Digital Imaging and Communications in Medicine (DICOM)

Supplement 95: Audit Trail Messages

Prepared by:

DICOM Standards Committee

1300 N. 17th Street, Suite 1847

Rosslyn, Virginia 22209 USA

VERSION: Final Text 27 August 2010

Prepared persuent to Work Item 2001-11-C

Table of Contents

1 Scope and Field of Application

This Supplement describes a mechanism for DICOM entities to send audit trail information to a collection and logging application. The goal is to simplify the collection of audit trail information. Rather than having a security administrator extract audit information from each individual node, the nodes send selected audit information to a collection point.

The joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC) in its white paper "Security and Privacy Auditing in Health Care Information Technology", HL7, IHE, and ASTM in PS 115 "Audit and Disclosure Logs for Use in Health Information Systems" outlined requirements for audit information collection in the medical environment. Collection and review of such information is required by various governmental regulations, such as HIPAA, and should be part of most institutions' local security policies. The use cases and suggestions in these documents pertaining to audit trail generation for surveillance purposes guided the creation of this supplement.

Audit trails can be used for surveillance purposes, to detect when interesting events might be happening that warrant further investigation. Or they can be used forensically, after the detection of a security breach, to determine what went wrong and who or what was at fault. Although any audit trail information can be helpful to a forensic investigation, this supplement focuses on exchanging information needed for the surveillance aspects of an audit log. It is likely that a node might maintain more comprehensive audit logs, useful for forensic investigations, with information that is not sent to the central collection point where surveillance occurs.

The information contained within an audit trail might also be useful in creating disclosure logs. However, disclosure logs were not considered within the scope of this supplement.

Auditable events happen in a distributed fashion; however, most sites have a single entity responsible for auditing compliance to security rules. To simplify the collection and subsequent analysis of audit information, this supplement specifies messages and transport mechanisms through which devices can send audit data triggered by DICOM transactions to that single entity. The HL7 Security and Accountability SIG and DICOM WG 14 have jointly defined the base format of the payload for the syslog message, after consultation with ASTM and the SPC. This common message format is defined in an IETF Draft Internet Standard as an XML schema. This Supplement augments the base format by defining the vocabulary necessary for DICOM application to fill in the XML-based audit trail message. The reliable syslog mechanism defined by the IETF is used to communicate the audit trail message to the collection point.

The IHE initiative performed the initial work leading up to this specification of audit trail message formats, vocabularies, and transfer mechanisms. This supplement attempts to cover the use cases and scenarios outlined in the IHE Radiology Technical Framework using DICOM specializations of the base IETF format.

2 Additions to PS 3.2

Modify Section 7.6

7.6 SECURITY PROFILES

….

An implementation shall list in its Conformance Statement any Security Profiles that it supports, how it selects which Security Profiles it uses, ~~and~~ how it uses features of that Security Profile**, and any extensions it makes to that Security Profile**.

Modify Section A.7.1

Any support for Security ~~p~~**P**rofiles as defined in PS 3.15 shall be described here~~:~~**. Any extensions to Security Profiles shall be described, e.g. extended schema for audit trail messages.**

4 Additions to PS 3.6

Add the following data elements to PS3.6, Annex A:

Table A-3
CONTEXT GROUP UID VALUES

Context UID	Context Identifier	Context Group Name
1.2.840.10008.6.1.903	400	Audit Event ID
1.2.840.10008.6.1.904	401	Audit Event Type Code
1.2.840.10008.6.1.905	402	Audit Active Participant Role ID Code
1.2.840.10008.6.1.906	403	Security Alert Type Code
1.2.840.10008.6.1.907	404	Audit Participant Object ID Type Code
1.2.840.10008.6.1.908	405	Media Type Code

5 Additions to PS 3.15

Add the following references to section 2 Normative References

RFC5424 The Syslog Protocol

RFC5425 Transport Layer Security (TLS) Transport Mapping for Syslog

RFC5426 Transmission of Syslog Messages over UDP

Add the following section to PS 3.15

6.X AUDIT TRAIL PROFILES

An implementation may claim conformance to one or more Audit Trail Profiles. Such profiles outline the generation and transport of audit messages for security and privacy policy enforcement.

Audit Trail Profiles are specified in Annex A.

Add sections A.x, A.y, and A.z to PS 3.15

A.X AUDIT TRAIL MESSAGE FORMAT PROFILE

To help assure healthcare privacy and security in automated systems, usage data need to be collected. These data will be reviewed by administrative staff to verify that healthcare data is being used in accordance with the healthcare provider's data security requirements and to establish accountability for data use. This data collection and review process is called security auditing and the data itself comprises the audit trail. Audit trails can be used for surveillance purposes to detect when interesting events might be happening that warrant further investigation.

This profile defines the format of the data to be collected and the minimum set of attributes to be captured by healthcare application systems for subsequent use by a review application. The data includes records of who accessed healthcare data, when, for what action, from where, and which patients' records were involved. No behavioral requirements are specified for when audit messages are generated, or for what action should be taken on their receipt. These are subject to local policy decisions and legal requirements.

Any implementation that claims conformance to this Security Profile shall:

a. format audit trail messages in accordance with the XML schema specified in A.X.1 in a fashion that allows those messages to be validated against that XML schema, following the general conventions specified in Section A.X.2.

b. for the events described in this Profile comply with the restrictions specified by this Profile in Section A.X.3, and describe in its conformance statement any extensions.

   Note: An implementation may include implementation-specific extensions as long as the above conditions are met.

c. describe in its conformance statement the events that it can detect and report,

d. describe in its conformance statement the processing it can perform upon receipt of a message

e. describe in its conformance statement how event reporting and processing can be configured

   Note: Other profiles specify the transmission of audit messages.

A.X.1 DICOM Audit Message Schema

Implementations claiming conformance to this profile shall use the following XML schema to format audit trail messages. This schema is derived from the schema specified in RFC 3881 IETF draft internet standard “Security Audit and Access Accountability XML Message Data Definitions for Healthcare Applications”, according to W3C Recommendation "XML Schema Part 1: Structures," version 1.0, May 2001, and incorporates the DICOM extensions and restrictions outlined in section A.X.2.

This schema is provided in Relax NG Compact format.

