

DICOM Change Proposal

STATUS	Letter Ballot
Date of Last Update	2025-09-03
Person Assigned	Rob Horn
Submitter Name	Jörg Riesmeier <dicom@jriesmeier.com>
Submission Date	2025-03-20

Change Number	CP-2530
Log Summary: Fix various inconsistencies in the Audit Trail Message Format Profile	
Name of Standard PS3.15	
<p>Rationale for Change:</p> <p>The section on “Audit Trail Message Format Profile” in PS3.15 is rather inconsistent regarding the use of terms and their spelling. It is, therefore, proposed to harmonize this throughout Section A.5. For example, according to Table A.5.2-1, the name of the entity is “ParticipantObject” and not “ParticipatingObject”. The name of the associated “Real-World Entity” is sometimes also missing. Furthermore, the values “true” and “false” should be written consistently throughout this section when referring to the Boolean values used for XML attributes. It is proposed to follow the spelling that is used for the definition of the underlying XML datatype definition (xsd:boolean), i.e., lower case, and use quotation marks around them.</p> <p>Unfortunately, there is also an inconsistency regarding a field name (“Instance” vs. “Instances”), which might result in non-backward compatible changes. The Audit Message Schema and the General Message Format are consistent, but the DICOM Specific Audit Messages are not.</p> <p>Note: Yellow color is used to highlight certain parts of the following text in order to make it easier for the reader of this CP to find relevant information. This formatting should be removed for the “Final Text”.</p> <p>[Editorial instruction: change all enumerated values and defined terms to use correct DocBook construct to bold correctly.]</p>	
Change Wording:	

Modify PS3.15 Section 3.11 as indicated

5 **3.11 DICOM Data Structures and Encoding**

This Part of the Standard makes use of the following terms defined in [PS3.5](#):

Data Set [See Data Set in PS3.5.](#)

Defined Term [See Defined Term in PS3.5.](#)

Enumerated Value [See Enumerated Value in PS3.5.](#)

10

Modify PS3.15 Section A.5 as indicated

(changes to existing text are bold and underlined for additions and bold and struckthrough for removals):

A.5 Audit Trail Message Format Profile

15 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.

20 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:

- 25 a. format audit trail messages in accordance with the XML schema specified in Section A.5.1 in a fashion that allows those messages to be validated against that XML schema, following the general conventions specified in Section A.5.2.
- b. for the events described in this Profile comply with the restrictions specified by this Profile in Section A.5.3, and describe in its conformance statement any extensions.

Note

30 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

35 Other profiles specify the transmission of audit messages.

A.5.1 DICOM Audit Message Schema

40 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], 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.5.2.

This schema is provided in Relax NG Compact format.

Note

45 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.

A.5.1.1 Audit Message Schema

The following is the content of the audit message schema:

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

50 # 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 =
55     (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 }?,
60     attribute originalText { token }           # Note: this also corresponds to DICOM
"Code Meaning"
```

```

CodedValueType =
    attribute csd-code { token },
    other-csd-attributes
65
# Define the event identification, used later

EventIdentificationContents =
    element EventID { CodedValueType },
70    element EventTypeCode { CodedValueType }*, # Note: DICOM/IHE defines and uses this
                                                # differently than RFC-3881
    attribute EventActionCode {                # Optional action code
        "C" |                                ## Create
        "R" |                                ## Read
75        "U" |                                ## Update
        "D" |                                ## Delete
        "E" |                                ## Execute
    }?,

80    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)
85        "12" |                               ## Major failure, (reporting application now unavailable)
    },

    element EventOutcomeDescription { text }?

90 # Define AuditSourceIdentification, used later

AuditSourceIdentificationContents =
    attribute AuditEnterpriseSiteID { token }?,
    attribute AuditSourceID { token },
95    element AuditSourceTypeCode { AuditSourceTypeCodeContent }*

# Define AuditSourceTypeCodeContent so that an isolated single digit
# value is acceptable, or a token with other csd attributes so that
# any controlled terminology can also be used.
100
AuditSourceTypeCodeContent =
    attribute csd-code {
        "1" |                                ## End-user display device, diagnostic device
        "2" |                                ## Data acquisition device or instrument
105        "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
110        "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

115 # Define ActiveParticipantType, used later

ActiveParticipantContents =
    element RoleIDCode { CodedValueType }*,
    element MediaIdentifier {
120        element MediaType { CodedValueType }
    }?,
    attribute UserID { text },
    attribute AlternativeUserID { text }?,
    attribute UserName { text }?,
125    attribute UserIsRequestor { xsd:boolean },
    attribute NetworkAccessPointID { token }?,
    attribute NetworkAccessPointTypeCode {
        "1" |                                ## Machine Name, including DNS name
        "2" |                                ## IP Address
    }

```

```

130     "3" |          ## Telephone Number
        "4" |          ## Email address
        "5" }?       ## URI (user directory, HTTP-PUT, ftp, etc.)

# The BinaryValuePair is used in ParticipantObject descriptions to capture parameters.
135 # 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,
140 # so security logs can be expected to need to capture them without modification by the
# audit encoding process.

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

# Define ParticipantObjectIdentification, used later
150 # Participant Object Description, used later

DICOMObjectDescriptionContents =
    element MPPS {
155         attribute UID { token }          # OID pattern="[0-2](\\.(0)|\\.[1-9][0-9]*)*"
    },
    element Accession {
        attribute Number { token }
    },
160     element SOPClass {                  # SOP eclass for one sstudy
        element Instance {
            attribute UID { token }          # OID pattern="[0-2](\\.(0)|\\.[1-9][0-9]*)*"
        },
165         attribute UID { token }?,        # OID pattern="[0-2](\\.(0)|\\.[1-9][0-9]*)*"
        attribute NumberOfInstances { xsd:integer }
    },
    element ParticipantObjectContainsStudy {
        element StudyIDs {
            attribute UID { token }
170         },
    },
    },
    element Encrypted { xsd:boolean }?,
    element Anonymized { xsd:boolean }?

