IHE Change Proposal

Tracking information:

|  |  |
| --- | --- |
| IHE Domain | Radiology |
| Change Proposal ID: | CP-RAD-468 |
| Change Proposal Status: | Assigned |
| Date of last update: | October-6-2022 |
| Person assigned: | Steve Nichols |

Change Proposal Summary information:

|  |
| --- |
| WIC and WIA – update security considerations |
| Submitter’s Name(s) and e-mail address(es): | Steve Nichols |
| Submission Date: | 2021-11-18 |
| Integration Profile(s) affected: | WIC, WIA |
| Actor(s) affected: | WIC: Imaging Document Source, Imaging Document WIA: Consumer, Image Capturer and Image Manager |
| IHE Technical Framework or Supplement modified: | WIC TI Supplement, Rev. 1.5 2022-03-10WIA TI Supplement, Rev. 1.2 2022-03-10 |
| Volume(s) and Section(s) affected: | WIA: Vol 1 Sec 42WIC: Vol 1 Sec 38 |
| Rationale for Change:The DICOMweb Search (QIDO-RS), Retrieve (WADO-RS) and Store (STOW-RS) URLs can include individually identifiable information query parameter and that is a possible PHI breach. This CP is to update the Security Considerations to account for this.In WIA, search parameters containing private health information may be in the QIDO URL (RAD-129) and a UID is in the WADO request URL (RAD-107).In WIC, the STOW request URL may contain a Study Instance UID (RAD-108).See: <https://healthcaresecprivacy.blogspot.com/2009/12/double-standard.html?_sm_au_=isVj27QSrwT4s6QMML8tvK34L00HF>, <https://security.stackexchange.com/questions/77302/is-conveying-patient-mrn-in-a-web-service-url-a-hipaa-phi-violation> and <https://www.healthcareitnews.com/news/5-tips-protecting-phi-web-apps>  |

*Modify section 42 in the WIA TI Supp. Vol 1 as follows.*

## 42.5 WIA Security Considerations

The WIA Profile has similar considerations to the IT Infrastructure domain’s Mobile Access to Health Documents (MHD) Profile as well as other profiles that are based on HTTP or REST. The mobile security considerations are stated in [ITI TF-2: Appendix Z.8](https://profiles.ihe.net/ITI/TF/Volume2/ch-Z.html#z.8-mobile-security-considerations). These include recommendations for secure transportation, authentication and authorization. Implementers are encouraged to review that section for applicability to their product environment.

When WIA actors are grouped with XDS actors to access XDS-I infrastructure, all the XDS security requirements apply. See [ITI TF-1: 10.7](https://profiles.ihe.net/ITI/TF/Volume1/ch-10.html#10.7) for details.

Implementers may also consider implementing Cross-Origin Resource Sharing (CORS) (<https://www.w3.org/TR/cors/>) support to allow browser-based clients to retrieve information from distributed sources (for example, queries are performed on server A, and instances are downloaded from server B).

Deployments should consider whether or not:

* The Imaging Document Consumer performs user authentication to access patient data.
* The Imaging Document Responder and Imaging Document Source use credentials or tokens supplied by the Imaging Document Consumer in the QIDO-RS Query and WADO-RS Retrieve transactions
* The Imaging Document Consumer, Imaging Document Responder or the Imaging Document Source (or all) records access in an audit log.

This profile does not define how the Imaging Document Consumer supplies credentials to the Imaging Document Responder or Imaging Document Source in order to provide the user with a seamless "single sign on" experience. The HTTP GET URL transaction allows for a range of authentication mechanisms including HTTP basic authentication (over a secure connection to protect the cleartext credentials), digest authentication, client certificate-based authentication, provision of a SAML assertion in an authentication header, or other mechanisms that are suitable for stateless atomic transaction.

The user authentication and authorization methods are outside the scope of the WIA Profile. Implementers should consider the use of the IHE ITI Profiles [Enterprise User Authentication](https://profiles.ihe.net/ITI/TF/Volume1/ch-4.html) (EUA) and [Internet User Authorization](https://profiles.ihe.net/ITI/TF/Volume1/ch-34.html) (IUA) in their implementations.

Implementations should also consider how availability and integrity will be protected including intentional attacks such as a maliciously crafted query that interfere with service availability.