Note: This schema can be converted into an equivalent XML schema or other electronic format. It includes some modifications to the RFC 3881 schema that reflect field experience with audit message requirements. It extends the RFC 3881 schema.

```
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

# This defines the coded value type. The comment shows a pattern that can be used to further
# constrain the token to limit it to the format of an OID.  Not all schema software
# implementations support the pattern option for tokens.

other-csd-attributes =
            (attribute codeSystemName {token} | # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
            attribute codeSystemName {token}),  # This makes clear that codeSystemName is either
an OID or String
            attribute displayName {token}?,
            attribute originalText {token}    #Note: this also corresponds to DICOM " Code Meaning"
CodedValueType =
            attribute csd-code {token},
            other-csd-attributes

# Define the event identification, used later

EventIdentificationContents =
         element EventID {CodedValueType },
         element EventTypeCode {CodedValueType}*,   # Note: DICOM/IHE defines and uses this
differently than RFC-3881
         attribute EventActionCode {                        # Optional action code
                  "C" |          ## Create
                  "R" |          ## Read
                  "U" |          ## Update
                  "D" |          ## Delete
                  "E" }?,        ## Execute
          attribute EventDateTime {xsd:dateTime},
         attribute EventOutcomeIndicator {
                  "0" |               ## Nominal Success (use if status otherwise unknown or
ambiguous)
                      "4" |           ## Minor failure (per reporting application definition)
                      "8" |           ## Serious failure (per reporting application definition)
                      "12"},          ## Major failure, (reporting application now unavailable)
         element EventOutcomeDescription {text}?

# Define AuditSourceIdentification, used later
#  Note: This includes one constraint that cannot be represented yet in RNC.  The use of a token
other
#        than the specified codes is permitted only if the codeSystemName is present.
#  Note: This has no elements, only attributes.

AuditSourceIdentificationContents =
```

```
                attribute code {
                        "1" |        ## End-user display device, diagnostic device
                        "2" |        ## Data acquisition device or instrument
                        "3" |        ## Web Server process or thread
                        "4" |        ## Application Server process or thread
                        "5" |        ## Database Server process or thread
                        "6" |        ## Security server, e.g., a domain controller
                        "7" |        ## ISO level 1-3 network component
                        "8" |        ## ISO level 4-6 operating software
                        "9" |     ## other
                        token },             ## other values are allowed if a codeSystemName is
present
            other-csd-attributes?, ## If these are present, they define the meaning of code
                attribute AuditEnterpriseSiteID {token}?,
                attribute AuditSourceID {token},
                element AuditSourceTypeCode {token}*

# Define ActiveParticipantType, used later

        ActiveParticipantContents =
                element RoleIDCode {CodedValueType}*,
                element MediaIdentifier {
                  element MediaType {CodedValueType}}?,
                attribute UserID {text},
                attribute AlternativeUserID {text}?,
                attribute UserName {text}?,
                attribute UserIsRequestor {xsd:boolean},
                attribute NetworkAccessPointID {token}?,
                attribute NetworkAccessPointTypeCode {
                        "1" |        ## Machine Name, including DNS name
                        "2" |        ## IP Address
                        "3" |        ## Telephone Number
                        "4" |      ## Email address
                        "5"}?      ## URI (user directory, HTTP-PUT, ftp, etc.)

# The BinaryValuePair is used in ParticipantObject descriptions to capture parameters.
# All values (even those that are normally plain text) are encoded as xsd:base64Binary.  This
# is to preserve details of encoding (e.g., nulls) and to protect against text contents that
contain
# XML fragments.  These are known attack points against applications, so security logs
# can be expected to need to capture them without modification by the audit encoding process.

                ValuePair      = # clarify the name
                        attribute type {token},
                        attribute value {xsd:base64Binary}    # used to encode potentially binary,
mal-formed XML text, etc.

# Define ParticipantObjectIdentification, used later

# Participant Object Description, used later

        DICOMObjectDescriptionContents =
                element MPPS {
                        attribute UID {token}}*, #  # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
                element Accession {
                        attribute Number {token}}*,
                element SOPClass {     # SOP class for one study
                        element Instance {
                                attribute UID {token}}*,  # OID pattern="[0-2]((\.0)|(\.[1-9][0-
9]*))*"
                        attribute UID {token}?, # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
                        attribute NumberOfInstances {xsd:integer}
                        },
        element ParticipantObjectContainsStudy {
             element StudyIDs {
                 attribute UID {token}}*
            },
```

```
        element Encrypted {xsd:boolean}?,
290             element Anonymized {xsd:boolean}?

ParticipantObjectIdentificationContents =
                element ParticipantObjectIDTypeCode {CodedValueType},
                (element ParticipantObjectName {token} |     # either a name or
295              element ParticipantObjectQuery {xsd:base64Binary}), # a query ID field,
                element ParticipantObjectDetail {ValuePair}*, # optional details, these can be
extensive and large
                element ParticipantObjectDescription {token}*, # optional descriptive text
                DICOMObjectDescriptionContents, # These are extensions made by DICOM to RFC-3881
300 schema for use describing DICOM objects
                attribute ParticipantObjectID {token}, #mandatory ID
                attribute ParticipantObjectTypeCode {( # optional type
                        "1" |    #3 Person
                        "2" |    #3 System object
305                     "3" |    #3 Organization
                        "4")}?,         ## Other
                attribute ParticipantObjectTypeCodeRole {( ## optional role
                        "1" |    ## Patient
                        "2" |    ## Location
310                     "3" |    ## Report
                        "4" |    ## Resource
                        "5" |    ## Master File
                        "6" |    ## User
                        "7" |    ## List
315                     "8" |    ## Doctor
                        "9" |    ## Subscriber
                        "10" |   ## guarantor
                        "11" |   ## Security User Entity
                        "12" |   ## Security User Group
320                     "13" |   ## Security Resource
                        "14" |   ## Security Granulatiry Definition
                        "15" |   ## Provider
                        "16" |   ## Report Destination
                        "17" |   ## Report Library
325                     "18" |   ## Schedule
                        "19" |   ## Customer
                        "20" |   ## Job
                        "21" |   ## Job Stream
                        "22" |   ## Table
330                     "23" |   ## Routing Criteria
                        "24")}?,    ## Query?,
                attribute ParticipantObjectDataLifeCycle {( # optional life cyucle stage
                        "1" | ## Origination, Creation
                        "2" | ## Import/ Copy
335                     "3" | ## Amendment
                        "4" | ## Verification
                        "5" | ## Translation
                        "6" | ## Access/Use
                        "7" | ## De-identification
340                     "8" | ## Aggregation, summarization, derivation
                        "9" | ## Report
                        "10" | ## Export
                        "11" | ## Disclosure
                        "12" | ## Receipt of Disclosure
345                     "13" | ## Archiving
                        "14" | ## Logical deletion
                        "15")}?,  ## Permanent erasure, physical destruction
                attribute ParticipantObjectSensistity {token}?

350


# The basic message

message = element AuditMessage {
```

```
                element EventIdentification {EventIdentificationContents},  # The event must be
identified
                element ActiveParticipant {ActiveParticipantContents}+, # It has one or more active
participants
                element AuditSourceIdentification {AuditSourceIdentificationContents}, # It is
reported by one source
                element ParticipantObjectIdentification {ParticipantObjectIdentificationContents}*
# It may have other objects involved
                }

# And finally the magic statement that message is the root of everything.

start=message
```

Figure A.X.1-1 Audit Message Schema

A.X.2 General Message Format Conventions

The following table lists the primary fields from the message schema specified in A.X.1, with additional instructions, conventions, and restrictions on how DICOM applications shall fill in the field values. Please refer to RFC 3881 for the complete definition and specification of fields taken from the schema specified therein. In addition, the following table lists the additional fields that are part of DICOM-specific extensions in the DICOM Audit Message Schema (see A.X.1). The fields names are only those leaf elements and attributes that are specialized or extended for this profile. Note that these fields may be enclosed in other XML elements, as specified by the schema.

