DICOM Correction Proposal

STATUS	Assigned
Date of Last Update	20 November 2016
Person Assigned	Rob Horn
Submitter Name	Rob Horn
Submission Date	15 January 2016

Correction Number CP- 1323
Log Summary: Clarify Audit Code Meanings
Name of Standard PS 3.15
Rationale for Correction: The DICOM standard incorporates the Schema that originated from RFC-3881. It has since updated that schema, and will continue to update that schema. The RFC process for updating is glacial and this RFC will not be updated by the IETF. The codes used within the audit messages are defined between DICOM and the RFC. There are no DCID defined for the RFC codes. This is causing problems in IHE and elsewhere because the RFC organization is very confusing. It inhibits adding new capabilities also. The codes used for events are not clearly explained by the RFC and this has also been a source of confusion. It is not practical to use the IETF process to clarify or add codes, nor to make any other documentation improvements. RFC-3881 was published in 2004 and the IETF is not interested in maintaining it on an ongoing basis. Also, several DCM codes were assigned for some patient related events. These were removed from CID 400, 401, 403 as Audit Event IDs at some point and are restored here. DICOM defines a message format for some of these IDs, and various IHE and other standards do use these as event IDs and have defined message formats for the rest. DICOM did define them as controlled vocabulary.
Correction Wording:

Discussion of alternatives

Haing DCID's that eliminate the tiresome searching through the obsolescent RFC is an appropriate step. People are accustomed to DCIDs that indicate external codes to be used.

In addition there is the problem that some of the existing codes require better definitions. And there is a need for more codes, based on experience since 2004. For those we could start defining DICOM codes.

Also RFC-3881 used position within the object to disambiguate codes. This means that we cannot simply move RFC codes into DCIDs without further changes. The code value "1" is re-used in different contexts to have more than five different meanings.

RFC code problems

One approach would be to define multiple code schemes for RC-3881, e.g., RFC-3881a, RFC-3881b, etc. This preserves the RFC values and removes the positional dependency.

Another approach would be to arbitrarily add block numbers to the RFC values. This seems

A more radical approach would be to assign DICOM codes for all the RFC codes. This would be much clearer to newcomers, but less in keeping with DICOM's efforts to preserve backward compatibility as much as possible. It would not violate backward compatibility. It would resolve the code confusion by

telling people to switch from the ambiguous and poorly defined RFC-3881 codes to the replacement DICOM codes.

The relevant Attributes that do not support coded values:

ParticipantObjectTypeCodeRole does not accommodate a coded terminology alternative.

ParticipantObjectDataLifeCycle does not accommodate a coded terminology alternative.

AuditSourceIdentificationContents does support coded terminology

ParticipantObjectIDTypeCode does support coded terminology

Deprecated values:

Some of the Participant Object Type Code Roles codes deserve deprecation and should be left out of the DCIDs. These are:

Resource – which was a kind of generic hold anything type for people and organizations. Why bother with an "other" code when the attribute is already optional. The DICOM style is to omit rather than define a code for other. This is a hold-over from the HL7 approach used when RFC-3881 was defined. HL7 usually includes an "other" in its lists. This code has just confused users.

List – which confuses people completely. There is no record of what kind of list this was. Unlike some of the other confusing codes, this one does not match terms of art from computer security, RBAC, HL7, or DICOM communities. It could have been a generic "other" for computer objects.

Security Granularity Definition - This is a highly specialized term used in some RBAC methodologies. It is only relevant to those terminologies for events related to the operation of that kind of security system. Leaving it out of the DCID does not prohibit its use in those situations, and avoids having to explain the inner workings of this kind of RBAC system as part of explaining the code.

Security User Group – This has confused all the users and there is no text to clarify the intended use. It appears that Security User Entity and Security Resource cover all the people, systems, data tables, etc. involved in modern security systems. It's not clear what would fall into this category.

Table – which confuses people completely. There is no record of what information was kept in this table, or how it was different from a list or masterfile. It does not match terms of art from computer security, RBAC, HL7, or DICOM communities. It could have been a generic "other" for computer objects. One conjecture was that this was for dynamically changing databases (e.g., normalized objects) as opposed to persistent objects (e.g., composite objects), but that's merely a conjecture with no basis in current use, standards, or documents from the time.

Significant Changes

There is a "Report Destination". There is no "Report Source" or equivalent. This CP adds a DICOM code for Report Source. Alternatively we could eliminate both source and destination.

