National Coordinator Micky Tripathi
Office of the National Coordinator for Health Information Technology
Mary E. Switzer Building
330 C. St SW, 7th Floor
Washington, DC 20024

Administrator Chiquita Brooks-LaSure
Centers for Medicare & Medicaid Services
Hubert H. Humphrey Building,
200 Independence Avenue, SW Room 445-G
Washington, DC 20201

January 5, 2022

National Coordinator Tripathi and Administrator Brooks La-Sure,

On behalf of the undersigned organizations, we request both The Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS) review the security and vulnerability flaws of Fast Healthcare Interoperability Resource (FHIR) based application program interfaces (APIs) identified by the Health Information Sharing and Analysis Center (H-ISAC)[1] and reevaluate the FHIR API polices outlined by both ONC and CMS. We appreciate the opportunity to raise these concerns and hope you will consider taking the necessary action to allow the healthcare community additional time to assess these risks and determine a path forward.

Our letter and the H-ISAC's alert comes in response to a widely viewed white paper *Playing with FHIR* released by Approov[2]. The white paper makes, and the H-ISAC has endorsed, five recommendations to secure FHIR based APIs now and into the future. Those recommendations include:

1. Allowing the use of sheilding solutions to ensure only legitimate applications and users can communicate with the APIs, with the goal of cutting down on unauthorized utilization of the API keys. The use of this would protect sensitive personal data from exfiltration and address vulnerabilities.
2. Updating information blocking rules to explicitly allow service providers and vendors to utilize security assessment mechanisms (like control reviews and pen testing).
3. Mandating the implementation of certificate pinning for FHIR mobile apps.
4. Allowing FHIR API owners to:
    - Assess the configuration of third-party apps prior to allowing them access to the environment;
    - Implement API threat management solutions, and
    - Incroporate pen-testing performed by a third party.
5. Allowances for apps and devices to be authenticated with SDK-powered solutions using a token for the API request.

Based on public communications from ONC, and in discussions with our respective organizations, we believe several of these recommendations are not allowable under the information blocking regulations. Providers are thus left in the vulnerable position of being unable to ensure the security of patient health data. Moreover, electronic health record (EHR) vendors are explicitly prohibited from taking necessary steps to review apps' FHIR data privacy and security controls prior to allowing API access to patients' medical records. Several of our organizations noted this concern in our comment letters to ONC on its information blocking proposed rule back in 2019.

[1] https://health-isac.cyware.com/webapp/user/myfeeds/de3d5038
[2] https://approov.io/for/playing-with-fhir/

The fact is that exploiting critical vulnerabilities in third-party FHIR APIs, and the resulting breach of medical records, will not be blamed on the app developer itself. Instead, the blame will fall on the provider. Even though a provider may not be subject to costly HIPAA breach penalties as a result of such breaches, they would still incur significant reputational damage from a perceived mishandling of patient data. That damage is not just to the business reputation but can also damage clinician-patient trust, which is crucial to optimal patient care. Additionally, determining whether an app has appropriate security (and privacy) will place a significant burden on physicians and other providers, who are likely unequipped to make this determination or provide patient education on app security.

With these facts in mind, we are asking ONC and CMS to reconsider the requirements currently in place for the delivery of the FHIR APIs by EHR vendors and the use of that technology by providers. Most notably, ONC must update its guidance to explicitly allow providers or EHR vendors the opportunity to review app and third-party software prior to its connection to a FHIR based API to ensure the security and privacy of patient data. Until this guidance can be updated or clarified, we ask ONC and CMS to utilize enforcement discretion related to the information blocking and FHIR APIs allowing providers and EHR vendors to act in good faith with the information currently available to them to protect patient data.

The undersigned organizations continue to fully support the work ONC and CMS are doing to put patients in control of their data. This should not, however, come at the expense of patient information security and privacy or with a significant increases in administrative burden for physicians and other providers. Patients must have confidence in who is handling their data. Likewise, trust between providers and patients must be maintained and strengthened. We have worked steadfastly with our members/clients and the federal government to educate providers on information blocking. We now ask for the government's help to protect patients and their valuable health data.

To discuss this letter in more detail or schedule time to meet with these organizations collectively please reach out to atomlinson@chimecentral.org.

Sincerely,

American Academy of Family Physicians (AAFP)
American Health Information Management Association (AHIMA)
American Medical Association (AMA)
College of Healthcare Information Management Executives (CHIME)
Medical Group Management Association (MGMA)