DRAFT

Recommendations to enhance patient privacy and security without compromising the patient's right of access

From: HL7 Patient Empowerment Working Group
To: HL7 Policy Advisory Committee (PAC)
2021-10-22c

Mission of the HL7 Empowerment Working Group

The HL7 Patient Empowerment Work Group's mission is to promote and amplify the viewpoint of patients and their caregivers in HL7's standards work, in support of the HL7 mission.[1] One facet of our work is ensuring that appropriate impacts on patients, both positive and negative, are considered in HL7 standards work.

"Playing with FHIR" report

On 13 Oct 2021, security blogger Alissa Knight released a report entitled "Playing with FHIR."[2] Briefly, the report covers her white hat penetration testing of patient-directed FHIR servers and clients. She finds numerous common (OWASP Top 10) security vulnerabilities in the implementations of FHIR servers and clients (most commonly, client aggregators). While unfortunately common, these security vulnerabilities expose sensitive patient information to unauthorized users. Detailed analysis is available elsewhere.[3]

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

Statement

The Patient Empowerment Working Group is deeply concerned by the vulnerabilities revealed in Ms. Knight's report. We are mad that our most sensitive data are stored in FHIR APIs with badly flawed implementations.

We welcome the input 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."

Security vulnerabilities in FHIR implementations should be addressed with a defense in depth: policy guidance, standards guidance, real world implementation testing, and finally responsible disclosure and breach notification.

---

[1] Patient Empowerment Working Group: Mission and Charter

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

[3] 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

Security vulnerabilities in FHIR implementations should not be used as an excuse to block patient access, or otherwise undermine the information blocking rules (as Ms. Knight calls for in some of her recommendations).

All vulnerabilities are not created equal. There exists a regulatory hierarchy by which vulnerabilities can be judged.

HIPAA-governed aggregator (BAA in place with health system)

A. Direct sharing from health system to BA
B. Consumer mediated sharing from health system to BA (via patient credentials)
C. Consumer mediated sharing from health system to BA (via SMART on FHIR)

FTC-governed aggregator (no BAA in place with health system)

D. Consumer mediated sharing from health system to non-BA (via patient credentials)
E. Consumer mediated sharing from health system to non-BA (via SMART on FHIR)

It is wrong to have our data stored and transmitted inappropriately when we choose, in good faith, to share our data. It is damning when we don't have a choice; when our data has been transmitted to a poorly secured API without our opt-in or consent.[4]

We ask the HL7 Policy Advisory Committee (PAC) to forward this letter, along with our recommendations, to the appropriate government authorities.

Recommendation 3: Include non-happy path security testing in ONC Inferno and ONC-ATL testing
To: ONC (Inferno, ONC-ATLs)

Many of the discovered vulnerabilities are common OWASP Top 10 vulnerabilities. For example, allowing authenticated patients to access data from other patients (i.e. the APIs were not checking authorization). All the guidance in the world is for naught if there aren't easy to use and accessible tests for developers.

ONC has two powerful tools at its disposal to catch security vulnerabilities before they reach production, ONC Inferno and ONC-ATL.

For ONC Inferno, the test suite is focused on the "happy path" of "can you interoperate", and not on "are you secure" - beyond the "can you successfully connect with TLS, OAuth, etc." We recognize that many consumer-directed APIs will not undergo ONC certification, meaning ONC Inferno could be the last line of defense between a development vulnerability and production.

For ONC-ATLs, we ask ONC to extend their certification process to include some fundamental security testing. For consumer-directed apps (not a covered entity, not a business associate) self-certification of adherence to basic security principles should be encouraged. For covered entities, business associates and EHRs, these self-certifications should be mandatory.

---

[4]https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html

Recommendation 4: Review the FHIR community responsible disclosure process
To: ONC

White hat hackers are powerful allies to patient security and privacy. ONC and HL7s policies 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.

Emerging industry codes of conduct address responsible disclosure in theory,[5] but not practice. Options for facilitating the transition to practice include:

- Requiring that ONC approved APIs have a responsible disclosure policy
- Incorporating HL7 Security responsible disclosure guidance by reference into codes of conduct
- Publishing a model responsible disclosure process tailored to healthcare aggregators

These options are not mutually exclusive, and would work in concert to ensure responsible disclosure, when – not if – vulnerabilities are discovered.

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

Patients should not need to be technical experts to understand whether their health data is being responsibly shared. Nor should patients be left to trust that a nonprofit regulatory body and voluntary codes of conduct are adequate to address this regulatory gap, when bad actors will not follow or seek codes of conduct.

Consider establishing an optional certification (and labeling process) for patient apps.

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.

Consider suggesting that Patient Access API Servers label, or otherwise visually indicate the "trusted" 3rd-party application versus "untrusted" application; for example, showing positive badges for CARIN Trust Framework and ONC vetted applications. To promote adoption, CMS could clarify that this labelling does not constitute information blocking, since patients can still choose to share their data with an untrusted application (that, for example, has not attested to privacy and security best practices).

---

[5] For example, the CARIN Code of Conduct includes a breach notification clause
> 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.

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: Enhanced penalties for breaches by TPOs
To: HHS OCR

Breaches by these TPO (Treatment, Payment, and Health Care Operations) BAA entities are therefore more egregious than breaches where the patient's opted-in.

Patient-driven governance and input are needed when HIPAA covered entities ship patient data over to their business associates, who in turn implement poorly secured access. This is a "worst of all worlds" scenario where the services are insecure and patients don't have any say about whether their data is exposed as part of the mix, because patients didn't opt in.

Recommendation 9: Prioritize enforcement of the health breach notification rule for aggregators
To: FTC

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 or Business Associate.

The term "Aggregator" is not well defined. A working definition is "any party that runs a business and collects clinical data from multiple sources." Aggregators collect information by two pathways.

1. Moving data from a provider to an aggregator under HIPAA BAA, where provisions like treatment, payment, and operations support this kind of sharing without a patient's authorization as long as there's a Business Associate Agreement in place. This sharing pathway is governed by HIPAA and Business Associates have obligations just like covered entities (to protect the data, to notify in the case of breaches, etc). The technical means of transfer could be a database export, or an HL7v2 message feed, or FHIR APIs, or anything else.
2. Moving data from a provider to an aggregator would be HIPAA's patient right of access, where a patient instructs a healthcare provider to share. This can involve technologies like FHIR APIs for patient access.

Note that not all patient facing apps should be considered "aggregators"; for example, Common Health or Apple Health store your health data on the device without it being transmitted remotely or "aggregated" with anyone else's data.

When both pathways "could" apply, the BAA route takes precedence. If an app is offered by or on behalf of a covered entity, even if the technical route of data exchange is a FHIR patient access API, the app still needs to have a BAA in place and is still governed under HIPAA.[6]

We request that you i) work closely with HHS OCR, and ii) prioritize enforcement of breach notification within FTCs regulatory authority.[7]

Recommendation 10: Build capacity for end-to-end, shift left security.
To: CISA

Someone needs to be taking an end-to-end approach to security. At present it seems like we are pursuing an "arms and legs" approach - individual pieces are looking at their own security needs, but no one is looking at the problem end-to-end

CHANGELOG

v1 2021-10-21	Ryan M Harrison
v2 2021-10-22	Andrea Downing Ryan M Harrison integrating comments from • @Brent Zenobia • @John Moehrke • @Josh Lamb • @Lloyd McKenzie

[6] See Q5 from this FAQ
[7] FTC Health Breach Notification Rule enforcement announcement