Table A.X.2-1 General Message Format

	Field Name	Opt.	Description from RFC 3881	Additional Conditions on Field Format/Value
Event	EventID	M	"Identifier for a specific audited event …"	The identifier for the family of event. E.g., "User Authentication". Extended by DICOM using DCID (400)
	EventActionCode	U	"Indicator for type of action performed during the event that generated the audit."	See Schema
	EventDateTime	M	"Universal coordinated time (UTC), i.e. a date/time specification that is unambiguous as to local time zones."	The time at which the audited event occurred. See section A.X.2.5
	EventOutcomeIndicator	M	"Indicates whether the event succeeded or failed."	When a particular event has some aspects that succeeded and some that failed, then one message shall be generated for successful actions and one message for the failed actions (i.e., not a single message with mixed results).
	EventTypeCode	U	"Identifier for the category of event."	The specific type(s) within the family applicable to the event, e.g., "User Login". Extended by DICOM using DCID (401)
Active Participant (multi-	UserID	M	"Unique identifier for the user actively participating in the event."	See section A.X.2.1

	AlternativeUserID	U	"Alternative unique identifier for the user."	See section A.X.2.2
	UserName	U	"The human-meaningful name for the user."	See section A.X.2.3
	UserIsRequestor	M	"Indicator that the user is or is not the requestor, or initiator, for the event being audited."	Used to identify which of the participants initiated the transaction being audited. If the audit source cannot determine which of the participants is the requestor, then the field shall be present with the value FALSE in all participants. The system shall not identify multiple participants as UserIsRequestor. If there are several known requestors, the reporting system shall pick only one as UserIsRequestor.
	RoleIDCode	U	"Specification of the role(s) the user plays when performing the event, as assigned in role-based access control security."	Extended by DICOM using DCID (402) Usage of this field is refined in the individual message descriptions below. Other additional roles may also be present, since this is a multi-valued field.
	NetworkAccessPointTypeCode	U	"An identifier for the type of network access point …"	See Section A.X.2.4
	NetworkAccessPointID	U	"An identifier for the network access point of the user device This could be a device id, IP address, or some other identifier associated with a device."	
Audit Source	AuditEnterpriseSiteID	U	"Logical source location within the healthcare enterprise network, e.g., a hospital or other provider location within a multi-entity provider group."	Serves to further qualify the Audit Source ID, since Audit Source ID is not required to be globally unique.
	AuditSourceID	M	"Identifier of the source …"	The identification of the system that detected the auditable event and created this audit message. Although often the audit source is one of the participants, it could also be an external system that is monitoring the activities of the participants (e.g., an add-on audit-generating device).
	AuditSourceTypeCode	U	"Code specifying the type of source …"	Used as defined in RFC 3881. E.g., an acquisition device might use "2" (data acquisition device), a PACS/RIS system might use "4 "(application server process).
Participant Object (multi-valued)	ParticipantObjectTypeCode	U	"Code for the participant object type being audited. This value is distinct from the user's role or any user relationship to the participant object."	Used as defined in RFC 3881
	ParticipantObjectTypeCodeRole	U	"Code representing the functional application role of Participant Object being audited."	Used as defined in RFC 3881

	ParticipantObjectDataLifeCycle	U	"Identifier for the data life-cycle stage for the participant object. This can be used to provide an audit trail for data, over time, as it passes through the system."	Used as defined in RFC 3881.
	ParticipantObjectIDTypeCode	M	"Describes the identifier that is contained in Participant Object ID."	Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.
	ParticipantObjectSensitivity	U	"Denotes policy-defined sensitivity for the Participant Object ID such as VIP, HIV status, mental health status, or similar topics."	Used as defined in RFC 3881.
	ParticipantObjectID	M	"Identifies a specific instance of the participant object."	Usage refined by individual message descriptions
	ParticipantObjectName	U	"An instance-specific descriptor of the Participant Object ID audited, such as a person's name."	Usage refined by individual message descriptions
	ParticipantObjectQuery	U	"The actual query for a query-type participant object."	Usage refined by individual message descriptions
	ParticipantObjectDetail	U	"Implementation-defined data about specific details of the object accessed or used."	Used as defined in RFC 3881. Note: The value field is xs:base64Binary encoded, making this attribute suitable for conveying binary data.
	SOPClass	MC	(DICOM extension)	The UIDs of SOP classes referred to in this participant object. Required if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") and any of the optional fields (AccessionNumber, ContainsMPPS, NumberOfInstances, ContainsSOPInstances,Encrypted,Anonymized) are present in this Participant Object. May be present if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") even though none of the optional fields are present.
	Accession	U	(DICOM extension)	An Accession Number(s) associated with this participant object.
	MPPS	U	(DICOM extension)	An MPPS Instance UID(s) associated with this participant object.
	NumberOfInstances	U	(DICOM extension)	The number of SOP Instances referred to by this participant object.

	Instance	U	(DICOM extension)	SOP Instance UID value(s) Note: Including the list of SOP Instances can create a fairly large audit message. Under most circumstances, the list of SOP Instance UIDs is not needed for audit purposes.
	Encrypted	U	(DICOM extension)	a single value of True or False indicating whether or not the data was encrypted. Note: If there was a mix of encrypted and non-encrypted data, then create two event reports.
	Anonymized	U	(DICOM extension)	A single value of True or False indicating whether or not all patient identifying information was removed from the data
	ParticipantObjectContainsStudy	U	(DICOM extension)	A Study Instance UID, which may be used when the ParticipantObjectIDTypeCode is not (110180, DCM, “Study Instance UID”).

A.X.2.1 UserID

If the participant is a person, then the User ID shall be the identifier used for that person on this particular system, in the form of loginName@domain-name.

If the participant is an identifiable process, the UserID selected shall be one of the identifiers used in the internal system logs. For example, the User ID may be the process ID as used within the local operating system in the local system logs. If the participant is a node, then User ID may be the node name assigned by the system administrator. Other participants such as threads, relocatable processes, web service end-points, web server dispatchable threads, etc. will have an appropriate identifier. The implementation shall document in the conformance statement the identifiers used, see A.Y. The purpose of this requirement is to allow matching of the audit log identifiers with internal system logs on the reporting systems. .