Both the WADO-RS and QIDO-RS transactions may include in their response a URL which specifies where the corresponding objects can be retrieved. In the absence of protection, such as TLS, a malicious attacker may intercept the response and rewrite these URL's to a location of suspect origin. An Imaging Document Consumer should verify that any received URL is valid and corresponds to a known secure location.

**Both the WADO-RS and QIDO-RS transactions may include private health information in the URL (e.g., query parameters, or a UID). In the absence of protection, such as TLS, an unauthorised individual may intercept a URL and obtain private health information. URLs may also be stored in device logs. Implementers should consider the use of the IHE ITI** [**Audit Trail and Node Athentication**](https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html) **(ATNA) Profile in for secure transportation, authentication and authorization.**

## 42.6 WIA Cross Profile Considerations

## …

## 42.6.5 ATNA – Audit Trail and Node Authentication

**An Imaging Document Consumer and Imaging Document Source might be grouped with Secure Node or Secure Application in order to 1) enable secure transport, using Secure Transport (STX) Options 2) control access to log entries that may contain individually identifiable information in unencrypted URLs using Authenticate Node [ITI-19] and 3) record Query and DICOM Instances Accessed audit events using Record Audit Events [ITI-20].**

*Update the WIC TI Supp. Vol 1 Sec 38 as follows.*

## 38.5 WIC Security Considerations

Since the Image Capturer may be running in a mobile device outside of the hospital private network, it is important to ensure that the communication between the Image Capturer and the Image Manager is secure. Encryption specified in the ITI [Audit Trail and Node Authentication](https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html) (ATNA) Profile can provide secure data transport. ATNA audit messages can ensure audit trails for private health information are captured.

It is recommended that the Image Manager will be grouped with the ATNA Secure Node or Secure Application to record audit messages for the transactions performed. It is not expected that the Image Capturer will record audit messages.

The Image Manager may want to restrict which users are authorized to upload. The ITI [Internet User Authorization](https://profiles.ihe.net/ITI/TF/Volume1/ch-34.html) (IUA) Profile provides OAuth-based user authorization.

The Image Manager may want to restrict which devices are authorized to upload. ATNA provides certificate-based node authentication.

Since the Image Capturer may be running in a mobile device that can easily be lost, it is important to consider how much information should be retained in the mobile device. This includes patient demographics as well as the images, videos or reports.

**The Image Capturer and Image Manager may want to restrict user access to system logs. Unencrypted URLs containing private health information (i.e., the Study Instance UID) may be stored in device logs. Node Authentication and Access Control specified in the ITI** [**Audit Trail and Node Athentication**](https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html) **(ATNA) Profile can control access to these log.**

## 38.6 WIC Cross Profile Considerations

**IID – Invoke Image Display**

An Image Capturer might be grouped with an Image Display in the Invoke Image Display Profile to create and store evidence documents back to the associated Image Manager based on images being viewed and their associated patient and study context.

**XDS-I.b – Cross-Enterprise Document Sharing for Imaging**

An Image Capturer might be grouped with an XDS-I.b Imaging Document Consumer to create and store new objects back to the Image Manager based on study objects it is viewing.

An Image Manager might be grouped with an XDS-I.b Imaging Document Source to receive objects sent from an Image Capturer and publish a new manifest.

**WIA – Web-based Image Access**

An Image Capturer might be grouped with an WIA Imaging Document Consumer to create and store new objects back to the Image Manager based on study objects it is viewing.

An Image Manager might be grouped with an WIA Imaging Document Source to receive objects sent from an Image Capturer.

**PDQm – Patient Demographics Query for Mobile**

An Image Capturer might be grouped with a PDQm Patient Demographics Consumer to retrieve reliable patient demographics from the Patient Demographics Supplier.

**ATNA – Audit Trail and Node Authentication**

**Both the Image Capturer and the Image Manager might be grouped with Secure Node or Secure Application in order to 1) enable encryption, using Secure Transport (STX) Options 2) control access to log entries that may contain Study Instance UIDs in unencrypted URLs using Authenticate Node [ITI-19] and 3) record DICOM Instances Transferred audit events using Record Audit Events [ITI-20].**