Health IT Joint Committee Collaboration

A Joint Policy and Standards Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

API Task Force

Meg Marshall, co-chair
Josh Mandel, co-chair

April 19, 2016

Agenda

- Introduction and Scope
- Discuss Draft Recommendations
- Action Items
- Workplan

Membership

Member	Organization	Role
Meg Marshall	**Cerner Corporation**	**Co-Chair**
Josh Mandel	**Harvard Medical School**	**Co-Chair**
Leslie Kelly Hall	Healthwise	Member
Rajiv Kumar	Stanford University School of Medicine	Member
Aaron Seib	National Association for Trusted Exchange	Member
Drew Schiller	Validic	Member
Richard Loomis	Practice Fusion	Member
David Yakimischak	Surescripts	Member
Aaron Miri	Walnut Hill Medical Center	Member
Robert Jarrin	Qualcomm Incorporated	Member
Ivor Horn	Seattle Children's Hospital	Member
Linda Sanches	*HHS Office for Civil Rights*	*Federal Ex Officio*
Rose-Marie Nsahlai	*ONC*	*ONC Lead*

Application Programming Interface (API)

Application Programming Interface (API) - a technology that allows one software program to access the services provided by another software program

- In its 2015 Edition CEHRT rule, ONC has included certification criteria for fully functioning APIs to support patient access to health data via view, download, and transmit (VDT).
- However, in discussing this concept in the proposed rule with our FACAs, *many members expressed concerns about privacy compliance and security of APIs.*

Therefore, the API Task Force was created to…

Task Force Charge and Questions

- **Identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in healthcare.**
  - » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example*, *identity proofing and authentication are not unique to APIs*);
- **Identify perceived privacy concerns and real privacy risks that are barriers to the widespread adoption of open APIs in healthcare.**
  - » For risks identified as real, identify those that are not already planned to be addressed in the Interoperability Roadmap (*for example*, *harmonizing state law and misunderstanding of HIPAA*);
- **Identify priority recommendations for ONC that will help enable consumers to leverage API technology to access patient data, while ensuring the appropriate level of privacy and security protection.**

Out of Scope Issues

- Terms of Use
- Licensing Requirements
- Policy Formulation
- Fee Structures
- Certifying Authorities
- Formulation of Standards
- Electronic documentation of consents required by law or policy
- Issues unique to write-APIs

Generic Use Case / User Flow for Patient-selected App

App Developer builds an app that can benefit from patient data. App Developer builds support for an API-based connection to EHR data, and registers App with Hospital A (or its EHR). Patient reviews App's data use and privacy policies (and features) and decides to connect App to her EHR data in Hospital A. Patient signs into Hospital A's portal, and Hospital A shows an approval screen. Patient agrees to share (some of) her EHR data for some duration of time with App, and Hospital A records this decision. Hospital A's portal sends Patient back to App, and App gets a unique, time- and scope-limited access token for this patient. App can use the token to access Patient's EHR data for some duration of time in keeping with the patient's approval.

Variants on Use Case

Personally-Controlled Health Record. For example, HealthVault. A site that stores information on a patient's behalf and makes it easily available.

Personal health app. For example, a tool to manage diabetes. This app could be discovered and selected by the patient, or recommended by a provider.

Patient-authored app. For example, a homemade tool to improve care coordination or plot lab results.

Rogue app. For example, an app specifically designed from the ground up to steal data from a patient for financial gain. Or a "good" app that has been hacked.