When importing or exporting data, e.g. by means of media, the UserID field is used both to identify people and to identify the media itself. When the Role ID Code is EV(110154, DCM, “Destination Media”) or EV(110155, DCM, “Source Media”), the UserID may be:

a. a URI (the preferred form) identifying the source or destination,
b. an email address of the form “mailto:user@address”
c. a description of the media type (e.g. DVD) together with a description of its identifying label, as a free text field,
d. a description of the media type (e.g. paper, film) together with a description of the location of the media creator (i.e., the printer).

The UserID field for Media needs to be highly flexible given the large variety of media and transports that might be used.

A.X.2.2 AlternativeUserID

If the participant is a person, then Alternative User ID shall be the identifier used for that person within an enterprise for authentication purposes, for example, a Kerberos Username (user@realm). If the

participant is a DICOM application, then Alternative User ID shall be one or more of the AE Titles that participated in the event. Multiple AE titles shall be encoded as:

AETITLES=*aetitle1;aetitle2;…*

When importing or exporting data, e.g. by means of media, the Alternative UserID field is used either to identify people or to identify the media itself. When the Role ID Code is (110154, DCM, "Destination Media") or (110155, DCM, "Source Media"), the Alternative UserID may be any machine readable identifications on the media, such as media serial number, volume label, or DICOMDIR SOP Instance UID.

A.X.2.3 UserName

A human readable identification of the participant. If the participant is a person, the person's name shall be used. If the participant is a process, then the process name shall be used.

A.X.2.4 Multi-homed nodes

The NetworkAccessPointTypeCode and NetworkAccessPointID can be ambiguous for systems that have multiple physical network connections. For these multi-homed nodes a single DNS name or IP address shall be selected and used when reporting audit events. DICOM does not require the use of a specific method for selecting the network connection to be used for identification, but it must be the same for all of the audit messages generated for events on that node.

A.X.2.5 EventDateTime

The EventDateTime is the date and time that the event being reported took place. Some events have a significant duration. In these cases, a date and time shall be chosen by a method that is consistent and appropriate for the event being reported.

The EventDateTime shall include the time zone information.

Creators of audit messages may support leap-seconds, but are not required to. Recipients of audit messages shall be able to process messages with leap-second information.

A.X.3 DICOM specific audit messages

The following subsections define message specializations for use by implementations that claim conformance to the DICOM Audit Trail Profile. Any field (i.e., XML element and associated attributes) not specifically mentioned in the following tables shall follow the conventions specified in A.X.1 and A.X.2.

An implementation claiming conformance to this Profile that reports an activity covered by one of the audit messages defined by this Profile shall use the message format defined in this Profile. However, a system claiming conformance to this Profile is not required to send a message each time the activity reported by that audit message occurs. It is expected that the triggering of audit messages would be configurable on an individual basis, to be able to balance network load versus the severity of threats, in accordance with local security policies.

Notes: 1. It is a system design issue outside the scope of DICOM as to what entity actually sends an audit event and when. For example, a Query message could be generated by the entity where the query originated, by the entity that eventually would respond to the query, or by a monitoring entity not directly involved with the query, but that generates audit messages based on monitored network traffic.

2. To report events that are similar to the events described here, these definitions can be used as the basis for extending the schema.

In the subsequent tables, the information entity column indicates the relationship between real world entities and the information elements encoded into the message.

A.X.3.1 Application Activity

This audit message describes the event of an Application Entity starting or stopping. This is closely related to the more general case of any kind of application startup or shutdown, and may be suitable for those purposes also.

Table A.X.3.1 – 1 Application Activity Message

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110100, DCM,"Application Activity")
	EventActionCode	M	Enumerated Value E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	DT (110120, DCM, "Application Start") DT (110121, DCM, "Application Stop")
Active Participant: Application started (1)	UserID	M	The identity of the process started or stopped formatted as specified in A.X.2.1.
	AlternativeUserID	MC	If the process supports DICOM, then the AE Titles as specified in A.X.2.2.
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110150, DCM, "Application")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Persons and or processes that started the Application (0..N)	UserID	M	The person or process starting or stopping the Application
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110151, DCM, "Application Launcher")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

No Participant Objects are needed for this message.

A.X.3.2 Audit Log Used

This message describes the event of a person or process reading a log of audit trail information.

Note: For example, an implementation that maintains a local cache of audit information that has not been transferred to a central collection point might generate this message if its local cache were accessed by a user.

Table A.X.3.2-1 Audit Log Used Message

Real World Entities	Field Name	Opt.	Value Constraints
	EventID	M	EV (110101, DCM, "Audit Log Used")

	EventActionCode	M	Shall be enumerated value: R = read
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: Persons and or processes that started the Application (1..2)	UserID	M	The person or process accessing the audit trail. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: **Identity of the audit log (1)** `	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 13 = security resource
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 12 = URI
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The URI of the audit log
	ParticipantObjectName	U	Shall be: “Security Audit Log”
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See A.X.2
	Accession	U	See A.X.2
	NumberOfInstances	U	See A.X.2
	Instances	U	See A.X.2
	Encrypted	U	See A.X.2
	Anonymized	U	See A.X.2
	ParticipantObjectContainsStudy	U	See A.X.2

A.X.3.3 Begin Transferring DICOM Instances

This message describes the event of a system beginning to transfer a set of DICOM instances from one node to another node within control of the system's security domain. This message may only include information about a single patient.

Note: A separate Instances Transferred message is defined for transfer completion, allowing comparison of what was intended to be sent and what was actually sent.

Table A.X.3.3 – 1 Audit Message for Begin Transferring DICOM Instances

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110102, DCM, "Begin Transferring DICOM Instances")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: **Process Sending the Data (1)**	UserID	M	The identity of the process sending the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **Process receiving the data (1)**	UserID	M	The identity of the process receiving the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Other Participants (0..N)	UserID	M	The identity of any other participants that might be involved and known, especially third parties that are the requestor
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")

	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Element "ContainsSOPClass" with one or more SOP Class UID values
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	not specialized
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: **Patient (1)**	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.X.3.4 Data Export

This message describes the event of exporting data from a system, meaning that the data is leaving control of the system's security domain. Examples of exporting include printing to paper, recording on film, conversion to another format for storage in an EHR, writing to removable media, or sending via e-mail. Multiple patients may be described in one event message.

A single user (either local or remote) shall be identified as the requestor, i.e., UserIsRequestor with a value of TRUE. This accommodates both push and pull transfer models for media.

