DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2016/06/22
Person Assigned	Rob Horn
Submitter Name	Rob Horn
Submission Date	2016/03/13

Correction Number CP- 1616
Log Summary: Remove RFC 3881 references and integrate context
Name of Standard PS 3.15 2017b
Rationale for Correction: The IETF is not interested in maintaining the RFC-3881 content. It has been frozen for over ten years now. As we make clarifications, extensions, etc. the text has become more and more complex. This is leading to confusion and questions from the users about how to interpret the text. It is difficult to combine the old RFC-3881 contents with the updates in DICOM. Now that connectathons and others are using and checking audit messages, there are more questions and clarification requests coming. IHE has eliminated the 3881 references and is just referring to DICOM as the base from which it profiles and extends. Keeping multiple overlapping references was too confusing. This change copies in the content from 3881 that has not changed, eliminates text that has been obsoleted, and merges extensions and changes. This can also deal with clarifications.

Modify A.5.1 as shown (including a change from "–" to a "." in section numbering. This is highlighted in yellow)

A.5.1–.1 Audit Message Schema

The following is the content of the audit schema:

Add A.5.1.2

A.5.1.2 Codes used within the schema

The following value sets are defined in the audit 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

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	Application 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

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 A.5.1.2.2-1 Participant Object Type Code Roles

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
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

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
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

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 2 – System Object
12	URI	2 – System Object

Modify A.5.2 as shown

A.5.2 General Message Format Conventions

The following table lists the primary fields from the message schema specified in A.5.1, 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 Section A.5.1).**~~ The field~~s~~ names are ~~**only those**~~ leaf elements and attributes that are **in the DICOM Audit Message Schema (see Section A.5.1).**~~**specialized or extended for this profile.**~~ 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 RFC3881. RFC3881 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 RFC3881 as the underlying standard. RFC3881 does not include corrections and additions to the audit schema made in DICOM since 2004.

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.

Modify A.5.2-1 as shown

Table A.5.2-1. 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) **Audit Event ID**
	EventActionCode	U	**"**Indicator for type of	~~**See Schema**~~ **C - Create a new database**

	Field Name	Opt.	Description ~~from RFC 3884~~	Additional Conditions on Field Format/Value
			action performed during the event that generated the audit.~~"~~	**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 Perform 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". ~~**Extended by DICOM using**~~ 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

	Field Name	Opt.	Description ~~from RFC 3881~~	Additional Conditions on Field Format/Value
				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) **Audit Active Participant Role ID Code** **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 A.5.2.4
	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.**~~ **See 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.~~"~~	~~**Used as defined in RFC 3881**~~ **1 – Person** **2 - System Object** **3 – Organization** **4 – Other**
	ParticipantObjectTypeCodeRole	U	~~"~~Code representing the functional application	~~**Used as defined in RFC 3881**~~

	Field Name	Opt.	Description ~~from RFC 3881~~	Additional Conditions on Field Format/Value
			role of Participant Object being audited.~~"~~	**See 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.~~"~~	~~**Used as defined in RFC 3881.**~~ **See A.5.1.2.3**
	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.**~~ **See A.5.1.2.4 and** **DCID (404) Audit Participant Object Role ID 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.**"**	~~Used as defined in RFC 3881.~~ **Locally defined terms.**
	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**~~ **This element is a Type-value pair. The "type" attribute is an implementation-defined text string. The "value" attribute is base 64 encoded data. The value is** ~~**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

	Field Name	Opt.	Description ~~from RFC 3881~~	Additional Conditions on Field Format/Value
				(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").

Modify Table A.5.3.4-1 as shown

….			
Active Participant:	UserID	M	See Section A.5.2.3
Media (1)	AlternativeUserID	U	See Section A.5.2.4
	UserName	U	not specialized

	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110155, DCM, "Source 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	M	Volume ID, URI, or other identifier for media. Required if digital media. May be present otherwise.
	MediaType	M	Values selected from DCID (405) **Media Type Code**
…			

Modify Table A.5.3.5-1 as shown

A.5.3.5 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.5.3.5-1. 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

Real World Entities	Field Name	Opt.	Value Constraints
	UserIsRequestor	M	See Section A.5.3.5
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Source Media (1)	UserID	M	See Section A.5.2.3
	AlternativeUserID	U	See Section A.5.2.4
	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) **Media Type Code**
Active Participant: Source (0..n)	UserID	M	See Section A.5.2.3
	AlternativeUserID	U	See Section A.5.2.4
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.5.3.5
	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

Real World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	See Table A.5.2-1
	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

Modify Table A.5.3.11-1 as shown

…			
Event	EventID	M	EV (110107, DCM, "Import")
	EventActionCode	M	Shall be: C = Create
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	~~**Values selected from**~~ DCID(403) **Security Alert Type Code**
…			

Modify A.6 as shown

A.6 Audit Trail Message Transmission Profile - SYSLOG-TLS

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 **DICOM Audit Message Schema (see A.5.1 DICOM Audit Message Schema)** ~~**RFC3881 format, as extended in the audit trail message format profile**~~.

The syslog message shall be created and transmitted as described in RFC5424.

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

Modify A.7 as shown

A.7 Audit Trail Message Transmission Profile - SYSLOG-UDP

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 **DICOM Audit Message Schema (see A.5.1 DICOM Audit Message Schema)** ~~**RFC3881 format, as extended in the audit trail message format profile**~~.

The syslog message shall be created and transmitted as described in RFC5424.

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