdentification@EventDateTime
outcome	EventIdentification@EventOutcomeIndicator
outcomeDesc	EventIdentification.EventOutcomeDescription
purposeOfEvent	EventIdentification.purposeOfUse
agent	ActiveParticipant
agent.type (Note 1)	ActiveParticipant.RoleIDCode
agent.role (Note 1)	ActiveParticipant.RoleIDCode
agent.who	ActiveParticipant@UserId
agent.altId	ActiveParticipant@AlternativeUserId
agent.name	ActiveParticipant@UserName
agent.requestor	ActiveParticipant@UserIsRequestor
agent.location	NOT PRESENT
agent.policy	ParticipantRoleIDCode
agent.media	ActiveParticipant.MediaIdentifier.MediaType
agent.network.address	ActiveParticipant@NetworkAccessPointID
agent.network.type	ActiveParticipant@NetworkAccessPointTypeCode
agent.purposeOfUse	NOT PRESENT
source	AuditSourceIdentification
source.site	AuditSourceIdentification@AuditEnterpriseSiteId
source.observer	AuditSourceIdentification@AuditSourceId
source.type	AuditSourceIdentification.AuditSourcetypeCode
entity	ParticipantObjectIdentification
entity.what	ParticipantObjectIdentification@ParticipantObjectID and ParticipantObjectIdentification.ParticipantObjectIDTypeCode
entity.type	ParticipantObjectIdentification@ParticipantObjectTypeCode
entity.role	ParticipantObjectIdentification@ParticipantObjectTypeCodeRole
entity.lifecycle	ParticipantObjectIdentification@ParticipantObjectDataLifeCycle
entity.securityLabel	ParticipantObjectIdentification@ParticipantObjectSensitivity
entity.name	ParticipantObjectIdentification.ParticipantObjectName

AuditEvent Resource	AuditMessage
entity.description	NOT PRESENT
entity.query	ParticipantObjectIdentification.ParticipantObjectQuery
entity.detail	ParticipantObjectIdentification.ParticipantObjectDetail
entity.detail.type	ParticipantObjectIdentification.ParticipantObjectDetail@type
entity.detail.ValueBase64Binary	ParticipantObjectIdentification.ParticipantObjectDetail@value

Note 1: If the Audit Record Repository knows the ActiveParticipant.RoleIDCode as a type, it should be mapped to `agent.type`. Otherwise the default mapping is to `agent.role`.

Note 2: Values recorded in the ParticipantObjectIdentification.ParticipantObjectDescription element shall be represented in the extension defined in https://www.hl7.org/fhir/R4/auditevent-profiles.html - extensions .

3.81.4.2.2.2 FHIR Bundle of Audit Events Messages

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

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 may involve the disclosure of sensitive information. Logging these retrieval transactions as a query event is appropriate. However, ATNA Profile does not require the Audit Record Repository to be able to send audit records using the Record Audit Event [ITI-20] transaction. The Audit Record Repository shall create and store locally an audit event as follows:

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV (110101, DCM, "Audit Log Used")
	EventActionCode	M	"R" (Read)
	EventDateTime	*U*	*not specialized*
	EventOutcomeIndicator	*U*	*not specialized*
	EventTypeCode	M	EV("ITI-81", "IHE Transactions", "Retrieve ATNA AuditEvent")
Source (Document Administrator) (1)			
Human Requestor (0..1)			
Destination (Document Registry) (1)			
Audit Source (Document Administrator) (1)			
AuditEvent Message (0..n)			

Where:

Source AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	The process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV(110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	M	"1" for machine (DNS) name, "2" for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Human Requestor (if known) AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*

	RoleIDCode	M	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*U*	*not specialized*
	NetworkAccessPointID	*U*	*not specialized*

1185

Destination AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV(110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	M	“1” for machine (DNS) name, “2” for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Audit Source AuditMessage/AuditSourceIdentification	*AuditSourceID*	*U*	*not specialized*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