175 ParticipantObjectIdentificationContents =
    element ParticipantObjectIDTypeCode { CodedValueType },
    (element ParticipantObjectName { token } |
        element ParticipantObjectQuery { xsd:base64Binary }), # either a name or
    element ParticipantObjectDetail { ValuePair }*, # a query ID field,
180     extensive # optional details, these can be
                                     # and large
    element ParticipantObjectDescription { DICOMObjectDescriptionContents }*,
    attribute ParticipantObjectID { token }, # mandatory ID
    attribute ParticipantObjectTypeCode { # optional type
185         "1" | ## Person
        "2" | ## System object
        "3" | ## Organization
        "4" | ## Other
    },
190     attribute ParticipantObjectTypeCodeRole { ## optional role
        "1" | ## Patient
        "2" | ## Location
        "3" | ## Report
195         "4" | ## Resource
        "5" | ## Master File
        "6" | ## User

```

```

200     "7" |      ## List
        "8" |      ## Doctor
        "9" |      ## Subscriber
        "10" |     ## Guarantor
        "11" |     ## Security User Entity
        "12" |     ## Security User Group
        "13" |     ## Security Resource
205     "14" |     ## Security Granularity Definition
        "15" |     ## Provider
        "16" |     ## Data Destination
        "17" |     ## Data Archive
        "18" |     ## Schedule
210     "19" |     ## Customer
        "20" |     ## Job
        "21" |     ## Job Stream
        "22" |     ## Table
        "23" |     ## Routing Criteria
215     "24" |     ## Query
        "25" |     ## Data Source
        "26" |     ## Processing Element
    }?,

220     attribute ParticipantObjectDataLifeCycle {          # optional life cycle stage
        "1" |      ## Origination, Creation
        "2" |      ## Import/ Copy
        "3" |      ## Amendment
        "4" |      ## Verification
225     "5" |      ## Translation
        "6" |      ## Access/Use
        "7" |      ## De-identification
        "8" |      ## Aggregation, summarization, derivation
        "9" |      ## Report
230     "10" |     ## Export
        "11" |     ## Disclosure
        "12" |     ## Receipt of Disclosure
        "13" |     ## Archiving
        "14" |     ## Logical deletion
235     "15" }?,     ## Permanent erasure, physical destruction

        attribute ParticipantObjectSensitivity { token }?

# The basic message
240 message =
    element AuditMessage {
        (element EventIdentification { EventIdentificationContents }, # The event must be
identified
        element ActiveParticipant { ActiveParticipantContents }+, # It has one or more
245 active
                                # participants
        element AuditSourceIdentification {                # It is reported by one
source
            AuditSourceIdentificationContents
250         },
        element ParticipantObjectIdentification {          # It may have other
objects involved
            ParticipantObjectIdentificationContents
        }*)
255     }

