

DICOM Correction Proposal

STATUS	Letter Ballot
Date of Last Update	2025/11/10
Person Assigned	steven.nichols@gehealthcare.com
Submitter Name	steven.nichols@gehealthcare.com
Submission Date	2021/06/17

Correction Number	CP-2163
Log Summary: Add application-type audit destinations and RoleID guidance	
Name of Standard PS3.15, PS3.16	
<p>Rationale for Correction:</p> <p>PS3.15, <i>Table A.5.3.4-1. Audit Message for Data Export</i>, the row, Active Participant: Media (1), Media Type reference values selected from DCID 405 "Media Type Code".</p> <p>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.</p> <p>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.</p> <p>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 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.</p> <p>(110031, DCM, "Email") is too broad for auditing: it denotes a communications system, not a specific export destination. MeSH (MSH:D034742) and NCI (C25170) describe Email generically, not an identifiable target. For traceable audits, we need the concrete destination (e.g., a particular message with an RFC 5322 Message-ID or a mailto: address/application endpoint).</p> <p>This CP retires the generic Email code and replace it with "Email Message" for audit trails.</p> <p>This CP does not incorporate changes proposed in CP-2530.</p>	

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

A.5.2.7 RoleIDCode

The RoleIDCode is a multi-valued element:

One or more values identify the role(s) played by the active participant:

- Initiator: the participant that initiated the handling of the information. The RoleIDCode will be (cp2163-05, DCM, "Initiator Role ID").
- Source: where the information came from. The RoleIDCode will be (110153, DCM, "Source Role ID").
- Destination: where the information is conveyed to. The RoleIDCode will be (110152, DCM, "Destination Role ID").

Additional values identify the type of active participant in this event, differentiating types of media and endpoints to provide traceability of the imported, exported or transferred instances in relevant system logs.

- Physical media is tangible storage with a unique persistent identity. E.g., a USB drive with a partition ID, a CDROM with a volume label, or printed film with a physical label. Include (110154, DCM, "Destination Media") or (110155, DCM, "Source Media") as a RoleIDCode value. The MediaType element will also be present.

- Digital media is a digital resource with a unique persistent identity. E.g., an email message with [RFC5322] Message-IDs, cloud storage objects with unique URIs, or network file shares with specific paths. Include (110154, DCM, "Destination Media") or (110155, DCM, "Source Media") as a RoleIDCode value. The MediaType element will also be present.
- Network access points are network endpoints with a unique identity. E.g., a DICOM Application Entity with an AE Title and/or an identifier for the network access point. Include (110153, DCM, "Source Role ID") or (110152, DCM, "Destination Role ID") as a RoleIDCode value. The MediaType, MediaIdentifier, and NetworkAccessPointID elements may also be present.
- Applications are services that cannot provide unique identification for individual transactions, messages, or media items. E.g., clipboard managers (which cannot uniquely identify clipboard contents), messaging systems that lack message-by-message tracking, and some email systems that do not provide Message-IDs. Include (110150, DCM, "Application") as a RoleIDCode value. Applications may be identified by values in other elements, e.g., mailto://person@example.com, process name, or service identifier.
- A person is someone associated with a persistent identity provided by an organization. E.g., a physician with provider ID or a hospital staff member with a network login. Include (110153, DCM, "Source Role ID"), (110152, DCM, "Destination Role ID") or (cp2163-05, DCM, "Initiator Role ID") as a RoleIDCode value. Persons may be identified by values in other elements, e.g., UserID or AlternativeUserID.

RoleIDCode facilitates:

1. Locating identifiable media. For example, email folders and databases can be searched for an email Message-ID; partition-ID in system device logs can be searched for system media mounts identifying a USB device.
2. Discovering other relevant system logs. For example, a transfer labeled as "to" or "from" "sms://123456789" can indicate that the SMS logs are pertinent.
3. Filtering transactions involving suspicious actors based on their type and role.