Discuss Draft Recommendations

Draft Recommendations- Topics

1. General support for APIs
2. Types of apps and organizations who provide them
3. Oversight (HIPAA- When does an app developer need a BAA?)
4. Registration Process (including "dynamic registration API" and "self-service registration“)
5. Process of Endorsement/Certification
6. How do Apps communicate their policies to users prior to sharing? (combined with Who’s In Charge if the Policies are Violated?)
7. Limitations and safeguards on sharing
8. Audit Trail and Recording Requirements (when a patient approves an app approval, and for subsequent API access)
9. Identity proofing, user authentication, and app authentication
10. Consent/authorization framework

Recommendations:

- ONC should continue its pursuit of an API strategy as an important mechanism for enabling patient choice and promoting a more efficient healthcare marketplace
- ONC should consider advice from this Task Force to mitigate privacy and security fears, and to provide an explicit framework that balances the risks and opportunities of a health API ecosystem
- The Task Force encourages ONC to collaborate with other agencies to offer guidance to app developers regarding best practices
- We recommend that ONC encourage OCR to develop guidance for covered entities and business associates*

**Details in Appendix C*

2. Types of Apps and Organizations who provide them

Findings:

- We heard from panelists across the industry who described various health apps that will likely participate in the ecosystem
- CEHRT/MU regulations do not differentiate based on who has written an app, or the app's purpose or credibility

Recommendations:

- ONC and CMS should explicitly state that the type of app, and the kind of organization who developed it, are not considerations with respect to a patient's right to access
- Relevant concerns = *technical compatibility* (works with the API technical specifications) and *patient choice*

3. Oversight

Findings:

- HIPAA status has downstream effects
- Not always clear to patient
- Relationships among HCOs and app developers can be complex- OCR's scenarios may not fit for all use cases

Recommendation:

- OCR should provide additional guidance to clarify whether a BAA is required in certain scenarios
  - (see Appendix Cfor Health App Use Scenarios)

Background:

Some technical protocols (e.g. OAuth) rely on a "registration" step that introduces the app to the API provider. This process generates identifiers that will be used later, when an app requests permissions. No patient data flows in this step.

In general, registration occurs between a "deployment" of an app and each API provider. So, between an app provider and a healthcare provider organization. EHR vendors may streamline this process by handling registration centrally.

4. Registration Process (cont.)

Recommendations:

- Ensure that app registration does not impose an unreasonable barrier to patient choice
- The registration process shall not impose delays. The registration process is not intended to be a point where apps undergo rigorous testing, clearinghouse approval, on-site inspection, or other "high bars" of control
- Self-service registration portals and dynamic registration protocols are two complementary ways to ensure frictionless app registration

Recommendations:

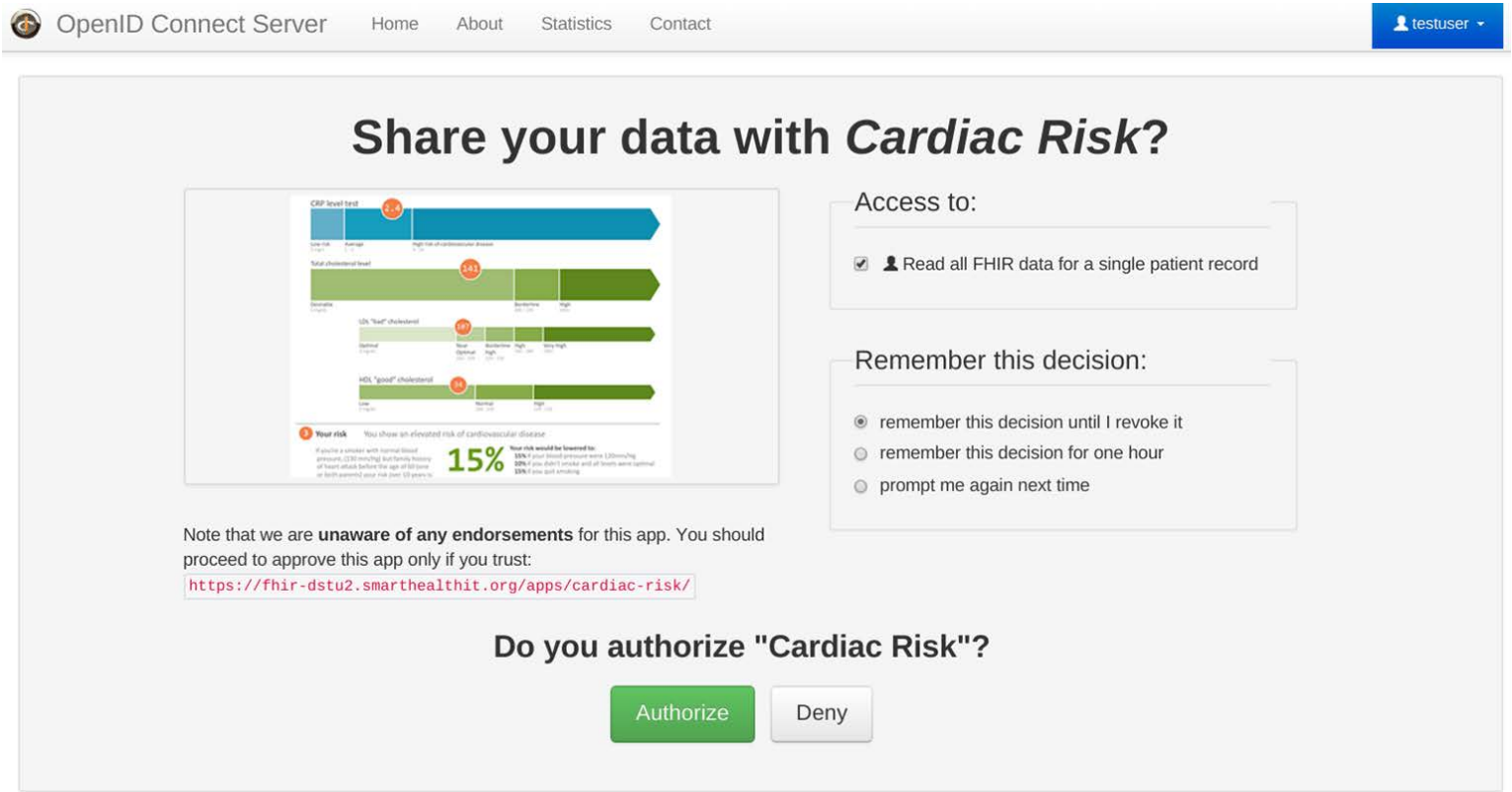
- ONC should retract its claim that existing certification criteria are "sufficient to allow access without requiring further application pre-registration," since this statement is out of line with real-world authorization protocols (e.g. OAuth 2.0) where registration is a requirement
- API providers must not charge a fee for the app *registration* process itself (and note that "reasonable" fees for *access* would be vanishingly low)
- ONC and OCR should specify how app developers should to report any "data blocking" issues with a provider's app registration process

Recommendations:

- ONC should avoid requiring any centralized certification or testing of apps. Instead, ONC should pursue regulations that enable a secondary market in app endorsements
  - In such a market, various kinds of organizations (EHR vendors; security experts; consumer advocacy groups; clinical professional societies; provider organizations, etc.) can "endorse" a given app through a distributed, publicly visible process, without centralized regulatory oversight
  - This approach to endorsements avoids the pitfalls of defining a centralized certification process and the difficulty of standardizing privacy policies, but still allows consumer-facing discoverability benefits

Recommendations:

- ONC should clarify that provider organizations must not use endorsements (or the lack of endorsements) as a reason to block the registration of an app, or to block a patient's ability to share data with an app



6. How do Apps Communicate their Policies to Users prior to Sharing?

Recommendations:

- ONC should encourage an app developer voluntary "Code of Conduct" that outlines best practices regarding how and what an app should communicate to consumers regarding its privacy and security policies
- ONC should support a Model Privacy Notice for app developers
  - Who is responsible for what; indemnification clauses
  - Standard definitions and terms
  - Privacy policies; notice of when they change
  - Meaningful controls such as opt-outs
  - Contact information
- ONC should provide guidance in its MPN for the minimum data set required for short form notices

7. Limitations and Safeguards on Sharing

Recommendations:

- ONC should clarify that while API Providers may impose security-related restrictions on app access, it is inappropriate for API providers to set limitations on what a patient-authorized app can do with data downstream.
- ONC should clarify that API providers are **not obligated** to protect patients by identifying "suspicious" apps.
  - API providers **may suspend API access** to an app that has breached the API provider's terms of service, or appears to have been compromised, or poses a threat to the provider's own system.
  - Patients must be able to override this suspension (unless a threat)
- Need clarification about where terms of service ends (between app and provider), and HIPAA begins; also where complaints should go.