# And finally the magic statement that message is the root of everything.
start = message
260

```

A.5.1.2 Codes Used Within The Schema

The following value sets are defined in the audit **message** schema above. These are not coded terminology. They are values whose meaning depends upon their use at the proper location within the message.

A.5.1.2.1 Audit Source Type Code

265 The Audit Source Type Code values specify the type of source where an event originated. Codes from coded terminologies and implementation defined codes can also be used for the AuditSourceTypeCode.

Table A.5.1.2.1-1. Audit Source Type Code Values

Value	Meaning
1	End-user interface
2	Data acquisition device or instrument
3	Web server process tier in a multi-tier system
4	Application server process tier in a multi-tier system
5	Database server process tier in a multi-tier system
6	Security server, e.g., a domain controller
7	ISO level 1-3 network component
8	ISO level 4-6 operating software
9	External source, other or unknown type

A.5.1.2.2 Participant Object Type Code Role

270 The Participant Object Type Code Role is an attribute of the ParticipantObjectIdentification, and is not extensible. This attribute may be omitted or one of the following values assigned. Coded terminologies are not supported.

Table

Table A.5.1.2.2-1. Participant Object Type Code Role Values

Value	Meaning	Likely associated Participant Object Type Code
1	Patient	1 - Person
2	Location	3 - Organization
3	Report	2 - System Object
4	Resource	1 - Person, or 3 - Organization
5	Master File	2 - System Object
6	User	1 - Person, or 2 - System Object
7	List	2 - System Object
8	Doctor	1 - Person
9	Subscriber	3 - Organization

Value	Meaning	Likely associated Participant Object Type Code
10	Guarantor	1 - Person, or 3 - Organization
11	Security User Entity	1 - Person, or 2 - System Object
12	Security User Group	2 - System Object
13	Security Resource	2 - System Object
14	Security Granularity Definition	2 - System Object
15	Provider	1 - Person, or 3 - Organization
16	Data Destination	2 - System Object
17	Data Repository	2 - System Object
18	Schedule	2 - System Object
19	Customer	3 - Organization
20	Job	2 - System Object
21	Job Stream	2 - System Object
22	Table	2 - System Object
23	Routing Criteria	2 - System Object
24	Query	2 - System Object
25	Data Source	2 - System Object
26	Processing Element	2 - System Object

275 A.5.1.2.3 Participant Object Data Life Cycle

The Participant Object Data Life Cycle is an attribute of the ParticipantObjectIdentification, and is not extensible. This attribute may be omitted or one of the following values assigned. Coded terminologies are not supported.

Table A.5.1.2.3-1. Participant Object Data Life Cycle Values

Value	Meaning
1	Origination or Creation
2	Import or Copy from original
3	Amendment
4	Verification

Value	Meaning
5	Translation
6	Access or Use
7	De-identification
8	Aggregation, summarization, derivation
9	Report
10	Export or Copy to target
11	Disclosure
12	Receipt of Disclosure
13	Archiving
14	Logical Deletion
15	Permanent erasure or physical destruction

280 A.5.1.2.4 Participant Object ID Type Code

The Participant Object ID Type Code describes the identifier that is contained in Participant-Object-ID. Codes from coded terminologies and implementation defined codes can also be used for the ParticipantObjectTypeCodeRole.

Table A.5.1.2.4-1. Participant Object ID Type Code Values

Value	Meaning	Likely associated Participant Object Type Code
1	Medical Record Number	1 - Person
2	Patient Number	1 - Person
3	Encounter Number	1 - Person
4	Enrollee Number	1 - Person
5	Social Security Number	1 - Person
6	Account Number	1 - Person, or 3 - Organization
7	Guarantor Number	1 - Person, or 3 - Organization
8	Report Name	2 - System Object
9	Report Number	2 - System Object
10	Search Criteria	2 - System Object
11	User Identifier	1 - Person, or

Value	Meaning	Likely associated Participant Object Type Code
		2 - System Object
12	URI	2 - System Object

A.5.1.2.5 Network Access Point Type Code

The Network Access Point Type Code describes the identifier that is contained in NetworkAccessPointID, and is not extensible. Coded terminologies are not supported.

Table A.5.1.2.5-1. Network Access Point Type Code Values

Value	Meaning
<u>1</u>	<u>Machine Name, including DNS name</u>
<u>2</u>	<u>IP Address</u>
<u>3</u>	<u>Telephone Number</u>
<u>4</u>	<u>Email address</u>
<u>5</u>	<u>URI (user directory, HTTP PUT, ftp, etc.)</u>

A.5.2 General Message Format Conventions

The following table lists the primary fields from the **DICOM Audit Message Schema** specified in **Section A.5.1**, with additional instructions, conventions, and restrictions on how DICOM applications shall fill in the field values. The field names are leaf elements and attributes that are in the **DICOM Audit Message Schema** (see **Section A.5.1**). Note that these fields may be enclosed in other XML elements, as specified by the schema.

Note

This schema, codes, and content were originally derived from [RFC 3881]. [RFC 3881] is not being maintained or updated by the IETF, and has gradually diverged from the DICOM schema and codes. Other documents exist that refer to [RFC 3881] as the underlying standard. [RFC 3881] does not include corrections and additions to the audit **message** schema made in DICOM since 2004.

Although XML permits empty elements and attributes with a value of the empty string, Audit Messages shall not contain empty elements and shall not contain attributes with a value of the empty string.

In subsequent tables the following notation is used for optionality:

M This element or attribute is mandatory.

U This element or attribute is user optional. The creator may include it or omit it.

MC This element or attribute is mandatory if a specified condition is true.

UC This element or attribute may be present only if a specified condition is true, if the user chooses to include it.

Table A.5.2-1. General Message Format

	Field Name	Opt.	Description	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". DCID 400 "Audit Event ID"

	Field Name	Opt.	Description	Additional Conditions on Field Format/Value
	EventActionCode	U	Indicator for type of action performed during the event that generated the audit.	C Create a new database object, such as Placing an Order R Read/View/Print/Query Display or print data, such as a Doctor Census U Update data, such as Revise Patient Information D Delete items, such as a master file record E Execute a system or application function such as log-on, program execution, or use of an object's method
	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.5.2.5.
	EventOutcomeIndicator	M	Indicates whether the event succeeded or failed.	0 Success 4 Minor failure; action restarted, e.g., invalid password with first retry 8 Serious failure; action terminated, e.g., invalid password with excess retries 12 Major failure; action made unavailable, e.g., user account disabled due to excessive invalid log-on attempts 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". DCID 401 "Audit Event Type Code"
Active Participant (multi-valued)	UserID	M	Unique identifier for the user actively participating in the event.	See Section A.5.2.1.
	AlternativeUserID	U	Alternative unique identifier for the user.	See Section A.5.2.2.
	UserName	U	The human-meaningful name for the user.	See Section A.5.2.3.
	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 "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	DCID 402 "Audit Active Participant Role ID Code"

