October 27, 2021

Dear HL7 Community,

On October 13, a white paper authored by Alissa Knight of Knight Ink, LLC was posted on Twitter. The author is considered to be a cybersecurity expert in penetration testing of APIs and applications.

The white paper, which we encourage everyone to read, can be downloaded at https://approov.io/for/playing-with-fhir/ and represents a continuation of a project that previously pointed out vulnerabilities in mHealth and telemedicine in the United States, a topic which should concern us all.

The white paper’s eye-catching title, “Playing with FHIR: Hacking and Securing FHIR APIs”, has led some casual readers to infer that FHIR and FHIR APIs are being faulted. With considerable diligence, the author painstakingly makes clear in the opening paragraphs and throughout that no vulnerabilities were found in the HL7 FHIR standard itself nor were any found in FHIR-based APIs from the EHRs that she tested.

Instead, the author explains that the vulnerabilities lie with the implementation of apps and by third-party FHIR aggregators. Recognizing that the title of the paper was being misinterpreted, she has since changed it to “Playing with FHIR: Hacking and Securing FHIR API Implementations.”

As such, the report makes a strong case for the new HL7 Standards Implementation Division, which is being created specifically to address concerns like these, as well as providing testing capabilities, reference servers and other resources for implementers.

As Alissa notes in her paper, “the weakest link in the security of FHIR API implementations is the last mile between the user and clinical data aggregators.”

In the coming weeks HL7 will be issuing additional statements regarding the findings of this white paper, the concerns it raises, and what can be done to implement safe and secure FHIR APIs.

For further information, please contact Wayne Kubick, HL7 International CTO.