Table A.X.3.4-1 Audit Message for Data Export

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110106, DCM, "Export")
	EventActionCode	M	Shall be: R = Read
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized

	EventTypeCode	U	not specialized
Participating Object: **Remote Users and Processes (0..n)**	UserID	M	The identity of the remote user or process receiving the data
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.X.3.4.1
	RoleIDCode	M	EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: User or Process Exporting the data(1..2)	UserID	M	The identity of the local user or process exporting the data. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.X.3.4.1
	RoleIDCode	M	EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **Media (1)**	UserID	M	See Section A.X.2.3
	AlternativeUserID	U	See Section A.X.2.4
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110154, DCM, “Destination Media”)
	NetworkAccessPointTypeCode	MC	Required if being exported to other than physical media, e.g. to a network destination rather than to film, paper or CD. May be present otherwise.
	NetworkAccessPointID	MC	Required if Net Access Point Type Code is present. May be present otherwise.
	MediaIdentifier	MC	Volume ID, URI, or other identifier for media. Required if digital media. May be present otherwise.
	MediaType	M	Values selected from DCID (405)
	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, “Study Instance UID”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized

	Anonymized	U	not specialized
Participating Object: **Patients (1..N)**	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.X.3.5 Data Import

This message describes the event of importing data into an organization, implying that the data now entering the system was not under the control of the security domain of this organization. Transfer by media within an organization is often considered a data transfer rather than a data import event. An example of importing is creating new local instances from data on removable media. Multiple patients may be described in one event message.

A single user (either local or remote) shall be identified as the requestor, i.e., UserIsRequestor with a value of TRUE. This accommodates both push and pull transfer models for media.

Table A.X.3.5-1 Audit Message for Data Import

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110107, DCM, “Import”)
	EventActionCode	M	Shall be: C = Create
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Participating Object: **User or Process Importing the data (1..n)**	UserID	M	The identity of the local user or process importing the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.X.3.5
	RoleIDCode	M	EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
	UserID	M	See Section A.X.2.3
	AlternativeUserID	U	See Section A.X.2.4
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE

	RoleIDCode	M	EV (110155, DCM, “Source Media”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.
	MediaIdentifier	M	Volume ID, URI, or other identifier for media
	MediaType	M	Values selected from DCID (405)
Active Participant: Source (0..n)	UserID	M	See Section A.X.2.3
	AlternativeUserID	U	See Section A.X.2.4
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.X.3.5
	RoleIDCode	M	EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present.
Participating Object: Studies (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, “Study Instance UID”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patients (1..N)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

495

A.X.3.6 DICOM Instances Accessed

This message describes the event of DICOM SOP Instances being viewed, utilized, updated, or deleted. This message shall only include information about a single patient and can be used to summarize all activity for several studies for that patient. This message records the studies to which the instances belong, not the individual instances.

If all instances within a study are deleted, then the EV(110105, DCM, "DICOM Study Deleted") event shall be used, see A.X.3.8.

Table A.X.3.6-1 Audit Message for DICOM Instances Accessed

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110103, DCM, "DICOM Instances Accessed")
	EventActionCode	M	Enumerated value: C = create R = read U = update D = delete
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: **Person and or Process manipulating the data** **(1..2)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: **Studies (1..N)**	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized

Participating Object: **Patient (1)**	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.X.3.7 DICOM Instances Transferred

This message describes the event of the completion of transferring DICOM SOP Instances between two Application Entities. This message may only include information about a single patient.

Note: This message may have been preceded by a Begin Transferring Instances message. The Begin Transferring Instances message conveys the intent to store SOP Instances, while the Instances Transferred message records the completion of the transfer. Any disagreement between the two messages might indicate a potential security breach.

Table A.X.3.7-1 Audit Message for DICOM Instances Transferred

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110104, DCM, “DICOM Instances Transferred”)
	EventActionCode	M	Enumerated Value: C = (create) if the receiver did not hold copies of the instances transferred R = (read) if the receiver already holds copies of the SOP Instances transferred, and has determined that no changes are needed to the copies held. U = (update) if the receiver is altering its held copies to reconcile differences between the held copies and the received copies. If the Audit Source is either not the receiver, or otherwise does not know whether or not the instances previously were held by the receiving node, then use “R” = (Read).
	EventDateTime	M	Shall be the time when the transfer has completed
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: **Process that sent the data (1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

Active Participant: **The process that received the data. (1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **Other participants that are known, especially third parties that are the requestor (0..N)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: **Studies being transferred (1..N)**	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, “Study Instance UID”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: **Patient (1)**	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.X.3.8 DICOM Study Deleted

This message describes the event of deletion of one or more studies and all associated SOP Instances in a single action. This message shall only include information about a single patient.

520 **Table A.X.3.8-1 Audit Message for DICOM Study Deleted**

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110105, DCM, “DICOM Study Deleted”)
	EventActionCode	M	Shall be: D = delete
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: **the person or process deleting the study (1..2)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: **Studies being transferred (1..N)**	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, “Study Instance UID”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized

	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.X.3.9 Network Entry

This message describes the event of a system, such as a mobile device, intentionally entering or leaving the network.

Note: The machine should attempt to send this message prior to detaching. If this is not possible, it should retain the message in a local buffer so that it can be sent later. The mobile machine can then capture audit messages in a local buffer while it is outside the secure domain. When it is reconnected to the secure domain, it can send the detach message (if buffered), followed by the buffered messages, followed by a mobile machine message for rejoining the secure domain. The timestamps on these messages is the time that the event was noticed to have occurred, not the time that the message is sent.

Table A.X.3.9-1 Audit Message for Network Entry

Real World Entities	Field Name	Opt.	Value
Event	EventID	M	EV (110108, DCM, "Network Entry")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV (110124, DCM, "Attach") EV (110125, DCM, "Detach")
Active Participant: **Node or System entering or leaving the network (1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

No Participant Objects are needed for this message.

A.X.3.10 Query

This message describes the event of a Query being issued or received. The message does not record the response to the query, but merely records the fact that a query was issued. For example, this would report queries using the DICOM SOP Classes:

a. Modality Worklist
b. General Purpose Worklist
c. Composite Instance Query

Notes: 1. The response to a query may result in one or more Instances Transferred or Instances Accessed messages, depending on what events transpire after the query. If there were security-related failures,

such as access violations, when processing a query, those failures should show up in other audit messages, such as a Security Alert message.
2. Non-DICOM queries may also be captured by this message. The Participant Object ID Type Code, the Participant Object ID, and the Query fields may have values related to such non-DICOM queries.