7. Limitations and Safeguards on Sharing (cont.)

Recommendations:

- ONC should update the HIT certification requirements to ensure that API providers enable patients to share data with certain (coarse-grained for now) categories, rather than "all or nothing".
  - Patient should be able to view a provider-generated list of apps that currently have access to their records; revoke access at any time; and to make sharing decisions that restrict the scope of access.
  - Implementing many narrowly-scoped access control policies would require a costly and difficult re-design of existing systems.
  - Short term- we propose a pragmatic approach that ties back to the capabilities described in the 2015 CEHRT Certification Criteria: since CEHRT must already enable access through separate API calls at the data category level (e.g. medications, vital signs, or lab results).

8. Audit Trail and Recording Requirements

Recommendations:

- We recommend that ONC should require EHRs to make API access audit logs available to patients through an Accounting of Disclosures via the portal.
  - Show patients a list of outstanding authorizations in the portal.
  - Include the ability for the patient to revoke any outstanding authorization.
  - Show patients a list of which apps have accessed their data via API (including details like source IP, location, and scope of data accessed).
  - Inform the patient of the process to flag an authorization as inappropriate
- We recommend that ONC collaborate with appropriate stakeholders to provide guidance to app developers regarding best practices of audit capture.
- ONC should provide guidance around breach notifications rules and responsibilities.

9. Identity Proofing, User Authentication

Recommendations:

- ONC should provide guidance that the patient identity proofing and authentication requirements in an API ecosystem are not different from the requirements for MU2-era patient portal sign-in and VDT
  - Any process that presents a substantially greater burden to the patient for API access approval should be considered information blocking
- Standards like OAuth 2.0 should be used to allow patients to leverage existing portal account infrastructure as the means for approving access to an app.
- API providers must not impose patient identify-proofing or authentication barriers for API access that go beyond what's required for View, Download, and Transmit access.
- ONC should collaborate with the OCR and the FTC to provide clear and distinct API developer and API appropriate usage privacy and security standards in order to encourage API development and adoption.

Recommendations:

- For registering patient-authored apps, existing patient identity-proofing and authentication is sufficient:
  - Any patient who is able to sign into the portal of an API provider should be able to register any app that they chose with that API provider.
- For non-patient-authored other apps, ONC should clarify that identity proofing of developers must be non-onerous and automatable
  - i.e. Email address or domain verification would be reasonable; a review of tax records or inspection of facilities would not)

9. Identity Proofing, User Authentication (cont.)

Recommendations:

- ONC should further clarify that in situations where greater assurance is desired, app endorsements can achieve this assurance in a non-blocking, low-friction way without preventing registration of non-endorsed apps
- ONC should recommend that at approval and data access time, authenticating apps via standards-based mechanisms like OAuth 2.0 client authentication should be acceptable
  - Providers must ensure that app approval and data access can occur without active involvement from the API provider or app developer
  - The only person who should have to take action to approve an app's access to patient data is the patient (or representative)

10. Patient Authorization Framework

Recommendations:

- ONC should coordinate with relevant agencies to publish guidance, for the respective actors (app developer, patient, etc.), on whether sharing data with a consumer-directed application is considered to be part of an individual's access, access by a third party, or a tool for engaging in treatment.
- ONC should continue advancing work in support of standardized, machine-computable consent.
- ONC should coordinate a model authorization form with reusable/reference-able language and a standardized mechanism by which a patient can compare authorization requirements for two or more providers.
- Providers should include statements, typical of HIPAA authorizations, to notify patients of their rights to revoke app authorization, the role of the covered entity, disclosure of any provider relationships to apps, and HIPAA coverage.