There wasn't an object role for significant processing elements like CAD systems, image processing systems, recommendation systems, etc. This CP adds a code for a processing element.

Should we add another element that would enable use of coded terminology?

The role code is a set of numbers that is controlled by DICOM and not locally extensible. Should this change? The IHE audit messages have had to make some rather obscure choices at times to fit within these constraints. If it is locally extensible, how do we ensure interoperability. This is a secondary key for sorting event information. The primary key is event type, from which the analysis system can assign more detailed meanings to the object's role.

Should we add another element to the participating object to hold codes identifying the kind of object with a coded terminology? This would be a better structure for conversion to other formats and future extensions. The risk with this approach is proper specification and maintenance of the context group. It's unlikely that the users will be familiar with the DICOM process for maintaining context groups, and it's unlikely that it will receive proper maintenance. Certainly a very strong ontological semantic definition will be needed. There will still be terminology confusion problems.

The objects also have IDs, which provide a slower but more comprehensive way to determine what the object is.

The present message uses an XML attribute, which prevents use of the multi-part element structure of a coded terminology. The schema can be extended with an optional coded element and an attribute that indicates to use the coded element. This preserves backward compatibility.

Modify the RNG schema in A.5.1

This takes the approach of continuing the present schema use of context for this code.

An alternative is to add an element that describes the role in terms of a code.

```
                attribute ParticipantObjectTypeCode {( # optional type
                          "1" |    #3 Person
                          "2" |    #3 System object
                          "3" |    #3 Organization
                          "4")}?,         ## Other
                attribute ParticipantObjectTypeCodeRole {( ## optional role
                          "1" |    ## Patient
                          "2" |    ## Location
                          "3" |    ## Report
                          "4" |    ## Resource
                          "5" |    ## Master File
                          "6" |    ## User
                          "7" |    ## List
                          "8" |    ## Doctor
                          "9" |    ## Subscriber
                          "10" |   ## guarantor
                          "11" |   ## Security User Entity
                          "12" |   ## Security User Group
                          "13" |   ## Security Resource
                          "14" |   ## Security Granulatiry Definition
                          "15" |   ## Provider
                          "16" |   ## Report Data Destination
                          "17" |   ## Report Library Data Archive
                          "18" |   ## Schedule
                          "19" |   ## Customer
                          "20" |   ## Job
                          "21" |   ## Job Stream
                          "22" |   ## Table
                          "23" |   ## Routing Criteria
                          "24" |   ## Query
                          "25" |   ## Data Source
                          "26"     ## Processing Element
                               )}?,    ## Query?
```

Add section A.5.2.6 ParticipantObjectTypeCodeRole

A.5.2.6 ParticipantObjectTypeCodeRole

The ParticipantObjectRoleCode 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.

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 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.

Modify Part 16, Table CID 400. Audit Event ID as shown

CID 400 Audit Event ID

Type: **Extensible**

Version: **yyyymmdd**

Table CID 400. Audit Event ID

Coding Scheme Designator	Code Value	Code Meaning
…		
DCM	110108	Network Entry
DCM	**110109**	**Order Record**
DCM	**110110**	**Patient Record**
DCM	**110111**	**Procedure Record**
DCM	110112	Query
…		

CID 401 Audit Event ID

Type: **Extensible**

Version: **yyyymmdd**

Table CID 401. Audit Event Type Code

Coding Scheme Designator	Code Value	Code Meaning
…		
DCM	110137	User Security Attributes Changed
DCM	**110138**	**Emergency Override Stopped**
DCM	**110139**	**Remote Service Operation Started**
DCM	**110140**	**Remote Service Operation Stopped**
DCM	**110141**	**Local Service Operation Started**
DCM	**110142**	**Local Service Operation Stopped**

CID 403 Audit Event ID

Type: **Extensible**

Version: **yyyymmdd**

Table CID 403. Security Alert Type Code

Coding Scheme Designator	Code Value	Code Meaning
DCM	**110120**	**Audit Event: Application Entity has started**

DCM	**110121**	**Audit Event: Application Entity has stopped**
DCM	**110122**	**Audit Event: User Login has been attempted**
DCM	**110123**	**Audit Event: User Logout has been attempted**
DCM	**110124**	**Audit Event: Node has been attached**
DCM	**110125**	**Audit Event: Node has been detached**
DCM	110126	Node Authentication
…		