HIMSS Electronic Health Record Association

Electronic Health Record Association (EHRA) Response
Application Programming Interface (API) Task Force Recommendations
October 2016

Introduction

On May 12, 2016, the Office of the National Coordinator for Health IT's (ONC's) Health IT Policy Committee and Standards Committee API Task Force issued its final recommendations on privacy and security considerations for the emerging consumer-focused application programming interface (API)/application (App) ecosystem.

The Electronic Health Record Association (EHRA) provided input to the recommendations through public comments and is pleased that a number of those recommendations have been included. Overall, the API Task Force did a commendable job within its charge to identify key challenges and provide practical approaches to addressing these challenges.

While the charge and scope primarily focused on APIs and API developers, we are very pleased that the API Task Force included considerations about the Apps that consume the APIs. We urge ONC to always consider both API and App requirements at the same time, as only together will they create a successful, patient- focused, health data access ecosystem.

The purpose of this paper is to review the final recommendations and express our support for certain recommendations, while offering opportunities for improvement to ONC when it begins to address the API Task Force's recommendations. In this review, the EHRA identifies a number of important gaps that were beyond the scope of the Task Force and remain to be addressed before a smooth deployment of interoperability between Apps and APIs can be expected:

- Topics listed as out-of-scope, and that have to be addressed for a successful API/App ecosystem:
    - Appropriate and inappropriate content of an API provider and developer Terms of Use.
    - Fee structures, deemed out of scope per the report, were still addressed but without full consideration of the implications of the suggestions. The suggestions included in the report short change the complexities of this topic in the context of viable business models and practical infrastructures. We request that these suggestions be set aside until this aspect can be addressed more adequately with better grounding to set realistic expectations.
    - Formulation of standards is essential to consistent re-use and access across health IT.

- Need to identify a first level of support between the API developer and the App developer before engaging a consumer complaint process at a national level.

- Need to address API experiences with App developers.

- Educating patients on the dos and don'ts when selecting Apps will go a long way toward establishing a healthy API/App ecosystem, which goes beyond the topics in the recommendations. For example:
    - How to get insight into App capabilities and limitations – where to get data on App capabilities, reviews, endorsements, etc.
    - What are terms of use of the App – is data disclosed to other parties or for other purposes?
    - Where to go for complaints?
    - What are patients' responsibilities?

- Clarification of the registration, approval, and data access steps is essential as current definitions do not provide clarity, and these steps as defined do not address the full development and deployment life cycle. For example:
    - Purpose, need, and opportunity for API/App validation is not sufficiently addressed continuing to raise concerns with deployment of insufficiently tested Apps impacting consumer and provider satisfaction.
    - Self-service registration vs. dynamic registration should not both be required.

- Clarification on asynchronous access on behalf of the patient requiring the App to fully disclose this to the patient.

- Clarifications on the registration service listing all running instances as this could be interpreted too broadly imposing unnecessary requirements.

- Clarifications on where the provider responsibilities stop and the patient responsibilities start, particularly when the provider may actually deploy the consumer App within the provider's infrastructure.

- Clarifications on the App's responsibilities in managing access to a patient's data, not just the API.

- Clarifications on the accounting for disclosures use has to address that reporting of disclosures to a patient is not limited to using a provider's portal, and delineate the role of an App in reporting on disclosures considering that providers (thus APIs) already have disclosure requirements but would not know what an App is doing with the data once it gets it.

- Clarifications for Apps on breach notifications that may not necessarily involve HIPAA, but would be considered by the Federal Trade Commission (FTC) or other agencies.

- Considerations on how providers and payers can collaborate on identity proofing.

Detailed Review

We found the document's organization – structured around the generic use case from API registration through an App's use of the API – very helpful in exposing the current landscape, findings, and recommendations. We organized our comments and considerations by section header as used in the API Task Force's recommendation document to provide easy cross-reference.

Scope and General Support

We appreciate the need to have an initial focus on critical aspects of API/App privacy and security. However, we note that without the industry addressing a number of the topics listed as out-of-scope, a successful API/App ecosystem is not attainable. For example:

- ***Terms of Use***
  Terms of use would benefit from agreement on minimum expectations and clarification on when terms of use may be considered information blocking, as opposed to appropriate constraints to maintain privacy, security, and acceptable performance characteristics. This should address not only an API developer's terms of use, but also a provider's terms of use that may be layered on top of the API developer's terms of use. Particularly for providers, a starter template for terms of use could provide clarity on the intent and create more consistent terms of use without restricting relevant local variations.

- ***Fee Structures***
  While the fee structure was determined to be out of scope, the recommendations still included considerations relative to fee structure aspects (e.g., free registration or increasingly low transaction fees). We suggest that without an appreciation of the necessary infrastructure to provide the desired access, such statements set unrealistic expectations, and we urge ONC to set these recommendations aside. We do not believe at this point that there is sufficient experience to reference which indicate that legislative or regulatory action is required.

