DRAFT

Statement on enhancing patient privacy and security without compromising the patient's right of access

Email

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

The five recommendations included have reached consensus within the Patient Empowerment Working Group (PE WG). We're working on additional, in progress recommendations, which we may send to the PAC after they have reached consensus within the PE WG.

Letter

From: HL7 Patient Empowerment Working Group
To: HL7 Policy Advisory Committee (PAC)
2021-10-25 v3 (DRAFT)

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: Hacking and Securing FHIR APIs" report

On 13 Oct 2021, vulnerability researcher Alissa Knight released a report entitled "Playing with FHIR: Hacking and Securing FHIR APIs."[2] Briefly, the report covers her white hat penetration testing of patient-directed FHIR servers and clients. She finds numerous common (OWASP API Security Top 10[3]) security vulnerabilities in the implementations of FHIR servers and FHIR mobile apps (most commonly, data aggregators). While unfortunately common, these security vulnerabilities expose sensitive patient information to unauthorized users. Detailed analysis is available elsewhere.[4]

---

[1] Patient Empowerment Working Group: Mission and Charter

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

[3] OWASP API Security Top 10: https://owasp.org/www-project-api-security/

[4] Reputable analysis 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
- Sean Noland LinkedIn Post: Untitled

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

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 pretext 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 security framework: policy guidance, standards guidance, real world implementation testing, a penetration testing guide, and finally coordinated disclosure and breach notification.

Security vulnerabilities in FHIR implementations should not be used as a rationalization to block patient access, or otherwise undermine the information blocking rules.

All of Ms. Knight's vulnerability findings were discovered in data aggregators -- third-parties providing patient access to their own data pulled from the EHR systems of the healthcare providers.

Patient data is covered under two distinct regulatory regimes, HIPAA and non-HIPAA. HIPAA entities are subject to enforcement by HHS OCR. Non-HIPAA entities are subject to enforcement by the FTC. Within each regulatory regime, there are a number of ways to share data, briefly…

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

A. Direct sharing from health system to BA (Business Associate)
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)

There is an expectation by patients that the confidentiality and integrity of their data is maintained when they choose, in good faith, to share their data with third-parties. .[5]
Per contra, when healthcare providers share patient data with third-parties without that patient's consent, there's insult to injury when the result of that transfer is the siting of that patient's data in a less secure, more vulnerable data lake. As evidenced by Ms. Knight's report, this lack of regulatory requirements around security and privacy on third-parties has created an expanding attack surface where vulnerabilities leading to unauthorized access of patient data is ubiquitous.

As you will notice in this letter: there is a patchwork of Privacy Policies in our current regulatory landscape. The very fact we need to have different sections speaking to ONC, CMS, HHS, FTC, and all of the states shows how complex our current system is when protecting sensitive health data for vulnerable patient populations. Patients are harmed by this non-coordinated effort: this chaos enables abuse of patient privacy in the gaps of our regulatory patchwork, and prevents failures from being enforced as the bodies presume other agencies are covering the gaps.

FHIR is a technology enabler for the patient's right to access. Implementation vulnerabilities should be remediated and risks treated to an acceptable level, but should not be used to undermine access to patient data.

Recommendations

Recommendations to ONC

Recommendation 1: Include application penetration testing in ONC Inferno and ONC-ATL (Authorized Testing Laboratories)
To: ONC (Inferno, ONC-ATLs)

Many of the discovered vulnerabilities in Ms. Knight's report are common OWASP API Security Top 10 vulnerabilities. For example, allowing authenticated patients to access data from other patients (i.e., OWASP API Security Top 10 API1:2019: Broken Object Level Authorization).

ONC has two powerful tools at its disposal to identify security vulnerabilities before they reach production, ONC Inferno and ONC-ATL (Authorized Testing Laboratories).[6]

For ONC Inferno, much of the test flows are seemingly more angled towards interoperability than actual security testing for different tactics and techniques used in breaching APIs.
We recognize that many consumer-directed APIs will not undergo ONC certification, meaning ONC Inferno could be the last line of defense between a vulnerability being exposed in development versus production.

---

[5]https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html
[6]While we focus this recommendation on ONC Inferno and ONC-ATLs, note that ONC also maintains a separate security assessment tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

For ONC-ATLs, including in their already required real-world testing, 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.

Recommendation 2: Contribute to the FHIR community's coordinated disclosure process
To: ONC

Security researchers are powerful allies to patient security and privacy. ONC policies should facilitate the responsible notification and correction of security vulnerabilities. While individual vendors should have their own coordinated vulnerability disclosure procedures,[7,8] including publishing advisories or assigning CVE (Common Vulnerabilities and Exposures) identifiers, ONC has an important coordination role to play.

Emerging industry codes of conduct address coordinated disclosure in theory,[9] but not practice. Options for facilitating the transition to practice include:

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

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

Recommendation 3: 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.

For example, consider including the following items into the ONC Certification and 3rd Party Attestation:

- FHIR Safety Checklist
- OWASP Top-10 Vulnerabilities
- Code of Conduct, e.g. the CARIN Code of Conduct

---

[7] https://vuls.cert.org/confluence/display/CVD
[8] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRST-Multiparty-Vulnerability-Coordination.pdf
[9] 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.

Recommendations to CMS

Recommendation 4: Create guidance for Patient Access API 3rd-party app onboarding, consent screens and trust labels.
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.[10,11] 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).

Recommendations to FTC

Recommendation 5: Prioritize enforcement of the health breach notification rule for PHR Vendors & 3rd party aggregators who are not covered by HIPAA
To: FTC

HHS OCR (Office of Civil Rights) 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.

---

[10] Note that CMS's Promoting Interoperability Program already requires regular security risk assessments, see: https://www.cms.gov/files/document/security-risk-analysis-fact-sheet-12-10-20.pdf
[11] While not specific to consent and trust labels, the HL7 Consumer Mobile Health Application Functional Framework (CMHAFF) provides guidance and context for best practices for Health applications, see: http://www.hl7.org/documentcenter/public/standards/dstu/HL7_CMHAFF_R1_STU_2018JUN.pdf

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.[12]

We appreciate the FTC's historical enforcement actions against unresponsive vendors.[13,14] We request that you begin to i) work closely with HHS OCR, ii) take enforcement actions against unresponsive aggregators, and iii) otherwise prioritize enforcement of breach notification within FTCs regulatory authority.[15]

[12] See Q5 from this FAQ
[13] https://www.ftc.gov/enforcement/cases-proceedings/terms/249
[14] https://vuls.cert.org/confluence/display/CVD/6.2+Unresponsive+Vendor
[15] FTC Health Breach Notification Rule enforcement announcement