Modify PS3.15 Table A.5.3.4-1 Audit Message for Data Export as follows

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

...			
Active Participant:	UserID	M	See Section A.5.2.1
	AlternativeUserID	U	See Section A.5.2.2
Media (1)	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110154, DCM, "Destination Media") 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 Not Access Point Type Code NetworkAccessPointTypeCode 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 "Media Type Code" or DCID 4xx "Application Type Code" . Required if NetworkAccessPointID 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:	UserID	M	See Section A.5.2.1
	AlternativeUserID	U	See Section A.5.2.2
Source Media (1)	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110153, DCM, "Source Media") Values selected from DCID 402 "Audit Active Participant Role ID Code". See Section A.5.2.7.
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	MC	Required if Net Access Point Type Code NetworkAccessPointTypeCode 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 "Media Type Code" or DCID 4xx "Application Type Code". Required if NetworkAccessPointID is not present. May be present otherwise.

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

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

...			
Active Participant:	UserID	M	not specialized
	AlternativeUserID	U	not specialized
Process that sent the data (1).	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Media") Values selected from DCID 402 "Audit Active Participant Role ID Code". See Section A.5.2.7
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
	MediaIdentifier	U	Volume ID, URI, or other identifier for digital media.
	MediaType	UC	Values selected from DCID 405 "Media Type Code" or DCID 4xx "Application Type Code". Required if MediaIdentifier is present.
Active Participant:	UserID	M	not specialized
	AlternativeUserID	U	not specialized
Process that received the data (1).	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	not specialized
	NetworkAccessPointID	U	not specialized
	MediaIdentifier	U	Volume ID, URI, or other identifier for digital media.

	MediaType	UC	Values selected from DCID 405 "Media Type Code" or DCID 4xx "Application Type Code".
			Required if MediaIdentifier is present.

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

50 [RFC 5322] IETF. October 2008. Internet Message Format. <http://www.rfc-editor.org/info/rfc5322>

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

53 Modify PS3.16 Chapter B Table CID 402 as follows:

54 **Table CID 402. Audit Active Participant Role ID Code**
55

Coding Scheme Designator	Code Value	Code Meaning
DCM	110150	Application
DCM	110151	Application Launcher
DCM	110152	Destination Role ID
DCM	110153	Source Role ID
DCM	110154	Destination Media
DCM	110155	Source Media
<u>DCM</u>	<u>cp2163-05</u>	<u>Initiator Role ID</u>
<u>SCT</u>	<u>125676002</u>	<u>Person</u>

56 Modify PS3.16 Chapter B Table CID 405 as follows:

57 **Table CID 405. Media Type Code**

Coding Scheme Designator	Code Value	Code Meaning
DCM	110030	USB Disk Emulation
DCM	<u>110031</u> <u>cp2163-04</u>	Email <u>Message</u>
DCM	110032	CD
DCM	110033	DVD
DCM	110034	Compact Flash
DCM	110035	Multi-media Card
DCM	110036	Secure Digital Card
DCM	110037	URI
DCM	110010	Film
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: ApplicationTypeCode

FHIR Keyword: dicom-cid-4xx-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 Manager
DCM	cp2163-01	Messaging System

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 Controlled Terminology Definitions (Coding Scheme Designator "DCM" Coding Scheme Version "01")

Code Value	Code Meaning	Definition	Notes
...			
110030	USB Disk Emulation	A device that connects using the USB hard drive interface. These may be USB-Sticks, portable hard drives, and other technologies.	
110031	Email	Email and email attachments used as a media for data transport.	Retired.
110032	CD	CD-R, CD-ROM, and CD-RW media used for data transport.	
110033	DVD	DVD, DVD-RAM, and other DVD formatted media used for data transport.	
110034	Compact Flash	Media that comply with the Compact Flash standard.	
110035	Multi-media Card	Media that comply with the Multi-media Card standard.	
110036	Secure Digital Card	Media that comply with the Secure Digital Card standard.	
110037	URI	URI Identifier for network or other resource, see RFC3968 [RFC 3986] .	
110038	Paper Document	Any paper or similar document.	
...			
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 persistent or transient storage media providing data during an import.	