10. Patient Authorization Framework (cont.)

Recommendations:

- Until clear guidance is available, providers should proceed to define their practices for EHR portals to ensure patients provide the essential information necessary for valid, informed go-ahead for the provider to enable consumer-directed app access to data.
  - The name of the patient whose records will be shared
  - The name of the app requesting information
  - The data categories the app is requesting access to (scope of permissions)
  - Whether the app can or cannot change information currently in the EHR.
  - Duration (expiration date)
  - Whether the app is authorized to access the EHR asynchronously (when the consumer is not present)
  - A representation of the individual's intent to complete the authorization (such as "Sign" "OK" "Complete" button)
  - When an app can be disabled by the provider

Action Items

- Refine draft recommendations
- Address outstanding comments and questions from the Task Force
- Agree upon form and format of final recommendations document and transmittal letter

Workplan

Meetings	Task
Apr 21, 2016 10:30am ET	API Task Force Call
Apr 26, 2016 10:30am ET	API Task Force Call
May 17 Joint Committee Meeting	**Present final recommendations to HITSC and HITPC**

Appendix A

2015 Health IT Certification Criteria – API Access

- ONC established new 2015 Edition criterion at § 170.315(g)(7) that requires health IT to demonstrate it can provide **a Consumer-facing** application access to the Common Clinical Data Set via an application programming interface (API)
- **At this time the Certification Criteria only requires Read-only APIs**
- Certification criterion is split into three separate certification criteria with each individual criterion focused on specific functionality to enable modularity and flexibility in certification
- The three certification criteria will be adopted at §170.315(g)(7), (g)(8), and (g)(9):
  - (g)(7) Application access—patient selection
  - (g)(8) Application access—data category request
  - (g)(9) Application access—all data request

https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-75

2015 Health IT Certification Criteria – API Access, cont.

- To be certified for the "API" criteria, three privacy and security criterion must also be met:
  - Section 170.315(d)(1) "authentication, access control, and authorization;"
  - Section 170.315(d)(9) "trusted connection;" and
  - Section 170.315(d)(10) "auditing actions on health information" or § 170.315(d)(2) "auditable events and tamper resistance."

https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-75

2015 Health IT Certification Criteria – 3rd Party Application Registration

- The intention is to encourage dynamic registration and strongly believe that registration should not be used as a means to block information sharing via APIs.[1]
  - Dynamic registration is that applications should **NOT** be required to pre-register (**or be approved in advance**) with the provider or their Health IT Module developer before being allowed to access the API.
- This is supported by the CMS Meaningful Use Stage 3 Final Rule
  - "Providers may not prohibit patients from using any application, including third-party applications, which meet the technical specifications of the API, including the security requirements of the API."[2]

1. https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technology-health-it-certification-criteria-2015-edition-base#h-102
2. https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications

CMS Meaningful Use Stage 3 Final Rule

- CMS included 2 objective in the Meaningful Use Stage 3 Final Rule [1], that references the use of APIs:
  - Objective 5: Patient Electronic Access to Health Information[2]
  - Objective 6: Coordination of Care Through Patient Engagement[3]
- CMS reiterates in these objectives that there are four basic actions that a patient (or patient-authorized representative) should be able to take:
  - View their health information;
  - Download their health information;
  - Transmit their health information to a third party; and
  - Access their health information through an API
- CMS believes that these actions may be supported by a wide range of system solutions, which may overlap in terms of the software function used to do an action or multiple actions, including facilitating provider-to-provider exchange as well as patient access
- CMS proposed for the Patient Electronic Access objective to allow providers to enable API functionality in accordance with the proposed ONC requirements in the 2015 Edition proposed rule

Appendix B

Virtual Hearings

- Virtual hearings for the Joint API Privacy and Security Task Force were held on January 26th and 28th, 2016
- Panelists were represented from across both non-healthcare and healthcare industries
- Written testimonies have been gathered
- Public comments have been gathered
- Analysis has been conducted to summarize common themes captured across the two days of testimony and discussion

Virtual Hearings, cont.