550 **Table A.X.3.10-1 Audit Message for Query**

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110112, DCM, “Query”)
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: **Process Issuing the Query (1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, “Source Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **The process that will respond to the query (1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, “Destination Role ID”)
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **Other Participants that are known, especially third parties that requested the query (0..N)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	DT (110181, DCM, “SOP Class UID”)
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	If the ParticipantObjectIDTypeCode is (110181, DCM, “SOP Class UID”), then this field shall hold the UID of the SOP Class being queried
	ParticipantObjectName	U	not specialized

	ParticipantObjectQuery	M	If the ParticipantObjectIDTypeCode is (110181, DCM, “SOP Class UID”), then this field shall hold the Dataset of the DICOM query, xs:base64Binary encoded. Otherwise, it shall be the query in the format of the protocol used.
	ParticipantObjectDetail	MC	Required if the ParticipantObjectIDTypeCode is (110181, DCM, “SOP Class UID”) A ParticipantObjectDetail element with the XML attribute ”TransferSyntax” shall be present. The value of the Transfer Syntax attribute shall be the UID of the transfer syntax of the query. The element contents shall be xs:base64Binary encoding. The Transfer Syntax shall be a DICOM Transfer Syntax.
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized

A.X.3.11 Security Alert

This message describes any event for which a node needs to report a security alert, e.g., a node authentication failure when establishing a secure communications channel.

Note: The Node Authentication event can be used to report both successes and failures. If reporting of success is done, this could generate a very large number of audit messages, since every authenticated DICOM association, HL7 transaction, and HTML connection should result in a successful node authentication. It is expected that in most situations only the failures will be reported.

Table A.X.3.11-1 Audit Message for Security Alert

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110113, DCM, ”Security Alert”)
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	Success implies an informative alert. The other failure values imply warning codes that indicate the severity of the alert. A Minor or Serious failure indicates that mitigation efforts were effective in maintaining system security. A Major failure indicates that mitigation efforts may not have been effective, and that the security system may have been compromised.
	EventTypeCode	M	Values selected from DCID(403)

Active Participant: **Reporting Person and/or Process (1..2)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: **Performing Persons or Processes (0..N)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: **Alert Subject (0..N)**	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	U	Defined Terms: 5 = master file 13 = security resource
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Defined Terms: 12 = URI (110182, DCM, “Node ID”) = Node Identifier
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	For a ParticipantObjectIDTypeCode of 12 (URI), then this value shall be the URI of the file or other resource that is the subject of the alert. For a ParticipantObjectIDTypeCode of (110182, DCM, “Node ID”) then the value shall include the identity of the node that is the subject of the alert either in the form of node_name@domain_name or as an IP address. Otherwise, the value shall be an identifier of the type specified by ParticipantObjectIDTypeCode of the subject of the alert.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	M	An element with the Attribute “type” equal to "Alert Description” shall be present with a free text description of the nature of the alert as the value
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See Table A.X.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized

A.X.3.12 User Authentication

This message describes the event that a user has attempted to log on or log off. This report can be made regardless of whether the attempt was successful or not. No Participant Objects are needed for this message.

Note: The user usually has UserIsRequestor TRUE, but in the case of a logout timer, the Node might be the UserIsRequestor.

Table A.X.3.12-1 Audit Message for User Authentication

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM, "User Authentication")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	Defined Terms: EV (110122, DCM, "Login") EV (110123, DCM, "Logout")
Active Participant: **Person Authenticated or claimed** **(1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	M	not specialized
	NetworkAccessPointID	M	not specialized
Active Participant: **Node or System performing authentication (0..1)**	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

A.Y AUDIT TRAIL MESSAGE TRANSMISSION PROFILE – SYSLOG-TLS

This profile defines the transmission of audit trail messages. Transport Layer Security (TLS) Transport Mapping for Syslog (RFC 5425) provides the mechanisms for reliable transport, buffering, acknowledgement, authentication, identification, and encryption. The RFC5424 states that the TLS used MUST be TLS version 1.2. For this DICOM profile TLS MUST be used, and version 1.2 or later is RECOMMENDED.

Note: The words MUST and RECOMMENDED are used in accordance with the IETF specification for normative requirements.

Any implementation that claims conformance to this profile shall also conform to the Audit Trail Message Format Profile. XML audit trail messages created using the format defined in Audit Trail Message Format Profile shall be transmitted to a collection point using the syslog over TLS mechanism, defined in RFC 5425. Systems that comply with this profile shall support message sizes of at least 32768 octets.

Notes: 1. Audit messages for other purposes may also be transferred on the same syslog connection. These messages might not conform to the Audit Trail Message Format.

2. RFC 5425 specifies mandatory support for 2KB messages, strongly recommends support for at least 8KB, and does not restrict the maximum size.

3. When a received message is longer than the receiving application supports, the message might be discarded or truncated. The sending application will not be notified.

The XML audit trail message shall be inserted into the MSG portion of the SYSLOG-MSG element of the syslog message as defined in RFC 5424 “The Syslog Protocol”. The XML audit message may contain Unicode characters that are encoded using the UTF-8 encoding rules.

Note: UTF-8 avoids utilizing the control characters that are reserved by the syslog protocol, but a system that is not prepared for UTF-8 may not be able to display these messages correctly.

The PRI field shall be set using the facility value of 10 (security/authorization messages). Most messages should have the severity value of 5 (normal but significant), although applications may choose other values if that is appropriate to the more detailed information in the audit message. This means that for most audit messages the PRI field will contain the value “<85>”.

The MSGID field in the HEADER of the SYSLOG-MSG shall be set. The value “DICOM+RFC3881” may be used for messages that comply with this profile.

The MSG field of the SYSLOG-MSG shall be present and shall be an XML structure following the RFC 3881 format, as extended in the audit trail message format profile.

The syslog message shall be created and transmitted as described in RFC 5424.

Any implementation that claims conformance to this Security Profile shall describe in its conformance statement:

a. any configuration parameters relevant to RFC 5424 and RFC 5425.
b. Any STRUCTURED-DATA that is generated or processed.
c. Any implementation schema or message element extensions for the audit messages.
d. The maximum size of messages that can be sent or received.

A.Z AUDIT TRAIL MESSAGE TRANSMISSION PROFILE – SYSLOG-UDP

This profile defines the transmission of audit trail messages. Transmission of Syslog Messages over UDP (RFC5426) provides the mechanisms for rapid transport of audit messages. It is the standardized successor to the informative standard “The BSD syslog protocol (RFC3164)”, which is widely used in a variety of settings.

The syslog port number shall be configurable, with the port number (514) as the default.

The underlying UDP transport might not accept messages longer than the MTU size minus the UDP header length. This may result in longer syslog messages being truncated. When these messages are truncated the resulting XML may be incorrect. Because of this potential for truncated messages and other security concerns, the transmission of syslog messages over TLS may be preferred (see section A.Y).

The PRI field shall be set using the facility value of 10 (security/authorization messages). Most messages should have the severity value of 5 (normal but significant), although applications may choose values of 4 (warning condition) if that is appropriate to the more detailed information in the audit message. This means that for most audit messages the PRI field will contain the value "<85>". Audit repositories shall be prepared to deal appropriately with any incoming PRI value.

