Proposed Restructuring and Additions to FHIR Implementer's Safety Check List

Kathleen Connor

1. Current FHIR Implementer Safety Check List – See Appendix below.

http://hl7.org/fhir/safety.html

Current Check List is a mixed bag of very different implementer safety concerns. Feedback is requested. The proposed restructuring and additional check list items below make it easier for implementers to focus on a type of safety concern, and are linked with relevant sections in the FHIR specification, which are lacking for some items in the current list.

Several current check list items had multiple topics, so these have been made separate items. Comments recommending omission of redundant caveats – e.g., the "right" consent when applicable. If the consent is "right" it is by definition applicable.

In addition, references to external guidance on API Privacy and Security are linked to the Safety Topics for further information and understanding of the expectations of the community of interest.

2. FHIR Conformance Safety Checks

#2 For each resource that my system handles, I've reviewed the Modifier elements.

#3 My system checks for modifierExtension elements.

My system checks the meta.tag and meta.security elements on the resource to determine whether any special processing rules apply

#4 My system supports elements labeled as "must-support" in the profiles that apply to my system.

#11 When other systems return http errors from the RESTful API and Operations (perhaps using Operation Outcome), my system checks for them and handles them appropriately.

#12 My system caters for parameters that have missing values when doing search operations, and responds correctly to the client with regard to erroneous search parameters.

#13 My system ensures checks for patient links (and/or merges) and handles data that is linked to patients accordingly.

#14 My system publishes a Capability Statement with StructureDefinitions, ValueSets, and OperationDefinitions, etc., so other implementers know how the system functions

3. Privacy Safety Checks[1]

#10 My system checks that the right Patient consent has been granted.[2]
#NEW My system sends an Accounting of Disclosure to the consenter as requested when permitted actions on resources are performed using a FHIR AuditEvent or Provenance Resource.

4. Security Safety Checks[3] Version 1 [See Version 2 Below]

#1 Production exchange of patient or other sensitive data will always use some form of encryption on the wire

#NEW My system validates all input received from other actors to assure the data is well formed and does not contain content that would cause unwanted system behavior. [Link to Input Validation FHIR Security page[4]]

#9b My system correctly logs AuditEvents

#9c My system uses the right security labels.

#13 My system ensures that system clocks are synchronized using a protocol like NTP or SNTP, or my server is robust against clients that have the wrong clock set

#NEW My system appropriately protects any authenticators/authenticator mechanisms, and carefully select the type of credential/strength of authenticator required, based on the use case and risk management. [Link to Protect Authenticators – Amplify FHIR Security Authentication Section @ https://www.hl7.org/fhir/security.html#authentication] [5]

#NEW My system ensures that the level of assurance for identity proofing reflects the appropriate risk, given the issued party's exposure to health information.[6] [Link to new identity proofing section at https://www.hl7.org/fhir/secpriv-module.html]

[1] See ONC Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (API) https://www.healthit.gov/sites/default/files/privacy-security-api.pdf and Precision Medicine Initiative: Privacy and Trust Principles

[2] https://www.hl7.org/fhir/secpriv-module.html#privacy-consent

[3] See ONC Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (API) https://www.healthit.gov/sites/default/files/privacy-security-api.pdf and Precision Medicine Initiative: Data Security Policy Principles and Framework https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/security-principles-framework.pdf

[4] From https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=15909&start=0 [Link "validates all input" to FHIR Security topic @... TBD - Add to bullet list at top of FHIR Security page: Input Validation - Validate all input received from other actors to assure the data is well formed and does not contain content that would cause unwanted system behavior. Testing ensures that the input is not susceptible to data input validation errors by using techniques such as fuzzing, invalid input attacks, and injection attacks]

[5] From https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16530. Link "authenticators/authenticator mechanisms" to FHIR Security Credentialing topic @.... When OAuth is used, see https://tools.ietf.org/html/rfc7521#section-8 and https://tools.ietf.org/html/rfc6749#section-10

[6] From https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16527. See FHIR Security topic @...

