DICOM Correction Proposal

STATUS	New
Date of Last Update	2016/8/29
Person Assigned	Rob Horn
Submitter Name	Robert.horn@agfa.com
Submission Date	2016/8/29

Correction Number	CP-1655
Log Summary: Revise User ID restrictions in Audit Schema	
Name of Standard PS 3.15, Annex A.5	
Rationale for Correction: Feedback from users indicate that restrictions on different forms of UserID interfere with ease of database, query, etc. The one preference expressed by IHE users is to allocate userID to the ID for humans, groups, etc. , and alternateID for software objects like tasks. This CP relieves the restrictions and allows other organizations like IHE to profile for specific purposes within categories of applications. It is not clear that any specific preference is sufficiently widespread that DICOM should impose it. For this profiling the request was that rather than require the presence of UserID, the schema require the presence of either UserID or AlternativeUserID. This does not invalidate any existing objects, but relaxing the present restriction would affect existing parsers.	
Correction Wording: <include proposed change below, following guidelines for formatting of changes in supplements>	

Modify Table A.5.2.1 General Message Format (adds "?" to UserID definition)

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

Modify Table A.5.2.1 General Message Format

Active Participant	UserID	~~M~~U	"Unique identifier for the user actively participating in the	See Section A.5.2.1. **Either UserID, AlternativeUserID, or both shall be**

(multi-valued)			event."	**present.**
	AlternativeUserID	U	"Alternative unique identifier for the user."	See Section A.5.2.2 . **Either UserID, AlternativeUserID, or both shall be present.**
	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 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.

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.

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

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

a. a URI (the preferred form) identifying the source or destination,

b. an email address of the form "mailto:user@address"

c. a description of the media type (e.g., DVD) together with a description of its identifying label, as a free text field,

d. a description of the media type (e.g., paper, film) together with a description of the location of the media creator (i.e., the printer).

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

A.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:

AETITLES= *aetitle1;aetitle2;…*

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

A.5.2.3 Username