	Field Name	Opt.	Description	Additional Conditions on Field Format/Value
			role-based access control security.	Note 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 5.1.2.5 for codes and Section A.5.2.4 for further details.
	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.	See Section A.5.1.2.1. 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.	1 Person 2 System Object 3 Organization 4 Other
	ParticipantObjectTypeCodeRole	U	Code representing the functional application role of Participant Object being audited.	See Section A.5.1.2.2.
	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.	See Section A.5.1.2.3.

	Field Name	Opt.	Description	Additional Conditions on Field Format/Value
	ParticipantObjectIDTypeCode	M	Describes the identifier that is contained in Participant-Object-ID.	See Section A.5.1.2.4 and CID 404 "Audit Participant Object ID Type Code". Note Usage of this field is refined in the individual message descriptions below. Multiple roles may also be present, since this is a multi-valued field.
	ParticipantObjectSensitivity	U	Denotes policy-defined sensitivity for the Participant-Object-ID such as VIP, HIV status, mental health status, or similar topics.	Locally defined terms.
	ParticipantObjectID	M	Identifies a specific instance of the pP Participant eO Object.	Usage refined by individual message descriptions.
	ParticipantObjectName	MC	An instance-specific descriptor of the Participant-Object-ID audited, such as a person's name.	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	The actual query for a query-type participant object.	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	Implementation-defined data about specific details of the object accessed or used.	This element is a T type-value pair. The "type" attribute is an implementation-defined text string. The "value" attribute is base 64 encoded data. The value is suitable for conveying binary data.
	SOPClass	MC		The UIDs of SOP eC lasses referred to in this pP Participant eO Object. Required if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") and any of the optional fields (Accession Number , Contains MPPS, NumberOfInstances, Contains SOPInstances, 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		An Accession Number(s) associated with this pP Participant eO Object.
	MPPS	U		An MPPS Instance UID(s) associated with this pP Participant eO Object.
	NumberOfInstances	U		The number of SOP Instances referred to by this pP Participant eO Object.
	Instance	U		SOP Instance UID value(s)

	Field Name	Opt.	Description	Additional Conditions on Field Format/Value
				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		A single value of T “true” or F “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		A single value of T “true” or F “false” indicating whether or not all patient identifying information was removed from the data.
	ParticipantObjectContainsStudy	U		A Study Instance UID, which that may be used when the ParticipantObjectIDTypeCode is not (110180, DCM, "Study Instance UID").

310 A.5.2.1 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.

315 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 **e**Conformance **s**tatement the identifiers used, ~~see Section A.6~~. The purpose of this requirement is to allow matching of the audit log identifiers with internal system logs on the reporting systems.

320 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".
- 325 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 **M**media needs to be highly flexible given the large variety of media and transports that might be used.

330 A.5.2.2 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:

335 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~~ File-set ID (0004,1130).

A.5.2.3 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.5.2.4 NetworkAccessPointTypeCode, NetworkAccessPointID

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.5.2.5 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.5.2.6 ParticipantObjectTypeCodeRole

The ParticipantObjectTypeCodeRole identifies the role that the object played in the event that is being reported. Most events involve multiple participating objects. ParticipantObjectTypeCodeRole identifies which object took which role in the event. It also covers agents, multi-purpose entities, and multi-role entities. For the purpose of the event one primary role is chosen.

Table A.5.2.6-1. Participant_Object_Type_Code_Role Values

Code	Short Description	Description
1	Patient	This object is the patient that is the subject of care related to this event. It is identifiable by patient ID or equivalent. The patient may be either human or animal.
2	Location	This is a location identified as related to the event. This is usually the location where the event took place. Note that for shipping, the usual events are arrival at a location or departure from a location.
3	Report	This object is any kind of persistent document created as a result of the event. This could be a paper report, film, electronic report, DICOM Study, etc. Issues related to medical records life cycle management are conveyed elsewhere.
4	Resource	(deprecated)
5	Master File	This is any configurable file used to control creation of documents or behavior. Examples include the objects maintained by the HL7 Master File transactions, Value Sets, etc.
6	User	A human participant not otherwise identified by some other category.
7	List	(deprecated)
8	Doctor	A person who is providing or performing care related to the event, generally a physician. The key distinction between doctor and provider is the nature of their participation. The

Code	Short Description	Description
		doctor is the human who actually performed the work. The provider is the human or organization that is responsible for the work.
9	Subscriber	A person or system that is being notified as part of the event. This is relevant in situations where automated systems provide notifications to other parties when an event took place.
10	Guarantor	Insurance company, or any other organization who accepts responsibility for paying for the healthcare event.
11	Security User Entity	A person or active system object involved in the event with a security role.
12	Security User Group	(deprecated)
13	Security Resource	A passive object, such as a role table, that is relevant to the event.
14	Security Granularity Definition	(deprecated) Relevant to certain RBAC security methodologies.
15	Provider	A person or organization responsible for providing care. This encompasses all forms of care, licensed or otherwise, and all sorts of teams and care groups. Note, the distinction between providers and the doctor that actually provided the care to the patient.
16	Data Destination	The destination for data transfer, when some other role is not appropriate.
17	Data Archive	A source or destination for data transfer that acts as an archive, database, or similar role.
18	Schedule	An object that holds schedule information. This could be an appointment book, availability information, etc.
19	Customer	An organization or person that is the recipient of services. This could be an organization that is getting services for a patient, or a person that is getting services for an animal.
20	Job	An order, task, work item, procedure step, or other description of work to be performed. E.g., a particular instance of an MPPS.
21	Job Stream	A list of jobs or a system that provides lists of jobs. E.g., an MWL SCP.