The MSGID field in the HEADER of the SYSLOG-MSG shall be set. The value "DICOM+RFC3881" may be used for messages that comply with this profile.

The MSG field of the SYSLOG-MSG shall be present and shall be an XML structure following the RFC 3881 format, as extended in this profile.

The syslog message shall be created and transmitted as described in RFC 5424.

Any implementation that claims conformance to this Security Profile shall describe in its conformance statement:

a. any configuration parameters relevant to RFC 5424 and RFC 5426.
b. Any STRUCTURED-DATA that is generated or processed.
c. Any implementation schema or message element extensions for the audit messages.
d. The maximum size of messages that can be sent or received.

6 Additions to PS 3.16

Add the following Defined Context Groups to PS 3.16

CID 400 Audit Event ID

Context ID 400
Audit Event ID
Type: Extensible Version: 20100826

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110100	Application Activity
DCM	110101	Audit Log Used
DCM	110102	Begin Transferring DICOM Instances
DCM	110103	DICOM Instances Accessed

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110104	DICOM Instances Transferred
DCM	110105	DICOM Study Deleted
DCM	110106	Export
DCM	110107	Import
DCM	110108	Network Entry
DCM	110112	Query
DCM	110113	Security Alert
DCM	110114	User Authentication

655 **CID 401 Audit Event Type Code**

Context ID 401
Audit Event Type Code
Type: Extensible Version: 20100826

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110120	Application Start
DCM	110121	Application Stop
DCM	110122	Login
DCM	110123	Logout
DCM	110124	Attach
DCM	110125	Detach
DCM	110126	Node Authentication
DCM	110127	Emergency Override Started
DCM	110128	Network Configuration
DCM	110129	Security Configuration
DCM	110130	Hardware Configuration
DCM	110131	Software Configuration
DCM	110132	Use of Restricted Function
DCM	110133	Audit Recording Stopped
DCM	110134	Audit Recording Started
DCM	110135	Object Security Attributes Changed
DCM	110136	Security Roles Changed

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110137	User Security Attributes Changed

CID 402 Audit Active Participant Role ID Code

Context ID 402
Audit Active Participant Role ID Code
Type: Extensible Version: 20100826

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110150	Application
DCM	110151	Application Launcher
DCM	110152	Destination Role ID
DCM	110153	Source Role ID
DCM	110154	Destination Media
DCM	110155	Source Media

CID 403 Security Alert Type Code

Context ID 403
Security Alert Type Code
Type: Extensible Version: 20100826

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110126	Node Authentication
DCM	110127	Emergency Override Started
DCM	110128	Network Configuration
DCM	110129	Security Configuration
DCM	110130	Hardware Configuration
DCM	110131	Software Configuration
DCM	110132	Use of Restricted Function
DCM	110133	Audit Recording Stopped

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110134	Audit Recording Started
DCM	110135	Object Security Attributes Changed
DCM	110136	Security Roles Changed
DCM	110137	User Security Attributes Changed
DCM	110138	Emergency Override Stopped
DCM	110139	Remote Service Operation Started
DCM	110140	Remote Service Operation Stopped
DCM	110141	Local Service Operation Started
DCM	110142	Local Service Operation Stopped

CID 404 Audit Participant Object ID Type Code

675 **Context ID 404**
Audit Participant Object ID Type Code
Type: Extensible Version: 20100621

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110180	Study Instance UID
DCM	110181	SOP Class UID
DCM	110182	Node ID

CID 405 Media Type Code

Context ID 405
Media Type Code
Type: Extensible Version: 20100824

Coding Scheme Designator (0008,0102)	Code Value (0008,0100)	Code Meaning (0008,0104)
DCM	110030	USB Disk Emulation
DCM	110031	Email
DCM	110032	CD
DCM	110033	DVD
DCM	110034	Compact Flash
DCM	110035	Multi-media Card
DCM	110036	Secure Digital Card
DCM	110037	URI
DCM	110010	Film
DCM	110038	Paper Document

Add the following Code Definitions to PS 3.16 Annex D

DICOM Code Definitions (Coding Scheme Designator "DCM" Coding Scheme Version "yy")

Code Value	Code Meaning	Definition	Notes
110100	Application Activity	Audit event: Application Activity has taken place	
110101	Audit Log Used	Audit event: Audit Log has been used	
110102	Begin Transferring DICOM Instances	Audit event: Storage of DICOM Instances has begun	
110103	DICOM Instances Accessed	Audit event: DICOM Instances have been created, read, updated, or deleted -audit event	
110104	DICOM Instances Transferred	Audit event: Storage of DICOM Instances has been completed	
110105	DICOM Study Deleted	Audit event: Entire Study has been deleted	
110106	Export	Audit event: Data has been exported out of the system	

110107	Import	Audit event: Data has been imported into the system	
110108	Network Entry	Audit event: System has joined or left network	
110109	Order Record	Audit event: Order has been created, read, updated or deleted	
110110	Patient Record	Audit event: Patient Record has been created, read, updated, or deleted	
110111	Procedure Record	Audit event: Procedure Record has been created, read, updated, or deleted	
110112	Query	Audit event: Query has been made	
110113	Security Alert	Audit event: Security Alert has been raised	
110114	User Authentication	Audit event: User Authentication has been attempted	
110120	Application Start	Audit event: Application Entity has started	
110121	Application Stop	Audit event: Application Entity has stopped	
110122	Login	Audit event: User login has been attempted	
110123	Logout	Audit event: User logout has been attempted	
110124	Attach	Audit event: Node has been attached	
110125	Detach	Audit event: Node has been detached	
110126	Node Authentication	Audit event: Node Authentication has been attempted	
110127	Emergency Override Started	Audit event: Emergency Override has started	
110128	Network Configuration	Audit event: Network configuration has been changed	
110129	Security Configuration	Audit event: Security configuration has been changed	
110130	Hardware Configuration	Audit event: Hardware configuration has been changed	
110131	Software Configuration	Audit event: Software configuration has been changed	
110132	Use of Restricted Function	Audit event: A use of a restricted function has been attempted	

110133	Audit Recording Stopped	Audit event: Audit recording has been stopped	
110134	Audit Recording Started	Audit event: Audit recording has been started	
110135	Object Security Attributes Changed	Audit event: Security attributes of an object have been changed	
110136	Security Roles Changed	Audit event: Security roles have been changed	
110137	User security Attributes Changed	Audit event: Security attributes of a user have been changed	
110150	Application	Audit participant role ID of software application	
110151	Application Launcher	Audit participant role ID of software application launcher, i.e., the entity that started or stopped an application.	
110152	Destination Role ID	Audit participant role ID of the receiver of data	
110153	Source Role ID	Audit participant role ID of the sender of data	
110154	Destination Media	Audit participant role ID of media receiving data during an export.	
110155	Source Media	Audit participant role ID of media providing data during an import.	
110180	Study Instance UID	ParticipantObjectID type: Study Instance UID	
110181	SOP Class UID	ParticipantObjectID type: SOP Class UID	
110182	Node ID	ID of a node that is a participant object of an audit message	
110138	Emergency Override Stopped	Audit event: Emergency Override has Stopped	
110139	Remote Service Operation Started	Audit event: Remote Service Operation has Begun	
110140	Remote Service Operation Stopped	Audit event: Remote Service Operation has Stopped	
110141	Local Service Operation Started	Audit event: Local Service Operation has Begun	
110142	Local Service Operation Stopped	Audit event: Local Service Operation Stopped	

