33 W. Monroe, Suite 1700
Chicago, IL 60603
Phone: 312-915-9582
Twitter: @EHRAssociation

January 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:

We appreciate the importance of understanding the privacy and security concerns and risks, as well as other barriers for consumers, as the industry takes on the newly emerging class of application programming interface (API) technology that has the potential to further expand consumers' access to their data and, potentially consolidate access to stimulate consumer engagement in their healthcare. Greater access in and of itself will most likely not translate to greater engagement. The access needs to be valuable, private, secure, convenient, and supported by value added functionality to actually engage consumers. The EHRA supports the API Task Force of the joint HIT Policy Committee (HITPC) and HIT Standards Committee (HITSC) addressing this topic, and offers the following for consideration as the API Task Force is formulating its recommendations.

Responsibilities of API consuming applications (APPs), APIs, and consumers/users: While the main focus of the API Task Force is on the APIs themselves, consumer engagement is actually realized in the API-consuming Applications (APPs) that the consumers will use to access their data. The APPs are the endpoints that enable access to and use of the data/capabilities the API exposes. We therefore suggest it is important to recognize the difference between:

- APIs that expose data and capabilities of the applications they are built on;
- Clients or applications (APPs) that leverage these APIs to provide consumers with better access to their data.

Consumers will mostly interact with the APPs and less so with the APIs. Therefore, the considerations around privacy and security should not only focus on the APIs and their ability to maintain appropriate protections, but also on the APPs' ability to appropriately protect consumers' data with clarity for the consumer about the risks involved.

APPs also will have accessibility and capability considerations that will influence the success of API investment and resultant consumer engagement. Note that those

issues will further vary based the target users of the APPs. For example the capabilities and privacy and security considerations for an API used by APPs supporting patients and their proxies may differ from those considerations where the APP supports users such as providers, payers, researchers or other health professionals.

Many of the emerging and envisioned APPs used by consumers are not subject to HIPAA, as consumers have the right to share data as they see fit. Developers may not even be aware of the privacy challenges involved in accessing and sharing patient data. However, being aware of the risks and having the appropriate tools available to manage data sharing is as important for APPs as it is for APIs and the applications to which they provide access.

Recommendations:

- Recognize the difference between APIs and APPs and address recommendations on how to consider privacy & security across both individually and together in support of consumer engagement.
- Emphasize education for consumers that clarifies not only their rights, but also their obligations on how to manage data sharing to avoid unexpected proliferation of their data.
- Provide education and guidance for APP developers about what privacy, security, and patient safety capabilities are appropriate to incorporate to help ensure the data obtained through the APIs is shared with the appropriate, intended user.
- Require clear documentation on data access and sharing capabilities of the APPs to enable consumers to understand how the data is managed by the APPs.
- To ensure the right data is provided to the right user type (e.g., patient or proxy) , the API must have the ability to prevent suspicious APPs from using the API and/or constrain in the API's Terms of Use the user types allowed to access the API. Such prevention, control, and/or constraint cannot be considered information blocking. This identifies the need for APPs to be evaluated carefully by the API service provider and/or a recognized third party before it can utilize the APIs or otherwise be blacklisted. Under all circumstances, API service providers must have the right to appropriately certify/authorize/register APPs that can interact with that API service without fear of being labeled as information blocking.

User identity, identity proofing, user-to-patient linking, patient relationship linking, and consent/PHI handling:

As APIs and APPs proliferate, the need for unique patient identification, user credentialing, APPs, and APIs, as well as record location services, will increase beyond even today's clear needs to ensure a consumer can get reliable and appropriate access to their data across different providers. The consumer must be able to correctly map to the respective patient records within and across providers' health IT, while providers must be confident that they share the data with the correct person or their authorized representative. The industry must, therefore, address the following challenges:

- Identity servers – Who provides them, and how do we trust them? What impact does proliferating identity servers have? Will providers and consumers trust existing identity servers, or does the healthcare industry need to stand-up their own identity servers?
- Identity proofing – How do we ensure the person or APP accessing the API is in fact who they say they are and accessing the API on behalf of the right person(s)? Identity servers only establish user identity. Identify proofing is essential to know that user identity belongs to the right human being.
- Identity and patient linking - an APP user, even a proofed user, may not have a patient identity, consistent patient identity, patient-relationship identity. All of these are required for clear identification and authorization.