#NEW My system utilizes a risk and use case appropriate OAuth profile.[7]

#NEW My system uses OpenID Connect (or other suitable authentication protocol) to verify identity of end user, where it is necessary that end-users be identified to the client application.[8]

#NEW My system ensures that Hypertext Transfer Protocol (HTTP) headers of a web server and API error messages or faults do not disclose detailed information about the underlying web server that could be the source of potential exploitation. [Track # TBD]. [Link to Safeguarding against Exploits section at https://www.hl7.org/fhir/secpriv-module.html]

#NEW My system uses security methods for an API to authenticate where Domain Name System (DNS) responses are coming from and ensure that they are valid. [Track # TBD]. [Link to Validate DNS source and validity section at https://www.hl7.org/fhir/secpriv-module.html]

#NEW Data Protection: Error Message Disclosures. (API Paper Pg 16) Ensure that Hypertext Transfer Protocol (HTTP) headers of a web server and API error messages or faults do not disclose detailed information about the underlying web server that could be the source of potential exploitation.

5. Provenance Safety Checks

#9a My system makes the right Provenance statements.

#NEW My system persists association between a Provenance statement and referenced artifact.

#NEW My system appropriately chains Provenance statements associated with a referenced artifact or permutation of an original artifact throughout its lifecycle.

6. Integrity Safety Checks

#6 My system can render narratives properly (where they are used). [Current link http://hl7.org/fhir/narrative.html%20-%20css is broken. Link to new Narrative url https://www.hl7.org/fhir/narrative.html and FHIR Security Narrative Section https://www.hl7.org/fhir/security.html#narrative

#NEW My system validates all input received from other actors to assure that the data is well-formed and does not contain content that would cause unwanted system behavior.

[7] https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16534 Add to checklist Authorization: When using OAuth, profile profiling needs to be done. Consider use of SMART App Authorization Guide where appropriate.

[8] https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16532 Add to the checklist Recommend use of OpenID Connect (or other suitable authentication protocol) to verify identity of end user, where it is necessary that end-users be identified to the client application. Reference SMART on FHIR, UMA, HEART etc.

#NEW My system ensures that the input is not susceptible to data input validation errors by using techniques such as fuzzing, invalid input attacks, and injection attacks.

Reworked Input Validation CP 15909 - *Validate all input received from other actors to assure the data is well formed and does not contain content that would cause unwanted system behaviour. Testing ensures that the input is not susceptible to data input validation errors by using techniques such as fuzzing, invalid input attacks, and injection attacks.*
https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=15909&start=0%20-%20_blank

Security Safety Check List Version 2

Make the following topics from FHIR Security page into sub-topics of the Security Safety Check List. Additions to or additions of Topics are *italicized.*

- Time Keeping - all clocks should be synchronized using NTP/SNTP, and the design of the system should be robust against a system clock with the wrong value

  #13 My system ensures that system clocks are synchronized using a protocol like NTP or SNTP, or my server is robust against clients that have the wrong clock set,

- Communications Security - all exchange of production data should be secured using TLS/SSL (e.g. https) *and encryption*

  #1 Production exchange of patient or other sensitive data will always use some form of encryption on the wire.

- NEW Security Topic – Identity Proofing

  #NEW My system ensures that the level of assurance for identity proofing reflects the appropriate risk, given the issued party's exposure to health information.[9] [Link to new identity proofing section at https://www.hl7.org/fhir/secpriv-module.html]

- Authentication - Users/Clients may be authenticated in any way desired. For web-centric use, OAuth is recommended

  #NEW My system utilizes a risk and use case appropriate OAuth profile.[10]

  #NEW My system uses OpenID Connect (or other suitable authentication protocol) to verify identity of end user, where it is necessary that end-users be identified to the client application.[11]

[9] From https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16527. See FHIR Security topic @...

[10] https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16534 Add to checklist Authorization: When using OAuth, profile profiling needs to be done. Consider use of SMART App Authorization Guide where appropriate.

[11] https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16532 Add to the checklist Recommend use of OpenID Connect (or other suitable authentication protocol) to verify identity of end user, where it is necessary that end-users be identified to the client application. Reference SMART on FHIR, UMA, HEART etc.

#NEW My system appropriately protects any authenticators/authenticator mechanisms, and carefully select the type of credential/strength of authenticator required, based on the use case and risk management. [Link to Protect Authenticators – Amplify FHIR Security Authentication Section @ https://www.hl7.org/fhir/security.html#authentication] [12]

#NEW My system uses security methods for an API to authenticate where Domain Name System (DNS) responses are coming from and ensure that they are valid. [Track # TBD]. [Link to Validate DNS source and validity section at https://www.hl7.org/fhir/secpriv-module.html]

- Authorization/Access Control - FHIR defines a Security Label infrastructure to support access control management. FHIR may also define a set of resources to administer access control management, but does not define any at present.

  #NEW My system verifies a requester's clearance.
  #NEW My system makes access control decisions based on whether a requester's verified clearance attributes (security labels) meet or exceed the security labels assigned to the requested FHIR Resource or Bundle.

