DICOM Correction Item

Correction Number CP-783	
Log Summary: Typos and Clarifications in Digital Signature	
Type of Modification Modification	Name of Standard PS 3.3
Rationale for Correction: 1. Fix references in Table C.12-1 and C.12-6 2. Clarify that Modified Attributes Sequence includes the original values, and may include Sequence Attributes. 3. Clarify that the Digital Signatures Macro statement "This Macro may appear in individual sequence items as well as in the main Data Set of the SOP Instance" does not relax the rules for defining a Standard Extended SOP Class.	
Sections of documents affected PS 3.3 Annex C.12	
Correction Wording:	

Table C.12-1
SOP COMMON MODULE ATTRIBUTES

Attribute Name	Tag	Type	Attribute Description
…			
Authorization Equipment Certification Number	(0100,0426)	3	…
*Include 'Digital Signatures Macro' Table C.12-~~5~~**6***			
Encrypted Attributes Sequence	(0400,0500)	1C	…
>Encrypted Content Transfer Syntax UID	(0400,0510)	1	…
>Encrypted Content	(0400,0520)	1	…
Original Attributes Sequence	(0400,0561)	3	Sequence of Items containing all attributes that were removed or replaced by other values in the main dataset. One or more Items may be permitted in this sequence.
>Source of Previous Values	(0400,0564)	2	…
>Attribute Modification Datetime	(0400,0562)	1	…
>Modifying System	(0400,0563)	1	…
>Reason for the Attribute Modification	(0400,0565)	1	…
>Modified Attributes Sequence	(0400,0550)	1	Sequence containing a single item that contains all the Attributes**, with their previous values,** that were modified or removed from the main data set.
*>>Any Attribute from the main data set that was modified or removed**; may include Sequence Attributes and their Items.***			

HL7 Structured Document Reference Sequence	(0040,A390)	1C	…
…			

…

C.12.1.1.3 Digital Signatures Macro

This Macro allows Digital Signatures to be included in a DICOM Data Set for the purpose of insuring the integrity of the Data Set, and to authenticate the sources of the Data Set. Table C.12-6 defines the Attributes needed to embed a Digital Signature in a Data Set. This Macro may appear in individual sequence items as well as in the main Data Set of the SOP Instance.

Note**s**: **1.** Each Item of a Sequence of Items is a Data Set. Thus, individual Sequence items may incorporate their own Digital Signatures in addition to any Digital Signatures added to the Data Set in which the Sequence appears.

2. The inclusion of this Macro in Sequence Items, other than as specified in this Part of the Standard, may be specified in an application-defined Standard Extended SOP Class or Private SOP Class (see PS3.2).

Table C.12-6
DIGITAL SIGNATURES MACRO ATTRIBUTES

Attribute Name	Tag	Type	Attribute Description
MAC Parameters Sequence	(4FFE,0001)	3	A sequence of one or more items that describe the parameters used to calculate a MAC for use in Digital Signatures.
>MAC ID Number	(0400,0005)	1	A number**, unique within this SOP Instance,** used to identify this MAC Parameters Sequence item **from an Item of the Digital Signatures Sequence**.
>MAC Calculation Transfer Syntax UID	(0400,0010)	1	…
>MAC Algorithm	(0400,0015)	1	…
>Data Elements Signed	(0400,0020)	1	…
Digital Signatures Sequence	(FFFA,FFFA)	3	Sequence holding one or more Digital Signatures.
>MAC ID Number	(0400,0005)	1	A number used to identify which MAC Parameters Sequence item was used in the calculation of this Digital Signature.
>Digital Signature UID	(0400,0100)	1	…
>Digital Signature DateTime	(0400,0105)	1	…
>Certificate Type	(0400,0110)	1	…
>Certificate of Signer	(0400,0115)	1	…
>Signature	(0400,0120)	1	The MAC generated as described in Section **C.**12.~~**2.**~~1.1**.3.1.1** and encrypted using the algorithm, parameters, and private key associated with the Certificate of the Signer (0400,0115). See Section C.12.1.1.3.1.2.
>Certified Timestamp Type	(0400,0305)	1C	…

>Certified Timestamp	(0400,0310)	3	…
>Digital Signature Purpose Code Sequence	(0400,0401)	3	…
>>Include 'Code Sequence Macro' Table 8.8-1			…