DICOM Correction Proposal

|  |  |
| --- | --- |
| STATUS | Draft Final Text |
| Date of Last Update | 2023/07/27 |
| Person Assigned | steven.nichols@ge.com |
| Submitter Name | steven.nichols@ge.com |
| Submission Date | 2021/06/17 |

|  |
| --- |
| Correction Number CP-2163 |
| Log Summary: Add term to represent the local client copy buffer to CID 405 for Data Export |
| Name of Standard  PS3.16, PS3.17 2022a |
| Rationale for Correction:  PS3.15, [*Table A.5.3.4-1. Audit Message for Data Export*](http://dicom.nema.org/medical/dicom/current/output/chtml/part15/sect_A.5.3.4.html), the row, Active Participant: Media (1), Media Type reference values selected from D[CID 405 “Media Type Code”](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/sect_CID_405.html).  PS3.15 and PS3.17 do not include options that address the use case of exporting media to a client, such as exporting data to the client desktop or copying data into the clipboard buffer.  *Issue: Generalize “media” to be any kind of import/export source/destination (option 1) or add a category of “application” (option 2) that encompasses the blurry gap between network endpoints and physical media. The clipboard manager is one such example. Depending on details of implementation and configuration that may be unknowable to the reporting system, a clipboard manager might transfer clipboard contents to another network device, and it might record a history of past clipboard entries for a long time. The reporting system might have knowledge of this or might not.*  *Another potential example is an S3 bucket that is mounted as a virtual local disk. The reporting system might think this is physical removable media due to virtualization. It might know it is virtualized.*  *DECISION: WG-14 has chosen option 2.*  Destination Media is intended to represent persistent media storage devices that have an identity of their own and that could potentially be transferred across security domain boundaries. We could generalize this (avoiding the challenge of defining terminology for all these grey zone situations), invent a fuzzy boundary term, or invent many terms.  *DECISION: WG-14 has chosen to establish a boundary between application services, clipboard manager, and messaging systems..*  The term “Clipboard Manager” reflects the terminology in general use today. Windows, Linux, MacOS, IOS, and Android all offer the potential to install a “clipboard manager” from at least 10 different vendors. From the perspective of the user these all provide at least “cut and paste” in a GUI environment with a variety of additional vendor specific features.  *[Comment. Canon. Agree that "Clipboard" is not well described by "persistent or transient storage media". By that token, it seems like Email and many/most URI don't fit that well either. Should Email also be application? Would "server" or "database" be appropriate RoleIDCodes? Fixed.]* |



*Add PS3.15 Section* *A.5.2.7 RoleIDCode as follows*

##### A.5.2.7 RoleIDCode

The RoleIDCode is a multi-valued field that is used to identify the type of active participant. Initially, it addressed three distinct events:

1. “Import” events from outside the security domain by physical media, such as CDROMs and USB drives.
2. “Export” events to outside the security domain, also by physical media.
3. "DICOM Instances Transferred” between networked systems within the security domain.

The demarcation between the inside and the outside of the security domain has become less clear; likewise, the assignment of "Import," "Export," or "DICOM Instances Transferred" is also less clear.

* Security responsibilities are often shared and subject to change. They are governed by contracts, service level agreements, and local procedures. As a result, there may multiple ways to classify same event in different institutions or at different times.
* The active participant class for applications and services is used to differentiate virtual media, cloud services, and system applications from physical media:
  + Applications such as DICOM Application Entities, may be best described by considering the application entity as an process or endpoint. The primary criterion for this determination lies in whether the identification is optimally accomplished using a NetworkAccessPointID.
  + The media category is used for participants identifiable by a unique identifier, such as a partition ID on a USB drive, a physical label on a CDROM, or a message-ID on an email message.
  + Applications and services that cannot be identified by a unique identifier are described as Applications. For example, clipboard managers and some messaging systems, including some email systems, lack message-IDs. In such cases, identification is based on the intended destination or claimed sender, e.g., <mailto://person@example.com> or the name of the local service.

To distinguish these kinds of active participants, the RoleIDCode is used:

* When the active participant can be described as an application entity with a network access point, then it can be designated as (110153, DCM, “Source Role ID”) or (110152, DCM, “Destination Role ID”). MediaType and MediaIdentifier may also be present for this kind of participant.
* When the media utilized provides a media ID, the RoleIDCode should include (110154,DCM,”Destination Media”) or (110155,DCM,”Source Media”). In such cases the MediaType shall be present.
* For active participants that are services incapable of identifying an endpoint, messages, or media, the RoleIDCode should include (110150, DCM, “Application”).