- ***Formulation of Standards***
  The industry (i.e., the Argonaut project and Integrating the Healthcare Enterprise (IHE) IT Infrastructure) is currently working on clear definitions of FHIR-based API standards (more specifically, profiles and implementation guidance) in support of:
  - The Common Clinical Data Set (CCDS). However, the initial roll-out of APIs will not be able to take advantage of those profiles and guidelines. API developers will use their best estimates of what those profiles and guidance may look like or use variant approaches. Consequently, App developers will likely have to deal with variations, both small and large, in API technical specs for the same CCDS data elements. We anticipate this will take at least two to three releases of the "CCDS on FHIR" specifications, as well as the underlying FHIR standard, and associated uptake by API developers before the desired consistency across EHRs has mostly been achieved.
  - Document-level access standards will be necessary to properly address an API access on the full set through a C-CDA document. We anticipate this will be done using mobile access to health documents (MHD), a FHIR-based IHE profile to retrieve documents

sometimes called “XDR or XDS on FHIR.”

We agree that for the API aspects that were within scope, the deployment of APIs addressing ONC’s 2015 Certification Edition criteria should not raise any “show-stopping” barriers. However, we are concerned that those items that were considered out of scope will raise barriers as highlighted above.

Oversight/Enforcement

We support the need for patients to have a clear place and process to register complaints with the Apps that they choose to use or for App developers to address complaints with the APIs they rely on for data access. We are concerned, however, that Recommendation 2), bullets 3) and 4), may be interpreted as having one national location for any and all App complaints and, similarly, one for API concerns. We suggest that the complaint process should have at least two stages. The first stage would provide the App developer with clear support channels for the patients using their application(s) (similarly, for API developers to App developers); and, a second stage to provide access for patients to App developers who are perceived not to live up to their terms of use and stated support commitments (similarly, for API developers). It would be inappropriate and unnecessary for the government to get into the business of managing support channels across all Apps and APIs.

We suggest that such clarity around support responsibilities between API developer, provider, and App developer must be aligned with clarifications on what constitutes information blocking, appropriate use of App endorsements and/or support deficiencies, as well as an appreciation of appropriate identity-proofing process steps to ensure the user using the App is the intended patient or their representative.

We were disappointed that the recommendations only address issues related to patients’ experiences with Apps, and App developers’ experiences with API developers. We suggest that equally important is the need for clarity on where API developers should go when App developers are not responsive to concerns when violating the terms of use, or where providers should go when API developers or App developers are not fulfilling their contracted or stated obligations. We note though that there is less of a need to address the provider-API developer relationship as this is already well established since providers started using health IT many decades ago.

Topic 1 – Types of Apps and Organizations Who Provide Them

We appreciate the need to clarify what criteria a provider or API developer can apply to applications that a patient wishes to have connected to their provider’s certified EHR technology (CEHRT). However, we are concerned that stating that the only relevant concerns are technical compatibility and patient choice is shortsighted and does not sufficiently educate providers, and particularly, patients on their choices. We suggest that education needs to cover these topics, plus a number of topics that were out of scope. For example, clarifications are needed on:

- How to get insight into App capabilities and limitations – where to get data on App capabilities, reviews, endorsements, etc.
- What are the terms of use of the App – is data disclosed to other parties or for other purposes?
- Where to go for complaints.
- What are patients’ responsibilities?

Educating patients on the dos and don'ts when selecting Apps will go a long way in establishing a healthy API/App ecosystem.

Topic 2 – App Registration

App registration is an important area to address to ensure that expectations of both App and API developers are clear, while facilitating smooth processes and patient experiences in connecting their Apps to their provider's CEHRT. As highlighted in our earlier comment letters to the API Task Force while developing their recommendations, we remain concerned regarding the rights of the API developer to help ensure Apps connected to their APIs conform to the technical specifications and terms of use. We believe that the API Task Force conclusions are incomplete until consideration is given to a more narrowly defined App registration or take-on process (e.g., is the "App approval" referenced in Recommendation 3.b App developer-focused, patient-focused, part of registration, or not? Where could testing occur?). We are concerned that critical aspects of connecting an App to an API have been incorrectly omitted from consideration.

Recommendation 2.c indicates that registration is not the place where Apps undergo rigorous testing, but does not address testing of Apps against APIs anywhere else in the document other than suggesting ONC should not require centralized certification or testing in Recommendation 3.c. However, an important step in software development and deployment is adequate testing of the applications, particularly when connecting to other applications beyond the developer's control.

We are concerned that the recommendations do not take this sufficiently into consideration. In particular, API developers should be allowed, but not required, to put reasonable testing protocols in place to ensure Apps interact appropriately with the APIs. We note that App stores (e.g., Apple, Google, and Microsoft) include varying degrees of testing requirements to ensure proper interaction with their operating systems. This approach should not be ignored.