...			
<u>cp2163-05</u>	<u>Initiator Role ID</u>	<u>Audit participant role ID of the entity that initiated the import, export, or transfer event.</u>	
<u>cp2163-04</u>	<u>Email Message</u>	<u>A message transported by email.</u>	
<u>cp2163-02</u>	<u>Clipboard Manager</u>	<u>A service that manages multiple copied or cut items and allows pasting of content within and between applications. A clipboard manager may have multiple independent storage areas and keep a history of copied items.</u>	
<u>cp2163-01</u>	<u>Messaging System</u>	<u>A service that communicates messages between applications or systems, identified by intended destination or claimed source (e.g., mailto:, sms:, chat handles).</u>	

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.

Example WW.X-1. Sample Data Export Event Report to Client Desktop

```

<ActiveParticipant
  UserID="smitty@readingroom.hospital.org"
  UserIsRequestor="true"
  NetworkAccessPointID="DOMAIN\COMPUTER"
  NetworkAccessPointTypeCode="1">
  <RoleIDCode
    csd-code="125676002"
    codeSystemName="SCT"
    originalText="Person"/>
  <RoleIDCode
    csd-code="cp2163-05"
    codeSystemName="DCM"
    originalText="Initiator Role ID"/>
</ActiveParticipant>
<ActiveParticipant
  UserID="PACS_VIEWER_APP_v2.1"
  UserIsRequestor="false">
  <RoleIDCode
    csd-code="110153"
    codeSystemName="DCM"
    originalText="Source Role ID"/>
  <RoleIDCode
    csd-code="110150"
    codeSystemName="DCM"
    originalText="Application"/>
</ActiveParticipant>
<ActiveParticipant
  UserID="file://C:\Users\smitty\Desktop\image.jpg"
  AlternativeUserID="NTFS"
  UserIsRequestor="false">
  <RoleIDCode
    csd-code="110152"
    codeSystemName="DCM"
    originalText="Destination Role ID"/>

```

```

116     <RoleIDCode
117         csd-code="110154"
118         codeSystemName="DCM"
119         originalText="Destination Media"/>
120     <MediaIdentifier>
121         <MediaType
122             csd-code="110037"
123             codeSystemName="DCM"
124             originalText="URI"/>
125         </MediaIdentifier>
126 </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.Y-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.

Example WW.Y-1. Sample Clipboard Destination Participant for Data Export Event

```

138 <ActiveParticipant
139     UserID="chrome.exe (PID=3532) "
140     AlternativeUserID="HWND=0x0003019E"
141     UserIsRequestor="false">
142     <RoleIDCode
143         csd-code="110152"
144         codeSystemName="DCM"
145         originalText="Destination Role ID"/>
146     <RoleIDCode
147         csd-code="110150"
148         codeSystemName="DCM"
149         originalText="Application"/>
150     <MediaIdentifier>
151         <MediaType
152             csd-code="cp2163-02"
153             codeSystemName="DCM"
154             originalText="Clipboard Manager"/>
155         </MediaIdentifier>
156 </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 a 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 [RFC5322].

Example WW.Z-1. Sample Email Destination Participant with Message-ID for Data Export Event

```

162 <ActiveParticipant
163     UserID="Message-ID: 5678.21-Nov-1997@example.com"
164     AlternativeUserID="mailto://person@example.com"
165     UserIsRequestor="false">
166     <RoleIDCode
167         csd-code="110152"
168         codeSystemName="DCM"
169         originalText="Destination Role ID"/>
170     <RoleIDCode
171         csd-code="110154"

```

```

        codeSystemName="DCM"
        originalText="Destination Media"/>
    <MediaIdentifier>
        <MediaType
            csd-code="cp2163-04"
            codeSystemName="DCM"
            originalText="Email Message"/>
    </MediaIdentifier>
</ActiveParticipant>

