HiMSS Electronic Health Record Association

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

February 22, 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:

As indicated in our letter of January 29, 2016, we offer the following additional suggestions as a follow-on comments and recommendations in that letter. To aid in your considerations, we organized our commentary into those that we believe must be addressed immediately, while others can be addressed in subsequent review cycles. As stated in our earlier comments, we appreciate the importance of understanding the privacy and security concerns, risks, and barriers for consumers as the industry takes on the newly emerging class of application programming interface (API) technology that has the potential to stimulate consumer engagement in their healthcare. The Association supports the API Task Force of the joint HIT Policy Committee (HITPC) and HIT Standards Committee (HITSC) addressing this topic, and offers the following additional input for consideration as the API Task Force is formulating its recommendations.

Most Pressing Challenges

Infrastructure, Standards, and Testing

We are concerned that the current combination of standards, infrastructure, and identity-proofing processes are either not widely adopted and/or are inadequate to fully support a reliable, secure API/application (APP) environment where the consumer can confidently access their data. We note that portals currently deployed under the EHR Incentive Program have experienced many of these challenges that were overcome through establishing and/or arriving at common standards (e.g., exchange, accessibility, logging) and establishing processes for user provisioning, identity proofing, etc. Such standards, processes, and infrastructure are not yet in place nor commonly accepted for APPs. As APPs evolve and emerge, such experiences must be considered, recognizing that API servers and APPs are analogous in nature to portals. We do agree with assertions made that APIs are not inherently more or less secure than other technologies. However, they add further complexity and challenges given their deployment environment. To this point, centralized deployment has made the challenges more manageable for portals (although leading to one portal per provider); but more decentralized and proliferated use of APIs and associated APPs provides another level of complexity and challenge, while having the clear promise of improved access for patients.

We appreciate the clarifications that the Office of Civil Rights (OCR) recently provided as to whether APPs are subject to HIPAA or not; and that security failures at the APP are not the responsibility of the disclosing party or system (i.e., the API). We must re-emphasize though that the disclosing party or system still has responsibility to ensure the data is shared with the correct destination and patient. Specifically, with regard to identify proofing, providers play an integral role in the identity proofing process to enable access to portals. The question is, how will this scale in the new APP ecosystem? Using existing identity proofing approaches in the current APP ecosystems outside of healthcare may sound appealing, but may not enjoy the same level of trust to support one's health data.

More work is required to address these concerns. This needs to occur in a learning, non-punitive environment.

Recommendations:

- Consider how the banking industry addressed identity proofing, having strong engagement by the banks themselves and using identity proofing solutions specific to the banking industry.
- Providers must be encouraged to be part of an identity proofing process that can take advantage of the identity proofing already occurring for insurance coverage.
- Recognize the responsibility of providers to protect the confidentiality, integrity, and accessibility of patient data, and the need to mitigate risk from malicious applications and users. Providers need the ability to adopt mitigation processes including blocking and/or registration of applications based on acceptable levels of risk a provider is willing to accept.
- Recognize that, in the process of ensuring data arrives at the intended destination, it may be necessary to prevent data from being consumed by particular APPs. Such "blocking" cannot be considered information blocking.
- Establish a trust framework for APPs, akin to Direct Trust for Direct messaging, that can also establish a directory of trusted APPs. Such a trust framework, which can be validated by an independent party that API service providers can rely on, should initially focus on APIs and APPs that involve:
  - the Common Clinical Data Set (CCDS) as defined in the 2015 Certification Edition final rule;
  - and the Mobile Health Document query and retrieve with CCDA 2.1.
- Consider a set of characteristics that APIs and APPs should disclose that enable providers and consumers alike to understand the security profile that it supports. For example:
  - Is your APP intended to be accessed by the patient and proxy only? Or can the provider access a patient's data through this APP as well?
  - Is your user/identity server identity-proofed?
  - Is your data stored in the APP secured? Encrypted?
  - Others questions will surely arise during these considerations.
- Raise the need for discussion on what policies and standards APP developers should consider as part of best practice development guidance to improve the consumer experience so they understand how their data is and is not used.
  - Encourage APP developers to adopt a code of conduct.
  - Encourage APP developers to have audits/activity logs for support.
  - Consider accessibility and usability considerations applied to APIs.
  - Clarify what parameters may be used to "throttle" excessive access patterns.
  - Consider incident management and breach handling as those processes apply to APPs.
  - Address which body will have jurisdiction in sanctioning an APP that does not manage the data in accordance with its claims or otherwise causes data breaches. Is that a role for FTC? ONC? Other?