- Audit & *Provenance* - FHIR defines provenance and audit event resources suitable for tracking the origins, authorship, history, status, and access of resources.

  #9b My system correctly logs AuditEvents

  #9a My system makes the right Provenance statements.

  #NEW My system persists association between a Provenance statement and referenced artifact.

  #NEW My system appropriately chains Provenance statements associated with a referenced artifact or permutation of an original artifact throughout its lifecycle.

- Digital Signatures - FHIR includes several specifically reserved locations for digital signatures
  #NEW My system ???
- Attachments - FHIR allows for binary resources and attachments. These have their own concerns.
  #NEW My system ???
- Labels - FHIR allows for set of security related tags that affect the way resources are handled.

  #9c My system uses the right security labels.

  #NEW My system persists security labels assigned to FHIR artifacts.

[12] From https://gforge.hl7.org/gf/project/fhir/tracker/?action=TrackerItemEdit&tracker_item_id=16530. Link "authenticators/authenticator mechanisms" to FHIR Security Credentialing topic @.... When OAuth is used, see https://tools.ietf.org/html/rfc7521#section-8 and https://tools.ietf.org/html/rfc6749#section-10

- Data Management Policies - FHIR defines a set of capabilities to support data exchange. Not all the capabilities that FHIR enables may be appropriate or legal for use in some combinations of context and jurisdiction (e.g. HIPAA for exchange between institutions). It is the responsibility of implementers to ensure that relevant regulations and other requirements are met.
- *KC – think this belongs to the Privacy Safety Check List*
- Narrative - Care must be taken when displaying the narrative from FHIR resources
  #NEW My system ???

http://build.fhir.org/security.html

Appendix: Current FHIR Implementer's Safety Check List

7.9 Clinical Safety

FHIR Infrastructure Work Group Maturity Level: N/A Ballot Status: Informative

This specification defines data elements, resources, formats, methods and APIs for exchanging healthcare data between different participants in the healthcare process. As such, Clinical Safety is a key concern with regard to the specification and its many and various implementations.
STU Note: This page, and the concept of *safety* in an API specification, needs further development. Feedback is welcome here
.

7.9.1 Implementer's Safety Check List

FHIR is as simple to implement as we know how to make it. However, due to the nature of healthcare, and healthcare processes, and cultural concerns, there are a number of features in FHIR that implementers are obliged to consider in order to implement safe systems.
This section is a check list to help implementers be sure that they've considered all the parts of FHIR that impact on their system design with regard to safety.

1. Production exchange of patient or other sensitive data will always use some form of encryption on the wire
2. For each resource that my system handles, I've reviewed the Modifier elements
3. My system checks for modifierExtension elements
4. My system supports elements labeled as "must-support" in the profiles that apply to my system
5. For each resource that my system handles, my system handles the full Life cycle (status codes, currency issues, and erroneous entry status)
6. My system can render narratives properly (where they are used)
7. My system has documented how distributed resource identification works in its relevant contexts of use, and where (and why) contained resources are used
8. My system manages lists of current resources correctly
9. My system makes the right Provenance statements and AuditEvent logs, and uses the right security labels where appropriate
10. My system checks that the right Patient consent has been granted (where applicable)
11. When other systems return http errors from the RESTful API and Operations (perhaps using Operation Outcome), my system checks for them and handles them appropriately

12. My system caters for parameters that have missing values when doing search operations, and responds correctly to the client with regard to erroneous search parameters
13. My system ensures that system clocks are synchronised using a protocol like NTP or SNTP, or my server is robust against clients that have the wrong clock set
14. My system ensures checks for patient links (and/or merges) and handles data that is linked to patients accordingly
15. My system publishes a Capability Statement with StructureDefinitions, ValueSets, and OperationDefinitions, etc., so other implementers know how the system functions

Obviously this list is only a small part of the overall safety check list for an application, which will have checks regarding jurisdictionally mandated policies, internal integrity, etc.

In addition, server developers should check these specific additional checks for client convenience:

1. Server: CORS (cross-origin resource sharing

) is enabled (many clients are javascript apps running in a browser)

2. JSON is supported (many clients are javascript apps running in a browser; XML is inconvenient at best)
3. JSON is returned correctly when errors happen (clients often don't handle HTML errors well)
4. the _format header is supported correctly
5. Errors are trapped and an OperationOutcome returned

From <http://hl7.org/fhir/safety.html>