While we believe API developers need to have the opportunity to introduce these steps as part of the take-on process of an App to access a provider's APIs, API developers are well advised to make their APIs as "bulletproof" as possible. But, even then, testing is essential to create a seamless patient experience. Reasonable testing procedures should not be considered information blocking.

Topic 8 introduces the notion of an approval step, but the scope of such a step is not fully clarified in the recommendation (i.e., is it just patient-focused, or also App-focused?). We suggest that App approval by the provider for the App to connect with an API should be part of the registration. Generally, these steps should be more fully defined to provide clarity on what is covered and what may still be a gap.

We suggest that APIs should not be required to support both self-service registration and dynamic registration. Rather, these should be considered best practice recommendations where an API developer can choose to support one, the other, or perhaps even another method.

It is not clear how much a provider or API developer can inform a patient when the App is known to have challenges in correctly connecting with an API, or to not use data in accordance with their stated terms of use of the data. We suggest that providers and API developers should be able to provide a patient with such information to assist the patient in making informed decisions.

Recommendation 2.e addresses applicability of a fee structure for registrations. We note that fee structures were placed out of scope of the Task Force's charge and are better addressed in the context of a larger discussion on the infrastructure necessary to maintain the emerging API/App ecosystem. At this time in the evolving API/App ecosystem, we do not see a need to address this topic as no systemic issues have come up requiring legislative or regulatory action.

Topic 3 – Endorsement/Certification of Apps

We generally support the recommendation that there is no need for a central certification or testing process, coordinated by ONC, for Apps. However, as indicated in Topic 2, we strongly believe in the need to allow, but not require, API developers to subject Apps to a testing regimen before they are allowed to consume APIs.

Recommendation 3.b raises questions:

- Is the intent to define endorsement criteria that are then only used by others to evaluate and score Apps?
- Or, is the intent that each entity would itself score the Apps that are accessing its APIs?
- Or, even further, is it intended that the entity could restrict access to its APIs when an App does not score sufficiently on the criteria?

We suggest clarification that federal agencies are held to the same requirements/obligations to provide access to the APIs they expose. Consistency with the private sector enabling data access is critical, and the API Task Force should not inadvertently suggest different rules for private vs. public settings. We also suggest clarification that removal of an endorsement cannot be grounds for removal of the registration of an App to an API. However, it should be clarified that a provider may inform their patients that endorsement was dropped so patients can make informed decisions.

Topic 4 – Communication of App's Privacy Policies

We support all recommendations provided in this section, recognizing these are essential to create transparency to patients to support their making informed decisions.

Topic 5 – Patient Authorization Framework

We generally support the recommendations made here, but would make the following suggestions for clarification:

- Recommendation 5.b suggests disclosure whether the App is authorized to access the EHR asynchronously (i.e., when the consumer is not present). We note that the term "asynchronously" can be used in a variety of ways and causes confusion in this context. We assume, and would support, that the recommendation is that the App discloses that it may access the API when the patient is not logged into the application or actively using the application (e.g., daily refresh overnight).

Topic 6 – Limitations and Safeguards on Sharing

We offer the following considerations on this topic:

- One of the findings states, "*Secondly, a registration service which lists all of the running instances of these APIs would allow for a central point of control, registration, version management, and verification of running status,"* we note that this finding could be concerning if taken too broadly. We support the value of certain registration capabilities that may emerge where providers, patients, App developers, API developers, and other stakeholders have better insight as to what is available. It is unclear, though, what it would mean to have "a central point of control," "version management," or "verification of running status." While the API Task Force is not taking a position on this through a recommendation, which we appreciate and support, we would like to express concern that the implications of this finding requires considerable clarification and thought before any action is taken on this topic.

- In general, we suggest that ONC should not prescribe architectural approaches, nor give the impression that this topic is easy to address in terms of infrastructure.

- We understand and appreciate that HIPAA regulations and guidance secure the freedom of choice of the patient to use their data however they see fit. We suggest that clear guidance is further needed as to where the provider's responsibility under HIPAA stops. There is a particular area requiring clarity regarding the deployment options for an App. An App could be deployed in the cloud by the App developer, on a patient's mobile device, or within a provider's IT infrastructure. When in the cloud or within a provider's IT infrastructure on one of their servers, the App can be included as a SMART App within a patient portal. We seek clarity for each configuration as to when the provider is required to exercise all protections under HIPAA and when are they released of that responsibility.

- Considering the scenarios described in the prior bullet where a provider may actually be the service provider for patient-focused Apps, the provider should be able to be selective about which Apps to host based on their capabilities, data sharing policies, and other considerations, while not limiting the patients' rights to use an App of their choice that is hosted outside of the provider's infrastructure. Such guidance would be very helpful for all stakeholders.