This serves a dual purpose:

1. It can aid in locating identifiable media. For example, in email folders and databases can be searched for an email message-ID , and partition-ID in system device logs can be searched for system media mounts identifying a USB device.
2. It can facilitate the discovery of other relevant system logs. For example, a transfer labeled as to or from “sms://123456789” can indicate that the SMS logs are pertinent.

**Export**

|  |  |  |  |
| --- | --- | --- | --- |
| … | | | |
| Active Participant:  Media (1) | UserID | M | See Section A.5.2.1 |
| AlternativeUserID | U | See Section A.5.2.2 |
| UserName | U | not specialized |
| UserIsRequestor | M | Shall be FALSE |
| RoleIDCode | M | **~~EV~~** [**~~(110154, DCM, "Destination Media")~~**](http://dicom.nema.org/medical/dicom/current/output/html/part16.html#DCM_110154)  **Values selected from DCID 402 “Audit Active Participant Role ID Code”**  **See Section A.5.2.7** |
| NetworkAccessPointTypeCode | MC | Required if being exported to other than physical media, e.g., to a network destination rather than to film, paper or CD. May be present otherwise. |
| NetworkAccessPointID | MC | Required if Net Access Point Type Code is present. May be present otherwise. |
| MediaIdentifier | MC | Volume ID, URI, or other identifier for media.  Required if digital media. May be present otherwise. |
| MediaType | M**C** | **~~Values selected from DCID 405 “Media Type Code”~~**  **Values selected from DCID 405 or DCID 4xx.**  **Required if NetworkAccessPoint ID is not present. May be present otherwise.** |

*Modify PS3.15 Table A.5.3.5-1 Audit Message for Data Import as follows*

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

|  |  |  |  |
| --- | --- | --- | --- |
| … | | | |
| Active Participant:  Source Media (1) | UserID | M | See Section A.5.2.1 |
| AlternativeUserID | U | See Section A.5.2.2 |
| UserName | U | not specialized |
| UserIsRequestor | M | Shall be FALSE |
| RoleIDCode | M | **~~EV~~** **~~[(110153, DCM, "Source Media")](http://dicom.nema.org/medical/dicom/current/output/html/part16.html" \l "DCM_110154)~~**  **Values selected from DCID 402 “Audit Active Participant Role ID Code”**  **See Section A.5.2.7** |
| NetworkAccessPointTypeCode | MC | Required if being exported to other than physical media, e.g., to a network destination rather than to film, paper or CD. May be present otherwise. |
| NetworkAccessPointID | MC | Required if Net Access Point Type Code is present. May be present otherwise. |
| MediaIdentifier | MC | Volume ID, URI, or other identifier for media.  Required if digital media. May be present otherwise. |
| MediaType | M**C** | **~~Values selected from DCID 405 “Media Type Code”~~**  **Values selected from DCID 405 or DCID 4xx.**  **Required if NetworkAccessPoint ID is not present.** **May be present otherwise.** |

*Modify PS3.15 Table A.5.3.7-1 Audit Message for DICOM Instances Transferred as follows*

**Table A.5.3.7-1. Audit Message for DICOM Instance Transferred**

|  |  |  |  |
| --- | --- | --- | --- |
| … | | | |
| Active Participant:  Process that sent the data (1). | UserID | M | not specialized |
| AlternativeUserID | U | not specialized |
| UserName | U | not specialized |
| UserIsRequestor | M | not specialized |
| RoleIDCode | M | **~~EV (110153, DCM, "Source Role ID")~~**  **Values selected from DCID 402 “Audit Active Participant Role ID Code”**  **See Section A.5.2.7** |
| NetworkAccessPointTypeCode | U | 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 | U | Required if Net Access Point Type Code is present. May be present otherwise. |
| **MediaIdentifier** | **MC** | **Volume ID, URI, or other identifier for media.**  **Required if digital media. May be present otherwise.** |
| **MediaType** | **MC** | **Values selected from DCID 405 or DCID 4xx.**  **Required if NetworkAccessPoint ID is not present.** **May be present otherwise.** |
| Active Participant:  Process that received the data (1). | UserID | M | not specialized |
| AlternativeUserID | U | not specialized |
| UserName | U | not specialized |
| UserIsRequestor | M | not specialized |
| RoleIDCode | M | **~~EV (110152, DCM, "Destination Role ID")~~**  **Values selected from DCID 402 “Audit Active Participant Role ID Code”**  **See Section A.5.2.7** |
| NetworkAccessPointTypeCode | U | 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 | U | Required if Net Access Point Type Code is present. May be present otherwise. |
| **MediaIdentifier** | **MC** | **Volume ID, URI, or other identifier for media.**  **Required if digital media. May be present otherwise.** |
| **MediaType** | **MC** | **Values selected from DCID 405 or DCID 4xx.**  **Required if NetworkAccessPoint ID is not present.** **May be present otherwise.** |

