<table>
<thead>
<tr>
<th>Status</th>
<th>Final Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Last Update</td>
<td>2022/07/08</td>
</tr>
<tr>
<td>Person Assigned</td>
<td>David Clunie <a href="mailto:dclunie@dclunie.com">mailto:dclunie@dclunie.com</a></td>
</tr>
<tr>
<td>Submitter Name</td>
<td>Kevin O’Donnell <a href="mailto:KOdonnell@MRU.MEDICAL.CANON">mailto:KOdonnell@MRU.MEDICAL.CANON</a></td>
</tr>
<tr>
<td>Submission Date</td>
<td>2021/10/20</td>
</tr>
</tbody>
</table>

Correction Number CP-2193

Log Summary: Add Encapsulated Document to de-identification profile

Name of Standard

PS3.15 2022b

Rationale for Correction:

The Encapsulated Document Attribute may contain identifying information and needs to be explicitly addressed, whether the Attribute occurs in IODs defined for encapsulated document storage, or in Standard Extended SOP Classes.

Specify that the Encapsulated Document Attribute is to be removed.

Correction Wording:
Amend PS3.15 as follows, according to this pattern:

E.1 Application Level Confidentiality Profiles

E.1.1 De-identifier

Note

1. The Attributes listed in Table E.1-1 may not be sufficient to guarantee confidentiality of patient identity. In particular, identifying information may be contained in Private Attributes, new Standard Attributes, Retired Standard Attributes and additional Standard Attributes not present in Standard Composite IODs (as defined in PS3.3) but used in Standard Extended SOP Classes. Table E.1-1 indicates those Attributes that are used in Standard Composite IODs as well as those Attributes that are Retired. Also included in Table E.1-1 are some Elements that are not normally found in a Dataset, but are used in Commands, Directories and Meta Information Headers, but that could be misused within Private Sequences. Textual Content Items of Structured Reports, textual annotations of Presentation States, Curves and Overlays are specifically addressed. It is the responsibility of the de-identifier to ensure that all identifying information is removed.

2. It should be noted that conformance to the Basic Application Level Confidentiality Profile does not necessarily guarantee confidentiality. For example, if an attacker already has access to the original images, the Pixel Data could be matched, though the probability and impact of such a threat may be deemed to be negligible. If the Encrypted Attributes Sequence is used, it should be understood that any encryption scheme may be vulnerable to attack. Also, an organization's Security Policy and Key Management policy are recognized to have a much greater impact on the effectiveness of protection.

3. National and local regulations, which may vary, might require that additional attributes be de-identified, though the Profile and Options have been designed to be sufficient to satisfy known regulations without compromising the usefulness of the de-identified instances for their intended purpose.

4. ...

5. ...

6. ...

7. ...

8. ...

9. ...

10. ...

11. ...

12. ...

13. ...

14. ...

15. Because of the varied nature of encapsulated documents (CDA, PDF, STL/OBJ, etc.), options for cleaning the content of the Encapsulated Document (0042,0011) Attribute are not specified by the Standard, and it is required to be replaced. If a De-identifier has additional knowledge of the content it may attempt to clean the Attribute, and document in its Conformance Statement how this is performed.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulated Document</td>
<td>(0042,0011)</td>
<td>N</td>
<td>Y</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>