- We suggest further clarification of the statement in Recommendation 6.d: "*ONC should update the HIT certification requirements to ensure API providers enable patients to share data with certain (coarse-grained, for now) limits, rather than "all or nothing.*" We already understand that APIs must make data available both at the individual CCDS data element level where reasonable grouping is allowed (e.g., patient demographics together rather than one API per data element) and all together. We are, therefore, not clear to what "all or nothing" refers.

- We also suggest further clarification of the statement in Recommendation 6.d: "*to make sharing decisions that restrict the scope of access.*" As APIs need to provide access to individual data elements, it appears to be largely up to the Apps to help the patient manage who does or does not get access to the data obtained, not just the API. The API does have responsibility to assess what the user is allowed to retrieve based on the patient's declaration on file regarding who can access their data. We suggest that these responsibilities need to be clearly addressed as part of patient education and outreach initiatives to ensure clarity about patient vs. provider responsibilities.

- Regarding recommendation 6.e, we believe that ONC's 2015 Certification Edition is already very clear on the need to share data at both the CCDS data element and aggregate document levels. We do support that managing access controls should not be more granular than these data elements, and that formal clarification that the CCDS demographic data elements can be grouped, is appropriate.

Topic 7 – Auditing and Accounting for Disclosures

We are concerned with the last bullet of Recommendation 7.a that states that the flagging process of potentially inappropriate disclosures should be electronically supported via the portal using accounting of disclosures mechanisms. While we understand the need for a patient to access a record of disclosures by the provider, the mechanism by which that is provided is not defined and may not involve a portal, nor is it clear what standard format should be used to provide that information to a patient. Furthermore, once the App has been authorized to access the APIs for that patient, it is unclear what the use case is for the API to maintain an audit log, beyond what the CEHRT in general needs to log, rather than the App that was authorized to access that data. The subsection on "HIPAA - Accounting of Disclosures" seems to support that. We, therefore, suggest that further definition of this use case is required to cover any disclosures, whether through APIs or otherwise, to address consistent reporting to the patient and subsequently address how patients can (electronically) report on inappropriate disclosures.

Regarding Recommendation 7.d, we believe that CEHRT and providers already have adequate guidance on how to address breach notifications in general, and under HIPAA in particular, whether it involves an API or not. Rather, the primary focus here should be on App developers and patients, as they are less familiar with the circumstances under which an event is considered a breach vs. authorized/permissible data sharing.

We suggest that potential challenges related to variations in state regulations, or perhaps lack thereof, that both APIs and Apps must take into consideration should also be addressed (e.g., when sharing/accessing data across state lines). We understand that once the patient has their data, there are no further constraints, HIPAA or otherwise, for the patient to use the data as they see fit.

Topic 8 - Identity Proofing, User Authentication, and App Authentication

We generally support the recommendations offered in this topic. These recommendations should evolve as they address complex challenges that need to be well understood by all stakeholders to ensure the right practical balance between privacy and security concerns and ease of access/authentication to address identity proofing and access to the appropriate data.

In addition to the identity proofing methods already in place to support view online, download, and transmit (VDT) capabilities for certification of EHR technology, it may be worth considering to what extent providers and payers can collaborate on common identity-proofing methods so one identity-proofing process can satisfy both requirements.

On this topic, the notions of approval and App approval time are introduced, indicating these may take minutes, days, months, if not years. We suggest that further definition of registration, approval, and data access would be beneficial, including what is addressed in each step and what reasonable expectations are for the time required. Further definition of this framework may address some of the concerns, where steps such as App to API testing and validation would fit, what to expect with identity proofing, and what would constitute information blocking versus reasonable privacy and security practices.

We note that Recommendations 8.f and 8.g underscore the need to clarify stakeholder responsibilities as further discussed in the oversight/enforcement section. In particular, regarding 8.f, we believe having a robust ecosystem that enables App reviews, disclosures, and endorsements can address concerns from patients, providers, and API developers alike on trustworthiness of Apps. Such an ecosystem can act in a more preventive manner, while oversight/enforcement focuses on corrective processes when things go wrong.

Other

The following are suggestions we made in earlier correspondence submitted by the EHRA in the first half of 2016, but that did not appear in any way in the final recommendations. We believe these remain deployment barriers and need to be addressed.

Consent and Intermediaries

Current 2014 and 2015 Certification Edition 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 EHR 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.

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 or no HIPAA guidance) vs. 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), vs. an application accessing the EHR independent from such patient portal vs. an application obtaining the information through an intermediary aggregator (thus located outside of a provider's health IT 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 the Office of Civil Rights (OCR) and the Federal Trade Commission (FTC) provide more 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.

Sustainable Business Model

We are concerned that the business model for deploying the infrastructure to support this new ecosystem is not clear. 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. The EHRA recommends:

- 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.