33 W. Monroe, Suite 1700
Chicago, IL 60603
swillis@himss.org
Phone: 312-915-9518
Twitter: @EHRAssociation

April 29, 2016

Michelle Consolazio
Federal Advisory Committee Act (FACA) Program Director
Office of the National Coordinator for Health Information Technology
US Department of Health and Human Services

Dear Ms. Consolazio,

On behalf of the Electronic Health Record Association, we appreciate the work of the joint Health IT Standards and Policy Committees' (HITSC and HITPC) API Task Force to establish a comprehensive set of considerations and recommendations that address the privacy and security challenges as the consumer-focused application programming interface/application (API/application) ecosystem interacting with EHRs emerges. We also appreciate the opportunity to provide further feedback on the draft recommendations presented at the April 19 joint HITPC and HITSC meeting.

Statements of Support

Following are a number of areas that we specifically want to call out as important recommendations that we support.

Endorsement or Certification

We strongly support the notion to avoid requiring centralized certification or testing of applications, and rather to rely on the market and various stakeholder groups to inform the consumer about applications that are worthy to use or that should be avoided. The Federal Trade Commission's (FTC's) authority to address false claims and/or data breaches should be adequate until there is clear evidence that further levers are required.

Code of Conduct and Privacy Notice

We appreciate the recommendation to encourage consumer-facing application developers to adopt a code (or codes) of conduct, and strongly support the value of a privacy notice that clearly indicates to a consumer how their data will or will not be used.

Identity Proofing and User Authentication

We agree that the requirements for identity proofing and user authentication should be consistent with those already required through the 2015 certification edition for view, download, and transport. We suggest clarification that consistency in process

should not be interpreted as requiring or implying that applications are expected to (or must) access APIs through a provider's patient portal.

Suggestions for Enhancements

The following points address important recommendations that deserve further consideration to establish a practical and viable API/application ecosystem.

API Access Suspension

We agree with the recommendations that API providers may suspend API access when the application is found to be in conflict with the technical specifications and terms of service. However, further clarity is needed as to what provider responsibilities or authorities to act are when known misuse of data occurs within an application connected to a provider's APIs (e.g., when the patient wishes to stop the application from using their data but the application does not, or when data is used contrary to the application disclosures without the patient's knowledge, or the application can cause clinical or other harm to the patient).

The Task Force recommendations do indicate that the patient should be able to override a suspension, unless the application poses a threat to the provider's health IT or violates allowable terms of service. It is unclear what circumstances could lead to a suspension that do not fall into either of these categories, and that a patient should have the ability to override, and we ask for such clarity.

Delineation of Data Responsibilities

In the context of our comments on API access suspension, as well as in response to the discussion topic on infrastructures that involve intermediaries between an EHR and the consumer's application using the data obtained, we want to highlight the need for clarity regarding the point at which the data is considered under consumer control (thus subject to limited/no HIPAA guidance) versus the provider's control. For example, an application that is made available through the provider that can be plugged into the provider's patient portal (thus co-located with other provider assets), versus an application accessing the EHR independent from such patient portal versus an application obtaining the information through an intermediary aggregator (thus located outside of a provider's HIT infrastructure). Where does the provider's responsibilities and HIPAA applicability stop?

A suggestion was made that these challenges may be easily addressed through a HIPAA business associate agreement (BAA), but Task Force members appropriately indicated that a BAA applies to a party associated with the provider, not a party working on behalf of the consumer. Understanding the point at which the data is considered to have left the responsibility of the provider in these various configurations will help set providers' and consumers' expectations about managing protected health information (PHI). It is critical for consumers to understand what responsibilities they have to maintain their data that cannot be passed back to providers and/or software developers, as well as what responsibilities a provider has when an application causes harm to the patient (e.g., misuse of data against their disclosure preferences, or other questionable data use).