*Add the following to PS3.15, Section 2 Normative References:*

[RFC 2822] IETF. April 2001. Internet Message Format. <http://www.rfc-editor.org/info/rfc2822>

[RFC 3986] IETF. January 2005. Uniform Resource Identifier (URI): Generic Syntax. <http://www.rfc-editor.org/info/rfc3986>

*Editorial note: PS3.16 Chapter B Table CID 405. Media Type Code is included for reference*

**Table CID 405. Media Type Code**

| **Coding Scheme Designator** | **Code Value** | **Code Meaning** |
| --- | --- | --- |
| DCM | [110030](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110030) | USB Disk Emulation |
| DCM | [110031](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110031) | Email **Message** |
| DCM | [110032](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110032) | CD |
| DCM | [110033](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110033) | DVD |
| DCM | [110034](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110034) | Compact Flash |
| DCM | [110035](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110035) | Multi-media Card |
| DCM | [110036](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110036) | Secure Digital Card |
| DCM | [110037](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110037) | URI |
| DCM | [110010](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110010) | Film |
| DCM | [110038](http://dicom.nema.org/medical/dicom/current/output/chtml/part16/chapter_D.html#DCM_110038) | Paper Document |

*Add a new Context Group to PS3.16 Chapter B as follows*

## CID 4xx application Type Code

**Resources:** **HTML | FHIR JSON | FHIR XML | IHE SVS XML**

**Keyword:** **MediaTypeCode**

**FHIR Keyword:** **dicom-cid-xxx-ApplicationTypeCode**

**Type:** **Extensible**

**Version:** **202xxxxx**

**UID:** **1.2.840.10008.6.1.xxx**

****Table CID 4xx. Application Type Code****

|  |  |  |
| --- | --- | --- |
| Coding Scheme Designator | Code Value | Code Meaning |
| DCM | cp2163-02 | Clipboard |
| DCM | cp2163-01 | Messaging System |
| DCM | 110037 | URI |

*Add the following to PS3.16 Chapter D Table D-1.* ***DICOM Controlled Terminology Definitions (Coding Scheme Designator "DCM" Coding Scheme Version "01")***

**Table D-1. DICOM Controllederminology Definitions (Coding Scheme Designator "DCM" Coding Scheme Version "01")**

| **Code Value** | **Code Meaning** | **Definition** | | **Notes** | |
| --- | --- | --- | --- | --- | --- |
| … | | | | | |
| 110037 | URI | URI Identifier for network or other resource, see **~~RFC3968 [~~RFC 3986].** | |  | |
|  |  |  | |  | |
| 110154 | Destination Media | Audit participant role ID of **persistent or transient storage** media receiving data during an export. | |  | |
| 110155 | Source Media | | Audit participant role ID of media providing data during an import. | |  |
| **cp2163-03** | **Application Service** | | **Audit participant role ID for application entities or services that are not best described by a network endpoint or media identifier. For example, a clipboard manager would be a kind of application service.** | |  |
| … |  |  | |  | |
| **cp2163-02** | **Clipboard Manager** | **A service provided by the operating environment that allows cut and paste transfers within and between application programs. A clipboard manager may have multiple independent storage areas and keep a history of copied items.** | |  | |
| **cp2163-01** | **Messaging System** | **A service that communicates messages between applications or systems; that does not provide message by message identification or tracking; and, identifies the intended destination or claimed source. Examples include some email systems, sms, and chat applications.** | |  | |
| … | | | | | |

*Add the following to PS3.16, Section 2.1 General:*

RFC 3986] IETF. January 2005. Uniform Resource Identifier (URI): Generic Syntax. http://www.rfc-editor.org/info/rfc3986

*Add the following to PS3.17 Chapter WW Audit Messages (Informative)*

**WW.X Data Export of Media to Web Client Desktop Example**

An example of the Media Active Participant and the Participant Object for an Audit Message in the case of a user exporting data from a browser-based image display to a client desktop is shown in Example WW.X-1. See [Table A.5.3.4-1. Audit Message for Data Export in PS3.15.](http://dicom.nema.org/medical/dicom/current/output/html/part03.html#sect_C.11.23.1)

**Example WW.X-1. Sample Data Export Event Report**

<ActiveParticipant

UserID="smitty@readingroom.hospital.org"

UserIsRequestor="true"

NetworkAccessPointID="DOMAIN\COMPUTER"