January 26th		January 28th		
Panel 1- Consumer Tech 1	**Panel 2- Consumer Tech 2**	**Panel 3- Healthcare Delivery**	**Panel 4- Health IT Vendors**	**Panel 5- Consumer Advocates**
David Wollman, PhD- NIST	Alisoun Moore- LexisNexis	Stanley Huff, MD- Intermountain	John Moehrke- GE Healthcare	Adrian Gropper, MD- Patient Privacy Rights (PPR)
Stephan Somogyi- Google	Evan Cooke, PhD- US Digital Service	Paul Matthews- Oregon Community Health Information Network (OCHIN)	Ted LeSueur- McKesson	Mark Savage- National Partnership for Women & Families (NPWF)
David Ting- Imprivata	David Berlind- Programmable Web	Sean Kelly, MD- Imprivata	Chris Bradley- Mana Health	Steven Keating- Patient Advocate/Consumer
Greg Brail- Apigee	Marc Chanliau- Oracle	Tim McKay, PhD- Kaiser Permanente	James Lloyd- Redox Engine	
Eve Maler- ForgeRock	Shue-Jane Thompson, PhD- IBM	Brian Lucas-Aetna		
	Gray Brooks- GSA			

API TF Testimony – Important Facts Shared on APIs

- API Resources can regulate how, when, and who uses the API
- APIs provide a well-documented. Popular way for organizations to share access to data and services with third parties, while maintaining strict security controls.
  - Clear and concise documentation is important for open standard APIs
- API is extremely precise and allows the opportunity for all the right levels of access and security, e.g. data granularity
- Technical solutions exist for technical problems
- Need consensus best practices to help secure the API
- Business & legal considerations may remain.
  - Does it matter if the discloser “owns” the PHI or not?
  - Provider liability and accountability for data usage and breach, even though OCR/ONC Fact sheets say a discloser is not liable for what a receiver does with data so long as the discloser discloses the data properly.

API TF Testimony – Consumer Perspective

- More Access, More Patient Control, More Engagement
  - A panelist indicated access to his data helped save his own life, and asked "why can't patients have access to more of their own data?"
- Choices should be given to patient, and patients are smart enough to make privacy & security choices that are right for them.
- Systems should account for diverse consumers:
  - some want personally to control every decision;
  - some want health information to move where it needs to go without
  - them having to manage that process.
- Transparent data practices are important for consumers
- Role of HIPAA in protecting consumer vs. protections outside HIPAA

API TF testimony – Healthcare Organizations, cont.

- Support for Open Standards-based APIs.
- Who do you trust? How do you know that person is accessing your system?
  - Need to verify identity of person accessing system, even through an app.
  - Need to verify that the app is operating on behalf of a verified person
  - Who is accessing and which apps are in use varies by role
    - Patient/individual/caregiver
    - Provider
    - Information systems administrator
- Long term, protections will be in place to allow for varying levels of access.
- Business and legal issues.

Appendix C

Health App Use Scenarios

Scenario	OCR Assessment: Is Developer a BAA?	Clarifications, assumptions and /or questions posed by the API task force.
OCR #1. Consumer downloads a health app to her smartphone. She populates it with her own information. For example, the consumer inputs blood glucose levels and blood pressure readings she obtained herself using home health equipment.	No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The consumer is using the developer's app to help her manage and organize her information without any involvement of her health care providers.	**Assumption**: API and app connect at the patient's direction No data flows back to the CE via the API
APITF #1a. Tweak on #1: Same app, but it now allows an opt-in feature to communicate PGHD data back to the CE via the API/App.	*(Need assessment)*	**Clarify**: Even with this tweak, the app developer is still not a BAA. **Rationale**: the app is not covered under HIPAA because there is no "PHI" until held by the CE

Health App Use Scenarios, cont.