```

Example WW.Z-2. Sample Messaging System Destination Participant for Data Export Event

```

<ActiveParticipant
    UserID="mailto://person@example.com?bcc=badguy@malware.com"
    UserIsRequestor="false">
    <RoleIDCode
        csd-code="110152"
        codeSystemName="DCM"
        originalText="Destination Role ID"/>
    <RoleIDCode
        csd-code="110150"
        codeSystemName="DCM"
        originalText="Application"/>
    <MediaIdentifier>
        <MediaType
            csd-code="cp2163-01"
            codeSystemName="DCM"
            originalText="Messaging System"/>
    </MediaIdentifier>
</ActiveParticipant>

```

Example WW.Z-3. Sample SMS Destination Participant for Data Export Event

```

<ActiveParticipant
    UserID="sms:1234567890"
    UserIsRequestor="false">
    <RoleIDCode
        csd-code="110152"
        codeSystemName="DCM"
        originalText="Destination Role ID"/>
    <RoleIDCode
        csd-code="110150"
        codeSystemName="DCM"
        originalText="Application"/>
    <MediaIdentifier>
        <MediaType
            csd-code="cp2163-01"
            codeSystemName="DCM"
            originalText="Messaging System"/>
    </MediaIdentifier>
</ActiveParticipant>

```

WW.ZA Data Import from Email Examples

This example illustrates a system administrator who received an email, reviewed it, and then chose to import it into the system. Two methods of Email import are shown: one that specifies the Message-ID (Example WW.ZA-1), and another that uses a messaging system to perform the import (Example WW.ZA-2). Note that the email message is identified by the Message-ID in accordance with [RFC5322].

Example WW.ZA-1. Sample Email Source Participants for Data Import Event

```

<ActiveParticipant
    UserID="admin@hospital.org"
    UserIsRequestor="true"

```



```

231         NetworkAccessPointID="WORKSTATION01"
232         NetworkAccessPointTypeCode="1">
233     <RoleIDCode
234         csd-code="125676002"
235         codeSystemName="SCT"
236         originalText="Person"/>
237     <RoleIDCode
238         csd-code="cp2163-05"
239         codeSystemName="DCM"
240         originalText="Initiator Role ID"/>
241 </ActiveParticipant><ActiveParticipant
242     UserID="Message-ID: 5678.21-Nov-1997@example.com"
243     UserIsRequestor="false">
244     <RoleIDCode
245         csd-code="110153"
246         codeSystemName="DCM"
247         originalText="Source Role ID"/>
248     <RoleIDCode
249         csd-code="110155"
250         codeSystemName="DCM"
251         originalText="Source Media"/>
252     <MediaIdentifier>
253         <MediaType
254             csd-code="cp2163-04"
255             codeSystemName="DCM"
256             originalText="Email Message"/>
257         </MediaIdentifier>
258 </ActiveParticipant>
259

```

Example WW.ZA-2. Sample Messaging System Source Participants for Data Import Event

```

261 <ActiveParticipant
262     UserID="admin@hospital.org"
263     UserIsRequestor="true"
264     NetworkAccessPointID="WORKSTATION01"
265     NetworkAccessPointTypeCode="1">
266     <RoleIDCode
267         csd-code="125676002"
268         codeSystemName="SCT"
269         originalText="Person"/>
270     <RoleIDCode
271         csd-code="cp2163-05"
272         codeSystemName="DCM"
273         originalText="Initiator Role ID"/>
274 </ActiveParticipant>
275 <ActiveParticipant
276     UserID="from: no-bounce@example.com"
277     UserIsRequestor="false">
278     <RoleIDCode
279         csd-code="110153"
280         codeSystemName="DCM"
281         originalText="Source Role ID"/> <RoleIDCode
282         csd-code="110155"
283         codeSystemName="DCM"
284         originalText="Source Media"/>
285     <RoleIDCode
286         csd-code="110150"
287         codeSystemName="DCM"
288         originalText="Application"/>
289     <MediaIdentifier>
290         <MediaType
291             csd-code="cp2163-01"
292             codeSystemName="DCM"
293             originalText="Messaging System"/>
294         </MediaIdentifier>
295 </ActiveParticipant>

```

296

297