- Consider such disclosure approach for portals as being sufficient to maintain consistency across the various technologies enabling access to one's data.
- Recognize the need for APIs to support standards that enable APIs to adjust data access based on characteristics provided by the APP. We note in this context that, ultimately, there is a trust level that is required of the APP to support this, thus requiring a need to independently verify adherence to an APPs declared privacy/security policies and the ability to blacklist those APPs found not to adhere to their declarations.

State Variances
The introduction of APIs and APPs is likely to further emphasize the need to address interstate harmonization of privacy and security policies. What policies is an APP supposed to follow if it interacts with API services that are situated in multiple states accessing one consumer's health records?

There is increased clarity on the patient's right to access their information, noting the recent guidance from ONC and updates to Clinical Laboratory Improvement Amendment (CLIA) regulations, including the right to get such data potentially before a provider has received them. However, there is ambiguity on the provider's right to determine what is in the best clinical interest of the patient regarding when to share what data. Until such ambiguity has been clarified, it will be challenging for APIs to support both patient and provider rights, and may create situations in conflict with these rights regardless of the best intentions for withholding or sharing data.

Recommendations:
- Continue the drive towards harmonized privacy and trust frameworks across all 50 states and territories.
  - Framework consistency to ensure that constraints provided in different "domains" can be bridged.
  - Operational deployment to enable a consumer to define consent once with nation-wide applicability, and be ensured that it will be enforced by all API services where his or her data is available.
- Recommend ongoing dialog through OCR and states to continue to clarify patient as well as provider rights to enable APIs to support these rights appropriately.

Consent and Intermediaries
Current 2014 and 2015 Edition certification criteria have encouraged proliferation of portals that require consumers to use multiple portals to access their data across multiple providers. APIs offer opportunities for APPs to aggregate data from various providers into one view that a consumer can use to manage their health data access. Several approaches to intermediaries facilitating access to multiple sources should be considered ranging from:
- Locator: a simple data locator approach, identifying the target address of API services where a specific patient has data;
- Aggregator: consumer-focused data aggregators with various data access capabilities and consumer-focused presentation of data;
- Data Analyzer: cross-patient anonymized statistical data collection and analysis.

These introduce different degrees of challenges in ensuring that these intermediaries are subject to consumer consents expressed at the national level.

Locators, aggregators, and data analyzers are expected to be major users of the APIs on behalf of consumers, as well as APPs extending single EMR capabilities through available APIs.

Recommendations:

- Emphasize the need for core API standards to enable both types of API uses: EHR-specific API services and cross-EHR locators, data aggregators, and data analyzers, for consumer as well as provider use.
- Clarify the need for education to API developers, intermediary providers, APP providers, and users (patients, providers) on their responsibilities concerning identity proofing, consents, and data sharing practices.
- Establish criteria and policies that can enable an API to assert that the APP has correctly expressed a patient's consent.

Responsibilities of APPs, APIs, and consumers/users)

In our January 29, 2016, letter to this task force, we made suggestions on the need for providers/vendor of APIs to prevent suspicious APPs from accessing the API in specific circumstances. We would like to further that discussion and suggest the need to develop an agreed-upon set of principles and/or criteria that are the basis on which an APP can be restricted access to an API. We consider this particularly relevant in the context of the discussion on dynamic registration. We suggest that further discussion as well as practical experience needs to inform the extent to which full dynamic registration does not adversely impact the need to ensure the API is used by or for the patient (or their representative), and does not unduly impact a provider's health IT infrastructure (e.g., excessive or unnecessary API calls). We also note that any notion of certification or a seal of "good housekeeping" is contrary to dynamic registration.

We note that portals have higher levels of trust since they are certified. APPs do not require HIPAA compliance and, as long as APPs are not certified, they will represent a lower level of trust. If the intent is to establish the same level of trust as with portals, disclosure, identity proofing, and blacklisting must be considered.

Recommendations:

- Establish best practice administrative policies template to support particularly smaller providers to manage API access.
- Recognize that, as, patient-focused APIs evolve from read-only to write as well, the complexity of access and data management gets increasingly more complex.

Ongoing Discussions

Patient Matching

During the API Task Force hearings that notion was raised that introduction of APIs will virtually eliminate the patient matching challenges as the patient is now in control. We strongly urge the API Task Force to maintain a strong focus on the need to resolve fundamental patient matching challenges that APIs with APPs under a patient's control will not resolve. While clearly, depending on the API's capabilities, patient's data can be aggregated into a single view, it still requires identity proofing and matching with each individual source. Additionally, as data is being requested from different sources on behalf of a patient, matching to the right sources will remain the same challenge as it is today. APIs will solve some patient matching issues, but will also further highlight the urgency to resolve patient matching at a more fundamental level that yields near-perfect or perfect matches.