NetworkAccessPointTypeCode="1">

<RoleIDCode

csd-code="110153"

codeSystemName="DCM"

originalText="Source Role ID"/>

</ActiveParticipant>

<ActiveParticipant

UserID="file://C:\Users\smitty\Desktop\image.jpg"

AlternativeUserID="NTFS"

UserIsRequestor="false">

<RoleIDCode

csd-code="110154"

codeSystemName="DCM"

originalText="Destination Media"/>

<MediaIdentifier>

<MediaType

csd-code="110037"

codeSystemName="DCM"

originalText="URI"/>

</MediaIdentifier>

</ActiveParticipant>

**WW.Y Data Export to Clipboard Example**

An example of the Active Process Participant and the Media Active Participant for an Audit Message in the case of a user copying an image from a client application to the client clipboard is shown in Example WW.X-1.

For brevity, only the Media Active Participant is shown.

Note

It is difficult (or impossible) to detect copy buffer activity from an application server. It is expected that the client application would notify the server of clipboard buffer activity through integrated clipboard functionality or screenshot detection.

See [Table A.5.3.4-1. Audit Message for Data Export in PS3.15.](http://dicom.nema.org/medical/dicom/current/output/html/part03.html#sect_C.11.23.1)

**Example WW.Y-1. Sample Data Export Event Report**

<ActiveParticipant

UserID="PID 3532"

AlternativeUserID="Clipboard User Service"

UserIsRequestor="false">

<RoleIDCode

csd-code="110150"

codeSystemName="DCM"

originalText="Application"/>

<MediaIdentifier>

<MediaType

csd-code="cp2163-01"

codeSystemName="DCM"

originalText="Clipboard Manager"/>

</MediaIdentifier>

</ActiveParticipant>

**WW.Z Data Export to Email Example**

Two examples of Email export. One specifying the Message-ID shown in Example WW.Z-1, and one using an messaging system to a destination is shown in Example WW.Z-2. Note that the email message is identified by the Message-ID in accordance with RFC2822 and RFC5321.

**Example WW.Z-1. Sample Data Export Event Report**

<ActiveParticipant

UserID="Message-ID: <5678.21-Nov-1997@example.com>"

AlternativeUserID="mailto://person@example.com"

UserIsRequestor="false">

<RoleIDCode

csd-code="110154"

codeSystemName="DCM"

originalText="Destination Media"/>

<MediaIdentifier>

<MediaType

csd-code="110031"

codeSystemName="DCM"

originalText="Email Message"/>

</MediaIdentifier>

</ActiveParticipant>

**Example WW.Z-2. Sample Email Data Export Event Report**

<ActiveParticipant

UserID="mailto:person@example.com?bcc=badguy@malware.com"

UserIsRequestor="false">

<RoleIDCode

csd-code="110150"

codeSystemName="DCM"

originalText="Application"/>

<MediaIdentifier>

<MediaType

csd-code="cp2163-02"

codeSystemName="DCM"

originalText="Messaging Service"/>

</MediaIdentifier>

</ActiveParticipant>

**Example WW.Z-3. Sample Chat Data Export Event Report**

<ActiveParticipant

UserID="sms:1234567890"

UserIsRequestor="false">

<RoleIDCode

csd-code="110150"

codeSystemName="DCM"

originalText="Application"/>

<MediaIdentifier>

<MediaType

csd-code="cp2163-02"

codeSystemName="DCM"

originalText="Messaging Service"/>

</MediaIdentifier>

</ActiveParticipant>

**WW.ZA Data Import from Email Examples**

Two examples of Email import. One import specifying the Message-ID shown in Example WW.Z-1, and one using an messaging system to import is shown in Example WW.Z-2. Note that the email message is identified by the Message-ID in accordance with RFC2822 and RFC5321.

**Example WW.Z-1. Sample Data Import Event Report**

<ActiveParticipant

UserID="Message-ID: <5678.21-Nov-1997@example.com>"

UserIsRequestor="false">

<RoleIDCode

csd-code="110155"

codeSystemName="DCM"

originalText="Source Media"/>

<MediaIdentifier>

<MediaType

csd-code="110031"

codeSystemName="DCM"

originalText="Email Message"/>

</MediaIdentifier>

</ActiveParticipant>

**Example WW.Z-2. Sample Data Import Event Report**

<ActiveParticipant

UserID="from: no-bounce@example.com"

UserIsRequestor="false">

<RoleIDCode

csd-code="110150"

codeSystemName="DCM"

originalText="Application"/>

<MediaIdentifier>

<MediaType

csd-code="cp2163-02"

codeSystemName="DCM"

originalText="Messaging Service"/>

</MediaIdentifier>

</ActiveParticipant>