110030	USB Disk Emulation	A device that connects using the USB hard drive interface. These may be USB-Sticks, portable hard drives, and other technologies.	
110031	Email	Email and email attachments used as a media for data transport.	
110032	CD	CD-R, CD-ROM, and CD-RW media used for data transport.	
110033	DVD	DVD, DVD-RAM, and other DVD formatted media used for data transport.	
110034	Compact Flash	Media that comply with the Compact Flash standard.	
110035	Multi-media Card	Media that comply with the Multi-media Card standard.	
110036	Secure Digital Card	Media that comply with the Secure Digital Card standard.	
110037	URI	URI Identifier for network or other resource, see RFC 3968	
110038	Paper Document	Any paper or similar document.	

7 Additions to 3.17

Add the following informative annex to 3.17

Annex Y Audit Messages (Informative)

This annex holds examples of audit messaging, as described by the Audit Trail Message Format Secure Use Profile in PS 3.15.

Y.1 MESSAGE EXAMPLE

An example of one of the DICOM Instances Transferred messages is shown in Figure Y.1-1

```
<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:noNamespaceSchemaLocation="D:\data\DICOM\security\audit-message.rnc">
  <EventIdentification EventActionCode="C" EventDateTime="2001-12-17T09:30:47"
EventOutcomeIndicator="0">
    <EventID code="110104" codeSystemName="DCM" displayName="DICOM Instances Transferred" />
  </EventIdentification>
  <ActiveParticipant UserID="123" AlternativeUserID="AETITLE=AEFOO" UserIsRequestor="false"
                     NetworkAccessPointID="192.168.1.2" NetworkAccessPointTypeCode="2">
```

```
    <RoleIDCode code="110153" codeSystemName="DCM" displayName=" Source Role ID "/>
  </ActiveParticipant>
  <ActiveParticipant UserID="67562" AlternativeUserID="AETITLE=AEPACS" UserIsRequestor="false"
                   NetworkAccessPointID="192.168.1.5" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="110152" codeSystemName="DCM" displayName=" Destination Role ID "/>
  </ActiveParticipant>
  <ActiveParticipant UserID="smitty@readingroom.hospital.org"
                   AlternativeUserID="smith@nema" UserName="Dr. Smith"
                   UserIsRequestor="true" NetworkAccessPointID="192.168.1.2"
NetworkAccessPointTypeCode="2">
    <RoleIDCode code="110153" codeSystemName="DCM" displayName=" Source Role ID "/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditEnterpriseSiteID="Hospital" AuditSourceID="ReadingRoom">
    <AuditSourceTypeCode code="1"/>
  </AuditSourceIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="1.2.840.10008.2.3.4.5.6.7.78.8"
                                   ParticipantObjectTypeCode="2" ParticipantObjectTypeCodeRole="3"
                                   ParticipantObjectDataLifeCycle="1">
    <ParticipantObjectIDTypeCode code="110180" codeSystemName="DCM" displayName="Study Instance
UID"/>
    <ParticipantObjectDescription>
      <MPPS UID="1.2.840.10008.1.2.3.4.5"/>
      <Accession Number="12341234" />
      <SOPClass UID="1.2.840.10008.5.1.4.1.1.2" NumberOfInstances="1500"/>
      <SOPClass UID="1.2.840.10008.5.1.4.1.1.11.1" NumberOfInstances="3"/>
    </ParticipantObjectDescription>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="ptid12345" ParticipantObjectTypeCode="1"
ParticipantObjectTypeCodeRole="1">
    <ParticipantObjectIDTypeCode code="2" />
    <ParticipantObjectName>John Doe</ParticipantObjectName>
  </ParticipantObjectIdentification>
</AuditMessage>
```

Figure Y.1-1 Sample Audit Event Report

The message describes a study transfer initiated at the request of Dr. Smith on the system at the IP address 192.168.1.2 to a system at IP address 192.168.1.5. The study contains 1500 CT SOP Instances and 3 GSPS SOP Instances. The audit report came from the audit source “ReadingRoom”.

Y.2 WORKFLOW EXAMPLE

The following is an example of audit trail message use in a hypothetical workflow. It is not intended to be all-inclusive, nor does it cover all possible scenarios for audit trail message use. There are many alternatives which can be utilized by the system designer, or that could be configured by the local site security administrator to fit security policies.

As this example scenario begins, an imaging workstation boots up. During its startup process, a DICOM-enabled viewing application is launched by the startup sequence. This triggers an Application Activity message with the Event Type Code of (110120, DCM, “Application Start”).

After startup, a curious, but unauthorized visitor attempts to utilize the reviewing application. Since the reviewing application cannot verify the identity of this visitor, the attempt fails, and the reviewing application generates a User Authentication message, recording the fact that this visitor attempted to enter the application, but failed.

Later, an authorized user accesses the reviewing application. Upon successfully identifying the user, the reviewing application generates a User Authentication message indicating a successful login to the application.

The user, in order to locate the data of a particular examination, issues a query, which the reviewing application directs to a DICOM archive. The details of this query are recorded by the archive application in a Query message.

The reviewing application, in delivering the results of the query to the user, displays certain patient related information. The reviewing application records this fact by sending a Patient Record message that is defined by some other standard. Audit logs will contain messages specified by a variety of different standards. The MSG-ID field is used to aid the recognition of the defining standard or proprietary source documentation for a particular message.

From the query results, the user selects a set of images to review. The reviewing application requests the images from the archive, and records this fact in a Begin Transferring Instances message.

The archive application locates the images, sends them back to the reviewing application, and records this fact in an Instances Transferred message.

The reviewing application displays the images to the user, recording this fact via an Instances Accessed message.

During the reviewing process, the use looks up details of the procedure from the hospital information system. The reviewing application performs this lookup using HL7 messaging, and records this fact in a Procedure Record message.

The user decides that a follow-up examination is needed, and generates a new order via HL7 messaging to the hospital information system. The reviewing application records this in an Order Record message.

The user decides that a second opinion is desirable, and selects certain images to send to a colleague in an e-mail message. The reviewing application records the fact that it packaged and sent images via e-mail in an Export message.