22	Table	(Deprecated)
23	Routing Criteria	An object that specifies or controls the routing or delivery of items. For example, a distribution list is the routing criteria for mail. The items delivered may be documents, jobs, or other objects.
24	Query	The contents of a query. This is used to capture the contents of any kind of query. For security surveillance purposes knowing the queries being made is very important.
25	Data Source	The source or origin of data, when there is no other matching role available.
26	Processing Element	A data processing element that creates, analyzes, modifies, or manipulates data as part of this event.

A.5.3 DICOM Specific Audit Messages

The following subsections define message specializations for use by implementations that claim conformance to the DICOM Audit Trail **Message Format** Profile. Any field (i.e., XML element and associated attributes) not specifically mentioned in the following tables shall follow the conventions specified in Section A.5.1 and Section A.5.2.

Note:

This means, e.g., that the meaning of the fields defined in Section A.5.2 is not changed. Furthermore, any of those fields or other optional extensions that are consistent with the schema may be present.

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.

Note

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.~~

In the subsequent tables, the Real-World Entities column indicates the real-world entities and their corresponding element defined in the AuditMessage element in the audit message.

A.5.3.1 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.5.3.1-1. Application Activity Message

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110100, DCM, "Application Activity")
	EventActionCode	M	Enumerated Value <u>Shall be:</u> E = Execute
	EventDateTime	M	n <u>Not</u> specialized
	EventOutcomeIndicator	M	n <u>Not</u> specialized
	EventTypeCode	M	DT (110120, DCM, "Application Start") DT (110121, DCM, "Application Stop")
Active Participant: <u>ActiveParticipant</u> Application started (1)	UserID	M	The identity of the process started or stopped formatted as specified in A.5.2.1.
	AlternativeUserID	MC	If the process supports DICOM, then the AE Titles as specified in A.5.2.2.
	UserName	U	n <u>Not</u> specialized
	UserIsRequestor	M	n <u>Not</u> specialized
	RoleIDCode	M	EV (110150, DCM, "Application")
	NetworkAccessPointTypeCode	U	n <u>Not</u> specialized
	NetworkAccessPointID	U	n <u>Not</u> specialized
Active Participant: <u>ActiveParticipant</u> Persons and/or processes that started <u>ending</u> the Aa application (0..N)	UserID	M	The persons or processes starting or stopping the Aa application.
	AlternativeUserID	U	n <u>Not</u> specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	UserName	U	n Not specialized
	UsersRequestor	M	n Not specialized
	RoleIDCode	M	EV (110151, DCM, "Application Launcher")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized

No Participant Objects are needed for this message.

A.5.3.2 Audit Log Used

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

395 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.5.3.2-1. Audit Log Used Message

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110101, DCM, "Audit Log Used")
	EventActionCode	M	Shall be: enumerated value: r R = <u>r</u> Read
	EventDateTime	M	n Not specialized
	EventOutcomeIndicator	M	n Not specialized
	EventTypeCode	U	n Not specialized
Active Participant: <u>ActiveParticipant</u> 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	n Not specialized
	UserName	U	n Not specialized
	UsersRequestor	M	n Not specialized
	RoleIDCode	U	n Not specialized
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Participant Object: <u>ParticipantObjectIdentification</u> Identity of the audit log (1)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 13 = Security Resource
	ParticipantObjectDataLifeCycle	U	n Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectIDTypeCode	M	Shall be: 12 = URI
	ParticipantObjectSensitivity	U	an Not specialized
	ParticipantObjectID	M	The URI of the audit log
	ParticipantObjectName	M	Shall be: "Security Audit Log"
	ParticipantObjectDetail	U	an Not specialized
	ParticipantObjectDescription	U	an Not specialized
	SOPClass	U	See Section A.5.2.
	Accession	U	See Section A.5.2.
	NumberOfInstances	U	See Section A.5.2.
	Instances	U	See Section A.5.2.
	Encrypted	U	See Section A.5.2.
	Anonymized	U	See Section A.5.2.
	ParticipantObjectContainsStudy	U	See Section A.5.2.

400 A.5.3.3 Begin Transferring DICOM Instances

This message describes the event of a system beginning to transfer a set of DICOM ~~SOP~~ 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

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

Table A.5.3.3-1. Audit Message for Begin Transferring DICOM Instances

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110102, DCM, "Begin Transferring DICOM Instances")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	an Not specialized
	EventOutcomeIndicator	M	an Not specialized
	EventTypeCode	U	an Not specialized
Active Participant: <u>ActiveParticipant</u>	UserID	M	The identity of the process sending the data.
	AlternativeUserID	U	an Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
Process S ending the D ata (1)	UserName	U	n Not specialized
	UserIsRequestor	M	n Not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Active Participant; ActiveParticipant Process receiving the data (1)	UserID	M	The identity of the process receiving the data.
	AlternativeUserID	U	n Not specialized
	UserName	U	n Not specialized
	UserIsRequestor	M	n Not specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Active Participant; ActiveParticipant Other P articipants (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	n Not specialized
	UserName	U	n Not specialized
	UserIsRequestor	M	n Not specialized
	RoleIDCode	U	n Not specialized
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Participant n g Object: ParticipantObjectIdentification Studies being transferred (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	n Not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.

Real-World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectDetail	U	Element "ContainsSOPClass" with one or more SOP Class UID values.
	ParticipantObjectDescription	U	<u>n</u> Not specialized
	SOPClass	MC	<u>n</u> Not specialized. See Section A.5.2 for conditions.
	Accession	U	<u>n</u> Not specialized
	NumberOfInstances	U	<u>n</u> Not specialized
	Instances	U	<u>n</u> Not specialized
	Encrypted	U	<u>n</u> Not specialized
	Anonymized	U	<u>n</u> Not specialized
Participant Object: <u>ParticipantObjectIdentification</u> Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	<u>n</u> Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	<u>n</u> Not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	<u>n</u> Not specialized
	ParticipantObjectDescription	U	<u>n</u> Not specialized

A.5.3.4 Data Export

410 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.

Table A.5.3.4-1. Audit Message for Data Export

415

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110106, DCM, "Export")
	EventActionCode	M	Shall be: R = Read
	EventDateTime	M	<u>n</u> Not specialized
	EventOutcomeIndicator	M	<u>n</u> Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	EventTypeCode	U	n Not specialized
Active Participant: <u>ActiveParticipant</u> Remote U users and/or P processes (0..n)	UserID	M	The identity of the remote user or process receiving the data.
