DICOM Correction Proposal

STATUS	Assigned
Date of Last Update	2017/02/14
Person Assigned	Rob Horn
Submitter Name	R Horn
Submission Date	2017-02-14

Correction Number CP- 1703
Log Summary: TLS Security Note for Web Services
Name of Standard PS 3.18
Rationale for Correction: The current WADO URI does not specify any security considerations. That section is missing. This adds a note referencing the IETF security recommendations for TLS. An alternative approach is to add a security section and put this information there.
Correction Wording:

Add to Section 3.1

[RFC7525] IETF. May 2015. TLS Recommendations. http://tools.ietf.org/html/rfc7525 .

Modify Section 6.0 as shown

DICOM Web Services use the HTTP and HTTPS protocols as its transport medium. Web Services supports versions 1.0, 1.1 and 2 **or later** of the protocol. ~~**If an origin server supports version 2, it shall also support version 1.1. If an origin server supports version 1.1, it shall also support version 1.0.**~~

It is recommended that user agents that want to use HTTP/2 first initiate an HTTP/1.1 connection to the origin server and then upgrade to HTTP/2. If the upgrade fails then the user agent can still use the HTTP/1.1 connection. [RFC7540] Section 3 explains how to initiate HTTP/2 connections.

Note: HTTPS may mean any SSL or TLS version and options. The IETF [RFC7525] TLS Recommendations cover selection of TLS versions and options. There may also be national or local regulations that apply, and site specific risk analysis may affect the selection. TLS version 1.2 or later is often required and always recommended. Earlier versions are known to be vulnerable to well publicized attacks. All SSL versions are known to be vulnerable to well publicized attacks.