DRAFT

Proposed response to “Playing with FHIR” from HL7 Patient Empowerment Working Group

Ryan M Harrison

2021-10-21

Context

On 13 Oct 2021, security blogger Alissa Knight released a report entitled “Playing with FHIR.”[1] Briefly, the report covers her white hat penetration testing of patient-directed exchange FHIR servers (EHR and Patient Access API) and clients. She finds numerous common (OWASP Top 10) security vulnerabilities in the implementations of Patient Access API FHIR servers and clients (aggregators). While unfortunately common, these security vulnerabilities expose can be used to expose sensitive patient information to unauthorized users. Detailed analysis is available elsewhere.[2]

Because of the report’s implications to patient privacy and security, the HL7 Patient Empowerment Working Group (WG) hosted Ms. Knight during is 14 Oct and 21 Oct 2021 weekly meetings.

Statement

The Patient Empowerment Working Group welcomes the feedback of the security community in balancing the interest of patients right of access with patient privacy and security. Too often are privacy and security concerns used as false idols to limit and restrict patients right to their own medical data. Our response to the question of patient access versus privacy/security is “both and.” We ask the FHIR patient-directed exchange community – HL7, CARIN, ONC, HHS OCR – to consider the following recommendations. Together, we can empower patients with access to their own medical data.

Recommendation 1: Provide an identified list of APIs and vulnerabilities to HL7

From: Alissa Knight, Security Blogger
To: HL7 Security WG

The Patient Empowerment WG respects Ms. Knights decision to refrain from publishing vulnerabilities linked to specific vendors and APIs. However, the work of remediating the specific vulnerabilities and making proactive updates across the FHIR ecosystem to reduce the likelihood of future vulnerabilities in hindered by the lack of a identifying information.

We recommend that the following information be included for each API tested

- Vendor Name
- Vendor Contact
- Vendor API details (url, version and date tested)
- Was the API/vendor certified by an ONC-ACB (Authorized Certification Body)? If so, which
- Did the API vendor sign a trust framework (e.g. CARIN Code of Conduct). If so, which?
- List of vulnerabilities discovered

---

1 Playing with FHIR is available for download, behind an email wall, at https://approov.io/for/playing-with-fhir/

2 Reputable ananlysis includes:

- Grahame Grieve's post Weds 13 Oct 2021: Security Vulnerabilities in FHIR implementations
- John Moehrke's blog post Thurs 14 Oct 2021: Security of #FHIR Implementation Concerns

- Was the vulnerability on the OWASP Top 10?
- Was the vulnerability detected by ONC Inferno?
- Was the vulnerability detected by AEGIS Touchstone?
- If applicable, was the vulnerability detected by the ONC-ATL?
- Nice to have: Steps for the reproduction of the vulnerability.

Recommendation 2: Inform the impacted vendors/APIs of their security vulnerabilities
From: HL7 Security
To: Impacted vendors

Recommendation 3: Inform test frameworks of API security vulnerabilities
From: HL7 Security
To: Test frameworks (ONC Inferno, Aegis Touchstone, ONC-ATLs)

It is possible that some of the security vulnerabilities should have been caught by the common FHIR test frameworks. The scope of the various test frameworks vary, so they should decide whether the vulnerability is in or out of their testing scope. Our expectation is that ONC Inferno will have the narrowest scope, while ONC-ATLs will have the broadest testing scope.

Recommendation 4: Review the FHIR community responsible disclosure process
To: ONC, HL7
White hat hackers are powerful allies to patient security and privacy. ONC and HL7s polices should facilitate the responsible notification and correction of security vulnerabilities. While individual vendors should have their own responsible disclosure procedures, including reporting to CVE, both ONC and HL7 have an important coordination role to play.

Recommendation 5: Consider publishing a model responsible disclosure guidance for aggregators.
To: CARIN Alliance, HL7 Security

The CARIN Code of Conduct includes breach notification
> V. Security
> d) Comply with applicable breach notification laws and provide meaningful remedies to address security breaches, privacy, or other violations incurred because of misuse of the user's personal data.

However, aggregators may not understand the implications of this provision without reference to a model CVE and responsible disclosure tailored to the health space. One option is to incorporate HL7 Security responsible disclosure guidance by reference in the CARIN Code of Conduct.

Recommendation 6: Create guidance for Patient Access API 3rd-party app onboarding and consent screens
To: CARIN Alliance, SMART
Cc: CMS

Patients should not need to be technical experts to understand whether their health data is being responsibly shared.

Consider including a requirement that Patient Access API Servers should require a privacy statement from 3rd-party apps. CMS may need to clarify that a FHIR implementation guide requirement for a privacy statement is not information blocking.

Consider a recommendation that Patient Access API 3rd-party apps use an existing and recognized Trust Framework and Code of Conduct, e.g. from CARIN.

Consider including a requirement that Patient Access API Servers visually indicate the "safety" of a 3rd-party application. For example, showing positive badges for CARIN Trust Framework and ONC vetted application, and/or showing negative warnings for apps that have not voluntarily attested.

Recommendation 7: Review the ONC-ATL and ONC-ACB guidance for vulnerabilities not covered by policy
To: ONC

It is unlikely that any of the aggregators with discovered vulnerabilities were vetted by an ONC-ATL; however, ONC should double check that the discovered vulnerabilities are covered by ONC-ATL and ONC-ACB rules.

Recommendation 8: Consider updates to breach notification enforcement to aggregators
To: HHS OCR

HHS OCR is the enforcement authority for the HIPAA Privacy rule, including breach notification. Under HIPAA, breach notification was only a requirement of covered entities. HITECH expanded the scope of breach notification to Business Associates. Aggregators, such as those enabled under the CMS Final Rule's Patient Access API, are often neither Covered Entities or Business Associates; however, a breach of aggregator data can be just as damaging to patient privacy as a breach to a Covered Entity. The Patient Empowerment WG asks the HHS OCR to consider expanding breach notification enforcement to CE/BA entities such as aggregators.