	AlternativeUserID	U	n Not specialized
	UserName	U	n Not specialized
	UserIsRequestor	M	See Section A.5.3.4.1.
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Active Participant: <u>ActiveParticipant</u> <u>Local</u> U user and/or P process E 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	n Not specialized
	UserName	U	n Not specialized
	UserIsRequestor	M	See Section A.5.3.4.1.
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	U	n Not specialized
Active Participant: <u>ActiveParticipant</u> Media (1)	UserID	M	See Section A.5.2.1.
	AlternativeUserID	U	See Section A.5.2.2.
	UserName	U	n Not specialized
	UserIsRequestor	M	Shall be FALSE " <u>false</u> ".
	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.

Real-World Entities	Field Name	Opt.	Value Constraints
	MediaType	M	Values selected from DCID 405 "Media Type Code"
Participant Object: <u>ParticipantObjectIdentification</u> Studies (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	a <u>N</u> ot specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	a <u>N</u> ot specialized
	ParticipantObjectDescription	U	a <u>N</u> ot specialized
	SOPClass	MC	See <u>TableSection A.5.2-4.</u>
	Accession	U	a <u>N</u> ot specialized
	NumberOfInstances	U	a <u>N</u> ot specialized
	Instances	U	a <u>N</u> ot specialized
	Encrypted	U	a <u>N</u> ot specialized
	Anonymized	U	a <u>N</u> ot specialized
Participant Object: <u>ParticipantObjectIdentification</u> Patients (1..N)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	a <u>N</u> ot specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	a <u>N</u> ot specialized
	ParticipantObjectDescription	U	a <u>N</u> ot specialized

A.5.3.4.1 UserIsRequestor

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

A.5.3.5 Data Import

420 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.

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

Table A.5.3.5-1. Audit Message for Data Import

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110107, DCM, "Import")
	EventActionCode	M	Shall be: C = Create
	EventDateTime	M	a <u>N</u> ot specialized
	EventOutcomeIndicator	M	a <u>N</u> ot specialized
	EventTypeCode	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> Users and or Processes is importing the data (1..n)	UserID	M	The identity of the local users or processes importing the data.
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UsersIsRequestor	M	See Section A.5.3.5.
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> Source M media (1)	UserID	M	See Section A.5.2.1.
	AlternativeUserID	U	See Section A.5.2.2.
	UserName	U	a <u>N</u> ot specialized
	UsersIsRequestor	M	Shall be FALSE “false”.
	RoleIDCode	M	EV (110155, DCM, "Source Media")
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	MC	Shall be present if Net-Access-Point-Type-Code is present.
	MediaIdentifier	M	Volume ID, URI, or other identifier for media
	MediaType	M	Values selected from DCID 405 “Media Type Code”

Real-World Entities	Field Name	Opt.	Value Constraints
Active Participant: <u>ActiveParticipant</u> Source (0..n)	UserID	M	See Section A.5.2.1.
	AlternativeUserID	U	See Section A.5.2.2.
	UserName	U	n Not specialized
	UserIsRequestor	M	See Section A.5.3.5.
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	n Not specialized
	NetworkAccessPointID	MC	Shall be present if Net-Access-Point-Type-Code is present.
Participating Object: <u>ParticipantObjectIdentification</u> Studies (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	n Not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	n Not specialized
	ParticipantObjectDescription	U	n Not specialized
	SOPClass	MC	See Table Section A.5.2-4.
	Accession	U	n Not specialized
	NumberOfInstances	U	n Not specialized
	Instances	U	n Not specialized
	Encrypted	U	n Not specialized
	Anonymized	U	n Not specialized
Participating Object: <u>ParticipantObjectIdentification</u> Patients (1..N)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	n Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	a <u>N</u> ot specialized
	ParticipantObjectDescription	U	a <u>N</u> ot specialized

A.5.3.6 DICOM Instances Accessed

430 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 ~~s~~Study are deleted, then the EV_(110105, DCM, "DICOM Study Deleted") event shall be used, see Section A.5.3.8.

435 **Table A.5.3.6-1. Audit Message for DICOM Instances Accessed**

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110103, DCM, "DICOM Instances Accessed")
	EventActionCode	M	Enumerated v <u>Values</u> : C = e <u>C</u> reate R = r <u>R</u> ead U = u <u>U</u> ppdate D = d <u>D</u> delete
	EventDateTime	M	a <u>N</u> ot specialized
	EventOutcomeIndicator	M	a <u>N</u> ot specialized
	EventTypeCode	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> Person and/or P <u>process</u> manipulating <u>accessing</u> the data (1..2)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Participating Object: <u>ParticipantObjectIdentification</u>	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report

Real-World Entities	Field Name	Opt.	Value Constraints
Studies (1..N)	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	n Not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table Section A.5.2-4
	Accession	U	n Not specialized
	NumberOfInstances	U	n Not specialized
	Instances	U	n Not specialized
	Encrypted	U	n Not specialized
	Anonymized	U	n Not specialized
Participant Object: <u>ParticipantObjectIdentification</u> Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	n Not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	n Not specialized
	ParticipantObjectDescription	U	n Not specialized

A.5.3.7 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

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

Table A.5.3.7-1. Audit Message for DICOM Instances Transferred

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110104, DCM, "DICOM Instances Transferred")
	EventActionCode	M	Enumerated Values: C = {c} C reate, if the receiver did not hold copies of the SOP instances transferred. R = {r} R ead, if the receiver already holds copies of the SOP Instances transferred, and has determined that no changes are needed to the copies held. U = {u} U ppdate, 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	a N ot specialized
	EventTypeCode	U	a N ot specialized
Active Participant: <u>ActiveParticipant</u> Process that sent the data (1)	UserID	M	a N ot specialized
	AlternativeUserID	U	a N ot specialized
	UserName	U	a N ot specialized
	UserIsRequestor	M	a N ot specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	a N ot specialized
	NetworkAccessPointID	U	a N ot specialized
Active Participant: <u>ActiveParticipant</u> The p Process that received the data- (1)	UserID	M	a N ot specialized
	AlternativeUserID	U	a N ot specialized
	UserName	U	a N ot specialized
	UserIsRequestor	M	a N ot specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	a N ot specialized
	NetworkAccessPointID	U	a N ot specialized

Real-World Entities	Field Name	Opt.	Value Constraints
Active Participant: <u>ActiveParticipant</u> Other participants that are known, especially third parties that are the requestor (0..N)	UserID	M	<u>n</u> Not specialized
	AlternativeUserID	U	<u>n</u> Not specialized
	UserName	U	<u>n</u> Not specialized
	UserIsRequestor	M	<u>n</u> Not specialized
	RoleIDCode	U	<u>n</u> Not specialized
	NetworkAccessPointTypeCode	U	<u>n</u> Not specialized
	NetworkAccessPointID	U	<u>n</u> Not specialized