- Consent and PHI management – When the API is not only available to consumers but also providers/payers/researchers/other professionals, how is consent managed and applied? How can users who are not the patient access a patient's data in accordance with the appropriate consent and HIPAA constraints? Where are rules applied and enforced for consent, data type handling, sensitive data handling, de-identification, patient age, etc.? These are also all dependent on user type, role, patient-relationship, etc.
- Directories – Where is data located for a consumer? What is that data and how is it expressed? How are providers contacted to access the data? An APP may know it is connected to five APIs, and the API knows the instance of an EMR it reflects; but the patient only knows that they had an appointment in Dr. Jones' office. How are those items rationalized for intelligent and efficient data return, data aggregation, and data isolation that will influence value assessment?

There will be many challenges to get to broad adoption of APIs and APPs by consumers. The challenges involve the many certified APIs as a result of 2015 Edition certification and MU Stage 3 objectives; each with their own approach to handling these requirements including use of varying or no standards; provider challenges in 80% threshold achievement; and therefore the overall value of the API capabilities and associated APPs. The EHRA believes of all these challenges the identity proofing is one of the most important challenges to address and clearly involves the API, the APP, and the user.

Recommendations:

- Establish guidance and process standards on how to perform identity proofing and clarify the responsibilities of APIs, APPs, and users to ensure data is shared with the right user.
- Establish a trust framework for APPs to ensure APPs are what they claim to be and can be trusted by APIs to manage the data for the right consumer according to their expectations.

Standards

While formulation of standards is out of scope for the task force, we recommend that the task force emphasizes the importance of standards in its recommendations. Standards not only establish basic building blocks for data exchange through those APIs (e.g., FHIR resources, vocabulary bindings), but also for the secure transport of the data and guidance on security practices for both the API and the APPs.

Impact on Existing Meaningful Use Program Objectives

Considering the challenges outlined and the efforts necessary to address these, we are concerned that the Meaningful Use Stage 3 objectives/measures that call for providers to make APIs available for use by their patients (or APPs on their behalf) will be challenging to achieve.

Recommendations:

- We suggest that the API Task Force recommends to CMS to reconsider its Meaningful Use Stage 3 targets for use and deployment of APIs such that progress can be made in that space, yet the goals are not insurmountable for many providers needing to ensure data is accessed by the intended consumers.

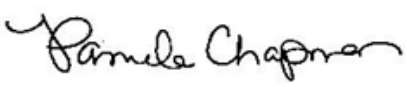
We appreciate the opportunity to provide these comments to the API Task Force for consideration. We would like to highlight that, while the primary focus is on consumers using APIs directly or indirectly to access their data held by providers or other record keepers, we suggest that the use of APIs raises the same questions and challenges when providers are the users of the APIs to access data for their patients in another provider's EHR. The EHRA continues to work on this topic and would like to provide further input over the next few weeks on additional points.

Sincerely,

Leigh Burchell
Chair, EHR Association
Allscripts

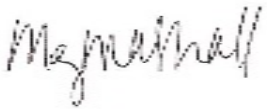
Sarah Corley, MD
Vice Chair, EHR Association
NextGen Healthcare

HIMSS EHR Association Executive Committee



Pamela Chapman
e-MDs

Richard Loomis, MD
Practice Fusion



Meg Marshall, JD
Cerner Corporation

Rick Reeves, RPh
Evident

Ginny Meadows, RN
McKesson 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.

CC:
Karen DeSalvo, MD, MPH, MSc, National Coordinator for Health Information Technology and Acting Assistant Secretary for Health