AuditEvent Message AuditMessage/ ParticipantObjectIdentification	ParticipantObjectTypeCode	M	“2” (System object)
	ParticipantObjectTypeCodeRole	M	“13” (Security Resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(“12”, “RFC-3881”, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The URI of the Audit log
	ParticipantObjectName	U	“Security Audit Log”
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

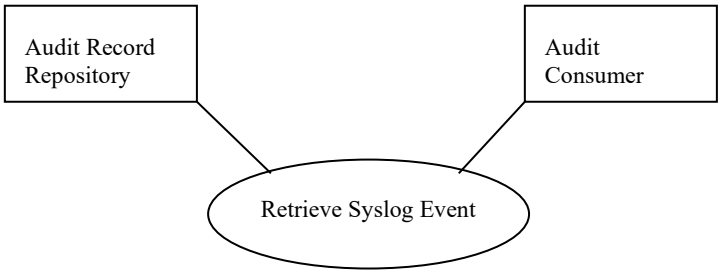
1190

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

1195 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 Standards

RFC2616	IETF Hypertext Transfer Protocol – HTTP/1.1
RFC4627	The application/json Media Type for JavaScript Object Notation (JSON)
RFC6585	IETF Additional HTTP Status Codes
RFC5424	The Syslog Protocol
RFC3339	Date and Time on the Internet: Timestamps

3.82.4 Messages

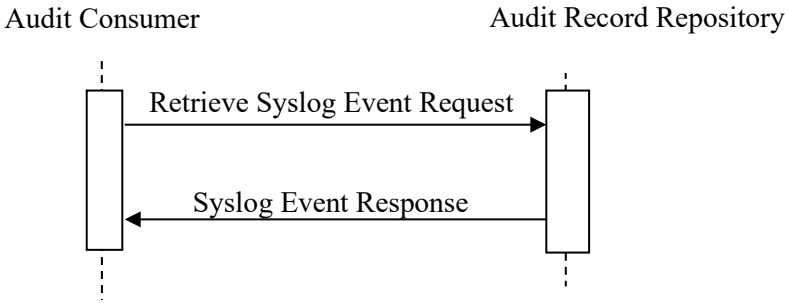


Figure 3.82.4-1: Interaction Diagram

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 Record Audit Event [ITI-20] transaction. See ITI TF-2: 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 from other services.
- "`syslogsearch`" is a required part of the URL that allows the Audit Consumer to ask for syslog messages stored in the Audit Record Repository.
- At least one `date` search parameters id required. 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.

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** parameters 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 RFC3339 format.

Note: RFC3339 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 RFC3986 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 RFC5424 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” 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 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: 9.4 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 RFC7231 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 RFC2616 Section 4.4, or subsequent versions of the HTTP specification.

Note: RFC2616 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 3.82.4.2.2-1: Syslog Message Encoding

Syslog Metadata	JSON element	dataType
PRI	Pri	<string>
VERSION	Version	<string>
TIMESTAMP	Timestamp	see RFC5424 (Sec. 6.2.3)
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

The Audit Record Repository shall construct a JSON array of syslog messages by parsing the message elements in each matching Syslog as defined in RFC5424 as strings identified by the element name in RFC5424. If an element is absent from the syslog message, the Audit Record Repository shall not include this element in the JSON encoding.

```
{
      {
      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"
        }
}
```

Figure 3.82.4.2.2.1-1: Example JSON encoded array of syslog messages

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: 9.5.

3.82.5.1 Security Audit Considerations

This transaction may involve the disclosure of sensitive information. Logging these retrieval transactions as a query event is appropriate. However, ATNA Profile does not require the Audit Record Repository to be able to send audit records using the Record Audit Event [ITI-20] transaction. The Audit Record Repository shall create and store locally an audit event as follows:

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV (110101, DCM, "Audit Log Used")
	EventActionCode	M	"R" (Read)
	EventDateTime	*U*	*not specialized*
	EventOutcomeIndicator	*U*	*not specialized*
	EventTypeCode	M	EV("ITI-82", "IHE Transactions", "Retrieve Syslog Event")
Source (Audit Consumer) (1)			
Human Requestor (0..1)			
Destination (Audit Record Repository) (1)			
Audit Source (Audit Record Repository) (1)			
Syslog message (0,..n)			

