DICOM Correction Proposal

STATUS	Assigned
Date of Last Update	2023/10/29
Person Assigned	Rob Horn
Submitter Name	rjhorniii@gmail.com
Submission Date	2023/08/28

Correction Number CP-2340
Log Summary: Specify DICOMWeb security for conformance
Name of Standard PS 2023c
Rationale for Correction: Add specific request for information on use of tokens, URI, and other methods of access, authentication, and authorization for DICOMWeb. Profiling activity such as SMART on FHIR may specify combined behaviors for headers, etc., hence the recommendation that a reference be provided

Modify PS3.2 section N.8.6

N.8.6 Web Services Security Features

[Describe in this section the security mechanisms utilized by the implementation. In particular (but not limited to), consider:

- *Audit control mechanism used*
- *Access authorizing policy*
  - ***Use of HTTP headers such as "Authorization: Bearer" should be summarized and provided for details.***
- *Personal authentication mechanisms*
  - ***Use of authentication mechanisms such as OpenID should be summarized and if possible a reference to a standard, profile, or policy provided for details.***
- *De-identification management*
- *~~Certification~~* ***Certificate*** *management tools and process*
- *Web server attack handling*
- ***Credentials Storage Protection (for tokens, assertions, etc.)***
- ***Provisioning, Deprovisioning, Load balancing, Failover, etc.***