We request that Task Force recommendations for the Office of Civil Rights (OCR) and the FTC more clearly seek clarification regarding delineation of responsibilities between providers and consumers and also that these agencies put in place appropriate consumer education programs to raise awareness and set expectations.

Specifically, the Association also suggests that ONC clarify that, while API providers may impose security-related restrictions on application access, it is inappropriate for API providers to set limitations on what a patient-authorized application can do with data downstream.

Registration Process

We recognize and appreciate the need for easy registration of new applications that a provider can enable for their consumers. To the extent that applications fully adhere to the API's technical specifications, we agree that such registration can be readily accomplished without having to go into what the application actually does with the data. However, to support easier registration and provide the expected level of data access, while maintaining the integrity of the data for which the provider has responsibility, some form of validation testing of the application's adherence to the API's technical specifications could help reduce and protect against any unexpected performance or general data exchange challenges. Such validation testing by the provider and/or API developer should be permissible, including adjustments to support processes to accommodate untested applications.

Cost and Fees

We understand that cost and fees structures are appropriately out of scope of the work of the Task Force. Consequently, we suggest that recommendations and assertions on fees for registration and access (e.g., Use Case Topic 2 recommendations) are beyond the charge of the API Task Force and should not be the subject of recommendations. More generally, we are unclear why ONC should address this topic.

Data Category Level Access

We would like to address a challenge that has arisen with the implementation of the 2015 edition requirements: whether it is required to have only one API or multiple APIs to access all or part of the Common Clinical Data Set (CCDS). We understand through updates to the Certification Companion Guide (page 5) for the API access criteria that either approach is allowed and therefore no preference for either approach should be expressed. We therefore suggest that the Task Force (and ONC) clarify throughout the recommendations that one or more APIs can be needed to access a patient's health information, data category data elements, or the full CCDS to avoid the impression that a single API must be provided.

Additionally, we want to note that Motivation for Limited Scope language indicates that, *"Specifically, our recommendations focus on read only access to a single patient's record for disclosure to an application selected by that patient, and used to access data elements defined in the Common Clinical Data Set."* Considering that the 2015 certification edition has three criteria around APIs – (g)(7) patient selection, (g)(8) data category request; (g)(9) all data request – we suggest referencing all three aspects, not only the data element or data category request.

Future Scope: Write APIs

As the scope of the Task Force's charge explicitly did not include write-APIs, and the primary focus was on read-APIs, we suggest that ONC follow up to address write-API security and privacy considerations shortly after the API Task Force completes its current charge. The industry is already moving toward write-APIs as well as ensuring that the audit logs necessary to support the read-APIs effectively involve writes to health IT as well. A number of challenges highlighted in the recommendations are amplified in deploying write-APIs (e.g., responsibility of providers managing the integrity of data, the impact of applications and potential need to suspend access from applications that do not meet the technical specifications, the need for validation testing to ensure data is represented correctly in the health IT).

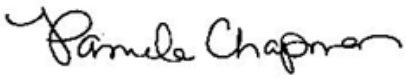
Again, on behalf of the EHR Association's member companies, we applaud this effort by the joint HITSC and HITPC API Task Force to address the privacy and security challenges related to the accelerating adoption of consumer-focused applications and APIs, and the impacts on the entire health IT infrastructure. We look forward to working with ONC and other stakeholders to address these challenges.

Sincerely,

Leigh Burchell
Chair, EHR Association
Allscripts

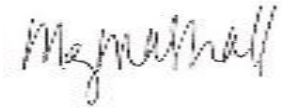
Sarah Corley, MD
Vice Chair, EHR Association
NextGen Healthcare

HIMSS EHR Association Executive Committee



Pamela Chapman
e-MDs

Richard Loomis, MD
Practice Fusion



Meg Marshall, JD
Cerner Corporation

Rick Reeves, RPh
Evident

Richard Landen
QuadraMed Corporation

Sasha TerMaat
Epic

About the EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of over 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehrassociation.org.