Participating Object: <u>ParticipantObjectIdentification</u> Studies being transferred (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	<u>n</u> Not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	<u>n</u> Not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See <u>TableSection</u> A.5.2-4.
	Accession	U	<u>n</u> Not specialized
	NumberOfInstances	U	<u>n</u> Not specialized
	Instances	U	<u>n</u> Not specialized
	Encrypted	U	<u>n</u> Not specialized
	Anonymized	U	<u>n</u> Not specialized
Participating Object: <u>ParticipantObjectIdentification</u> Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	<u>n</u> Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	<u>n</u> Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	a Not specialized
	ParticipantObjectDescription	U	a Not specialized

A.5.3.8 DICOM Study Deleted

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

Table A.5.3.8-1. Audit Message for DICOM Study Deleted

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110105, DCM, "DICOM Study Deleted")
	EventActionCode	M	Shall be: D = d Delete
	EventDateTime	M	a Not specialized
	EventOutcomeIndicator	M	a Not specialized
	EventTypeCode	U	a Not specialized
Active Participant: <u>ActiveParticipant</u> the p Person <u>and</u> /or process deleting the s Study (1..2)	UserID	M	a Not specialized
	AlternativeUserID	U	a Not specialized
	UserName	U	a Not specialized
	UserIsRequestor	M	a Not specialized
	RoleIDCode	U	a Not specialized
	NetworkAccessPointTypeCode	U	a Not specialized
	NetworkAccessPointID	U	a Not specialized
Participating Object: <u>ParticipantObjectIdentification</u> Studies being transferred deleted (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	a Not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	a Not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.

Real-World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See TableSection A.5.2-4
	Accession	U	n Not specialized
	NumberOfInstances	U	n Not specialized
	Instances	U	n Not specialized
	Encrypted	U	n Not specialized
	Anonymized	U	n Not specialized
Participating Object: <u>ParticipantObjectIdentification</u> Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	n Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	n Not specialized
	ParticipantObjectID	M	n he patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	n Not specialized
	ParticipantObjectDescription	U	n Not specialized

A.5.3.9 Network Entry

This message describes the event of a system, such as a mobile device, intentionally entering or leaving the network.
No Participant Objects are needed for this message.

Note

- 455 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
- 460 occurred, not the time that the message is sent.

Table A.5.3.9-1. Audit Message for Network Entry

Real-World Entities	Field Name	Opt.	Value
Event: <u>EventIdentification</u>	EventID	M	EV (110108, DCM, "Network Entry")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	n Not specialized

Real-World Entities	Field Name	Opt.	Value
	EventOutcomeIndicator	M	<u>n</u> Not specialized
	EventTypeCode	M	EV (110124, DCM, "Attach")EV (110125, DCM, "Detach")
Active Participant: ActiveParticipant Node or S system entering or leaving the network (1)	UserID	M	<u>n</u> Not specialized
	AlternativeUserID	U	<u>n</u> Not specialized
	UserName	U	<u>n</u> Not specialized
	UserIsRequestor	M	Shall be FALSE “false”.
	RoleIDCode	U	<u>n</u> Not specialized
	NetworkAccessPointTypeCode	U	<u>n</u> Not specialized
	NetworkAccessPointID	U	<u>n</u> Not specialized

No Participant Objects are needed for this message.

A.5.3.10 Query

465 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. UPS Pull

470 c. UPS Watch

- d. Composite Instance Query

Note

1. The response to a query may result in one or more **DICOM** Instances Transferred or **DICOM** 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.

475 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.

Table A.5.3.10-1. Audit Message for Query

480

Real-World Entities	Field Name	Opt.	Value Constraints
Event: EventIdentification	EventID	M	EV (110112, DCM, "Query")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	<u>n</u> Not specialized
	EventOutcomeIndicator	M	<u>n</u> Not specialized
	EventTypeCode	U	<u>n</u> Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
Active Participant: <u>ActiveParticipant</u> Process I ssuing the Q query (1)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	a <u>N</u> ot specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> The p rocess that will respond to the query (1)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	a <u>N</u> ot specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> Other P participants that are known, especially third parties that requested the query (0..N)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Participating Object: <u>ParticipantObjectIdentification</u> SOP C lass Q queried and the Q query (1)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	DT (110181, DCM, "SOP Class UID")
	ParticipantObjectSensitivity	U	a <u>N</u> ot 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.

Real-World Entities	Field Name	Opt.	Value Constraints
	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	a Not specialized
	SOPClass	U	See Table Section A.5.2-4.
	Accession	U	a Not specialized
	NumberOfInstances	U	a Not specialized
	Instances	U	a Not specialized
	Encrypted	U	a Not specialized
	Anonymized	U	a Not specialized

A.5.3.11 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

- 485 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 ~~a~~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.5.3.11-1. Audit Message for Security Alert

490

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110113, DCM, "Security Alert")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	a 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,

Real-World Entities	Field Name	Opt.	Value Constraints
			and that the security system may have been compromised.
	EventTypeCode	M	Values selected from DCID 403 "Security Alert Type Code".
Active Participant: <u>ActiveParticipant</u> Reporting P person and/or P process (1..2)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Active Participant: <u>ActiveParticipant</u> Performing P persons <u>and</u> /or P processes (0..N)	UserID	M	a <u>N</u> ot specialized
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	M	Shall be FALSE <u>"false"</u> .
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Participating Object: <u>ParticipantObjectIdentification</u> Alert S subject (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	U	Defined Terms: 5 = Master File 13 = Security Resource
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	Defined Terms: 12 = URI DT (110182, DCM, "Node ID")
	ParticipantObjectSensitivity	U	a <u>N</u> ot 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

Real-World Entities	Field Name	Opt.	Value Constraints
			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	M	n 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	n Not specialized
	SOPClass	U	See Table <u>Section</u> A.5.2-4_
	Accession	U	n Not specialized
	NumberOfInstances	U	n Not specialized
	Instances	U	n Not specialized
	Encrypted	U	n Not specialized
	Anonymized	U	n Not specialized

A.5.3.12 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

495 The user usually has UserIsRequestor ~~set to TRUE~~"true", but in the case of a logout timer, the ~~N~~nnode might be the UserIsRequestor.

Table A.5.3.12-1. Audit Message for User Authentication