Where:

Source AuditMessage/ ActiveParticipant	*UserID*	*U*	*not specialized*
	AlternativeUserID	M	The process ID as used within the local operating system in the local system logs.
	UserName	*U*	*not specialized*

	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV(110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	M	“1” for machine (DNS) name, “2” for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Human Requestor (if known) AuditMessage/ ActiveParticipant	UserID	M	Identity of the human that initiated the transaction.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	Access Control role(s) the user holds that allows this transaction.
	NetworkAccessPointTypeCode	*U*	*not specialized*
	NetworkAccessPointID	*U*	*not specialized*

1410

Destination AuditMessage/ ActiveParticipant	UserID	M	SOAP endpoint URI.
	AlternativeUserID	*U*	*not specialized*
	UserName	*U*	*not specialized*
	UserIsRequestor	*U*	*not specialized*
	RoleIDCode	M	EV(110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	M	“1” for machine (DNS) name, “2” for IP address
	NetworkAccessPointID	M	The machine name or IP address.

Audit Source AuditMessage/AuditSourceIdentification	*AuditSourceID*	*U*	*not specialized*
	AuditEnterpriseSiteID	*U*	*not specialized*
	AuditSourceTypeCode	*U*	*not specialized*

Syslog message AuditMessage/ ParticipantObjectIdentification	ParticipantObjectTypeCode	M	“2” (System object)
	ParticipantObjectTypeCodeRole	M	“13” (Security Resource)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	EV(“12”, “RFC-3881”, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	The URI of the Audit log
	ParticipantObjectName	U	“Security Audit Log”
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

Editor: Update the "Appendix Z on HL7 FHIR" TI supplement, Section Z.8:

Z.8 Mobile Security Considerations

There are many security and privacy concerns with mobile devices, including lack of physical control. Many common information technologies use of HTTP, including REST, access far less sensitive information than health information. These factors present an especially difficult challenge for the security model. Application developers should perform a Risk Assessment during design of their applications, and organizations responsible for the operational environment should perform Risk Assessments on the design and deployment of the operational environment. See FHIR Security and Privacy Module http://hl7.org/fhir/R4/secpriv-module.html.

Actors should not communicate any patient information unless proper authentication, authorization, and communications security have been performed.

There are many reasonable methods of securing interoperability transactions. These security models can be layered in without modifying the characteristics of the transaction. The use of TLS is encouraged, specifically the use of the ATNA Profile. User authentication on mobile devices is encouraged using Internet User Authorization (IUA) Profile. The IUA Profile is a profile of the OAuth protocol. IUA enables external Authorization providers, which can leverage pluggable authentication providers, such as OpenID Connect. The network communication security and user authentication are layered in at the HTTP transport layer and do not modify the interoperability characteristics defined in the transaction.

~~**Security audit logging (e.g., ATNA) is recommended. Support for ATNA-based audit logging on the mobile health device may be beyond the ability of the client-constrained environment. For example, the client actor may only support HTTP interactions using JSON encoding, while the Record Audit Event [ITI-20] transaction requires the SYSLOG protocol and XML encoding. For this reason, the use of ATNA Audit Logging is not mandated. This means that the organization responsible for the operational environment must choose how to mitigate the risk of relying only on the service side audit logging.**~~

Security audit logging (e.g., ATNA) is recommended. Support for ATNA-based audit logging on the mobile health device can be done using the Record Audit Event [ITI-20] transaction that supports HTTP interactions for both JSON and XML encoding.

Many transactions using HTTP REST will include query parameters that would be identifiers, quasi-identifiers, or sensitive health topics. For example, it is common for patient identifier to be a query parameter. With this URL pattern, the query parameters are typically visible in the server audit log or browser history. The risk from this visibility should be mitigated in system or operational design, by protecting the logs as sensitive data, or by designing other measures into the system to prevent inappropriate exposure.