Recommendations:

- Reinforce the need to resolve patient matching challenges as deployment of APIs will further contribute to the patient matching burden, considering the least amount of data (e.g., unique patient identifier) to minimize burden on the patient (or their representative).

Portals vs. APPs

As addressed earlier, portals are very similar to APPs, other than the ownership (provider vs. consumer). While this variance results in a different set of certain privacy and security requirements (e.g., ability to disclose information to other parties), it is unclear why it was asserted in the hearings that portals are closed and APPs are open. Per the 2015 Certification Edition Final Rule, both must provide access to the same Common Clinical Data Set (CCDS), while a portal that is to be certified must be able to allow the patient or their representative to share that data with any party they wish (transmit in view, download, transmit (VDT)). This is not a requirement for APPs, nor will APPs be required to offer APIs to be accessed by other APPs, whereas the CEHRT enabling the portal is. We suggest that the HITPC API Task Force should not propagate the characterization of portals being closed and APPs being open.

To Be or Not to Be an API

It is important to understand that interoperable data exchange covers a variety of methods and standards. In that context, it is also important that we look at refining our definition of what an API is. It has been proposed that an API may be any method of exchanging data, such as messages, documents, web services transactions, and many more. Vendors should be able to function with a reasonable expectation of standards that need to be supported. This is necessary in order to develop appropriate security policies and make the API readily available to those who need access to it.

In that context, we suggest that the privacy and security considerations being discussed in the API Task Force are not restricted and considered unique to certain types of APIs, but applicable across the variety of possible API approaches. They are fundamental principles of how to exchange data in a predictable, reliable, secure environment that supports the consent requirements of the patient, and in compliance with HIPAA disclosure considerations. This would enable a single privacy and security framework that can be supported regardless of the specific form an API may take, while specific techniques and standards may vary based on the specific API technology deployed.

Recommendations:

- Recognize there are differences of interpretation and that varying standards and technology apply to particular API, while the tenants of privacy and security must apply equally across all.
- Clarity on the various meanings and aspects of APIs is needed, although, not within the charge of this Task Force. In particular, it is important that one distinguishes and relate three levels of API definitions:
  - API in a conceptual sense. This relates to the use case or service provided by the interface, defined in non-technological/standards dependent manner (e.g., data element-based query for clinical health information, core data set or query for documents within a specific health information exchange domain).
  - API in aspects that are technology/standards specific in health IT (e.g., Blue Button, FHIR-based Restful query, MHD/FHIR based document query).
  - API in aspects that are technology/standards specific in generic IT (e.g., SOAP-based web services, Restful-based web services, e-mail messaging).

Sustainable Business Model

We are concerned that the business model for deploying the infrastructure to support this new ecosystem is not clear. That is., who will bear the costs and pay for the APIs, APPs, and various infrastructure to sustain that ecosystem? Currently, APIs are being developed to meet 2015 Certification Edition requirements, but there is uncertainty as to when we will have common, standard APIs and broad uptake of APPs. Considering the discussions on information blocking and the cost of interoperability, premature regulatory actions to address these challenges, while encouraging proliferation of non-standard APIs in the new ecosystem, may have adverse effects on innovation and, therefore, the growth of this emerging opportunity for consumers to access their data. The current trajectory may unfortunately yield one APP per provider, similar to one portal per provider in today's 2014 Certification Edition environment, thus not solving the consumer data access challenges.

Recommendations:

- Recognize the need to learn and find practical business models that can sustain the necessary access, and provide such learning in a non-punitive environment. Avoid being prescriptive upfront.
- Foster pilot programs and approaches outside of regulatory action to learn what is practical and useful, yielding consumer friendly, valuable solutions.

On behalf of the more than 30 member companies of the EHR Association, we appreciate the opportunity to provide these comments to the API Task Force. The Association continues to work on this topic and looks forward to our ongoing collaboration.

Sincerely,

Leigh C Burchell

Leigh Burchell
Chair, EHR Association
Allscripts

Sarah C. Corley MD, FACP

Sarah Corley, MD
Vice Chair, EHR Association
NextGen Healthcare

HIMSS EHR Association Executive Committee

Pamela Chapman

Pamela Chapman
e-MDs

Richard M [illegible] MD

Richard Loomis, MD
Practice Fusion

Meg Marshall

Meg Marshall, JD
Cerner Corporation

Rick Reeves, RPh
Evident

Ginny Meadows

Ginny Meadows, RN
McKesson Corporation

Sasha TerMaat

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