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110114, DCM, "User Authentication")
	EventActionCode	M	Shall be: <u>E</u> = Execute
	EventDateTime	M	n Not specialized
	EventOutcomeIndicator	M	n Not specialized
	EventTypeCode	M	Defined Terms: EVDT (110122, DCM, "Login") <u>EVDT</u> (110123, DCM, "Logout")
Active Participant: <u>ActiveParticipant</u> Person A <u>a</u> uthenticated or claimed_(1)	UserID	M	n Not specialized
	AlternativeUserID	U	n Not specialized
	UserName	U	n Not specialized

Real-World Entities	Field Name	Opt.	Value Constraints
	UserIsRequestor	M	<u>None</u> specialized
	RoleIDCode	U	<u>None</u> specialized
	NetworkAccessPointTypeCode	M	<u>None</u> specialized
	NetworkAccessPointID	M	<u>None</u> specialized
Active Participant: ActiveParticipant Node or S system performing authentication (0..1)	UserID	M	<u>None</u> specialized
	AlternativeUserID	U	<u>None</u> specialized
	UserName	U	<u>None</u> specialized
	UserIsRequestor	M	<u>None</u> specialized
	RoleIDCode	U	<u>None</u> specialized
	NetworkAccessPointTypeCode	U	<u>None</u> specialized
	NetworkAccessPointID	U	<u>None</u> specialized

A.5.3.13 Order Record

500 This message describes the event of an order being created, modified, accessed, or deleted. This message may only include information about a single patient.

Note

An order record typically is managed by a non-DICOM system. However, DICOM applications often manipulate order records, and thus may be obligated by site security policies to record such events in the audit logs.

505 **Table A.5.3.13-1. Audit Message for Order Record**

Real-World Entities	Field Name	Opt.	Value Constraints
Event: EventIdentification	EventID	M	EV (110109, DCM, "Order Record")
	EventActionCode	M	Enumerated <u>Values</u> : <u>C</u> = e <u>C</u> reate <u>R</u> = r <u>R</u> ead <u>U</u> = u <u>U</u> ppdate <u>D</u> = d <u>D</u> delete
	EventDateTime	M	<u>None</u> specialized
	EventOutcomeIndicator	M	<u>None</u> specialized
	EventTypeCode	U	<u>None</u> specialized
Active Participant: ActiveParticipant	UserID	M	The identity of the person or process accessing or manipulating the data. If both the person and the process are known, both shall be included.

Real-World Entities	Field Name	Opt.	Value Constraints
<u>User</u> Person and/or process accessing or manipulating the data (1..2)	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	U	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
<u>Participant Object:</u> <u>ParticipantObjectID</u> entification Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	a <u>N</u> ot specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	a <u>N</u> ot specialized
	ParticipantObjectDescription	U	a <u>N</u> ot further specialized

A.5.3.14 Patient Record

This message describes the event of a patient record being created, modified, accessed, or deleted.

Note

- 510 There are several types of patient records managed by both DICOM and non-DICOM system. DICOM applications often manipulate patient records managed by a variety of systems, and thus may be obligated by site security policies to record such events in the audit logs. This audit event can be used to record the access or manipulation of patient records where specific DICOM SOP Instances are not involved.

Table A.5.3.14-1. Audit Message for Patient Record

515

Real-World Entities	Field Name	Opt.	Value Constraints
<u>Event:</u> <u>EventIdentification</u>	EventID	M	EV (110110, DCM, "Patient Record")
	EventActionCode	M	Enumerated v <u>Values</u> : <u>C</u> = e <u>C</u> reate <u>R</u> = r <u>R</u> ead <u>U</u> = u <u>U</u> ppdate <u>D</u> = d <u>D</u> delete

Real-World Entities	Field Name	Opt.	Value Constraints
	EventDateTime	M	a <u>N</u> ot specialized
	EventOutcomeIndicator	M	a <u>N</u> ot specialized
	EventTypeCode	U	a <u>N</u> ot specialized
Active Participant: ActiveParticipant UserPerson and/or process accessing or manipulating the data (1..2)	UserID	M	The identity of the person or process accessing or manipulating the data. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	U	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
Participant Object: ParticipantObjectIdentification Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	a <u>N</u> ot specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	M	The patient name
	ParticipantObjectDetail	U	a <u>N</u> ot specialized
	ParticipantObjectDescription	U	a <u>N</u> ot further specialized

A.5.3.15 Procedure Record

This message describes the event of a procedure record being created, accessed, modified, accessed, or deleted. This message may only include information about a single patient.

Note

1. DICOM applications often manipulate procedure records, e.g., with MPPS update. Modality Worklist query events are described by the Query event message.
2. The same **a**Accession **a**Number may appear with several order numbers. The Study participant fields or the entire message may be repeated to capture such many to many relationships.

Table A.5.3.15-1. Audit Message for Procedure Record

Real-World Entities	Field Name	Opt.	Value Constraints
Event: <u>EventIdentification</u>	EventID	M	EV (110111, DCM, "Procedure Record")
	EventActionCode	C	Enumerated v <u>Values</u> : <u>C</u> = e <u>C</u> reate <u>R</u> = r <u>R</u> ead <u>U</u> = u <u>U</u> ppdate <u>D</u> = d <u>D</u> elete
	EventDateTime	M	a <u>N</u> ot specialized
	EventOutcomeIndicator	M	a <u>N</u> ot specialized
	EventTypeCode	U	a <u>N</u> ot specialized
<u>Active Participant:</u> <u>ActiveParticipant</u> <u>UserPerson and/or process accessing or manipulating the data (1..2)</u>	UserID	M	The identity of the person or process <u>accessing or</u> manipulating the data. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	a <u>N</u> ot specialized
	UserName	U	a <u>N</u> ot specialized
	UserIsRequestor	U	a <u>N</u> ot specialized
	RoleIDCode	U	a <u>N</u> ot specialized
	NetworkAccessPointTypeCode	U	a <u>N</u> ot specialized
	NetworkAccessPointID	U	a <u>N</u> ot specialized
<u>Participant Object:</u> <u>ParticipantObjectIdentification</u> Study (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = System Object
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = Report
	ParticipantObjectDataLifeCycle	U	a <u>N</u> ot specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	a <u>N</u> ot specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	MC	Required if ParticipantObjectQuery is not present.
	ParticipantObjectQuery	MC	Required if ParticipantObjectName is not present.
	ParticipantObjectDetail	U	Not further specialized
	ParticipantObjectDescription	U	Not further specialized
	SOPClass	MC	a <u>N</u> ot further specialized. <u>See Section A.5.2 for conditions.</u>

Real-World Entities	Field Name	Opt.	Value Constraints
	Accession	U	<u>a</u> N Not further specialized
	NumberOfInstances	U	<u>a</u> N Not further specialized
	Instances	U	<u>a</u> N Not further specialized
	Encrypted	U	<u>a</u> N Not further specialized
	Anonymized	U	<u>a</u> N Not further specialized
<u>Participant Object:</u> <u>ParticipantObjectIdentification</u> Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = Person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = Patient
	ParticipantObjectDataLifeCycle	U	<u>a</u> N Not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = Patient Number
	ParticipantObjectSensitivity	U	<u>a</u> N Not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectDetail	U	<u>a</u> N Not specialized
	ParticipantObjectDescription	U	<u>a</u> N Not further specialized