Scenario	OCR Assessment: Is Developer a BAA?	Clarifications, assumptions and /or questions posed by the API task force.
OCR #2. Consumer downloads a health app to her smartphone that is designed to help her manage a chronic condition. She downloads data from her doctor's EHR through a patient portal, onto her computer and then uploads it into the app. She also adds her own information to the app.	No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. Instead, the consumer obtains health information from her provider, combines it with health information she inputs, and uses the app to organize and manage that information for her own purposes. There is no indication the provider or a business associate of the provider hired the app developer to provide or facilitate this service.	**Question**: If there was indication or fact that the provider had hired the developer does this change the relationship? **Clarify**: Providers will hire development efforts, and in many cases the only data movement is based upon the patient-approved, explicit API access. An app should only be governed under HIPAA when the data flow between the app and the CE is managed by the CE/BAA, like for example when the app is pre-populated with data. The simple act of hiring an app developer should not automatically mandate HIPAA governance.

Health App Use Scenarios, cont.

Scenario	OCR Assessment: Is Developer a BAA?	Clarifications, assumptions and /or questions posed by the API task force.
OCR #3. Doctor counsels patient that his BMI is too high, and recommends a particular app that tracks diet, exercise, and weight. Consumer downloads app to his smartphone and uses it to send a summary report to his doctor before his next appointment.	No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The doctor's recommendation implies her trust in the app, but there is no indication that the doctor hired the app developer to provide services to patients involving the handling of PHI. The consumer's use of an app to transmit data to a covered entity does not by itself make the app developer a BA of the covered entity.	**Clarify:** As in scenario #2, a commercial relationship with the provider and developer should not in itself mandate HIPAA governance.

Health App Use Scenarios, cont.

Scenario	OCR Assessment: Is Developer a BAA?	Clarifications, assumptions and /or questions posed by the API task force.
OCR #5. At direction of her provider, patient downloads a health app to her smart phone. Provider has contracted with app developer for patient management services, including remote patient health counseling, monitoring of patients' food and exercise, patient messaging, EHR integration and application interfaces. Information the patient inputs is automatically incorporated into provider EHR.	Yes, the developer is a business associate of the provider, because it is creating, receiving, maintaining and transmitting protected health information (PHI) on behalf of a covered entity. In this case, the provider contracts with the app developer for patient management services that involve creating, receiving, maintaining and transmitting PHI, and the app is a means for providing those services.	OCR #5. At direction of her provider, patient downloads a health app to her smart phone. Provider has contracted with app developer for patient management services, including remote patient health counseling, monitoring of patients' food and exercise, patient messaging, EHR integration and application interfaces. Information the patient inputs is automatically incorporated into provider EHR.

Health App Use Scenarios, cont.

Scenario	OCR Assessment: Is Developer a BAA?	Clarifications, assumptions and /or questions posed by the API task force.
APITF #5a. Tweak on #5: Imagine that the scenario is altered slightly, so that: ● App only receives data after the patient approves it (not automatically) ● App only sends patient-generated data back to the provider upon patient approval (not automatically) ● App uses the provider's open API to access data (no proprietary connection) ● Provider suggests the app (but doesn't "direct" the patient to use it)	*(Need assessment)*	**Question**: With these tweaks, does the app developer still need a BAA? We think the developer should not need a BAA, since it functions effectively like a consumer app from scenario #2. We're interested in highlighting the specific changes that make the difference. Are all four tweaks required to to change the assessment, or would the top two tweaks (requiring patient approval for all data flow) be enough?

Appendix D

General Support for APIs

Recommendation:

- We recommend that ONC encourage OCR to develop guidance for covered entities and business associates that:
  - Current administrative security measures should be reviewed for risks and vulnerabilities associated with API endpoints under §164.308(a)(1)(ii)(B).
  - Existing administrative procedures used in system activity reviews should be updated to include review of data passing through API endpoints, especially data indicating API exploits (e.g., finding an unusual number of requests attempted from a single IP address, on behalf of a single user, or originating from an unlikely geographic area in system logs, as required by §164.308(a)(1)(ii)(D)).
  - Audit subsystems should be augmented to include activity at API endpoints. §164.312(b) creates a responsibility to implement mechanisms that detect and record activity over APIs that transmit PHI. Similarly, §164.312(e)(1) will require the deployment of new technical measures to guard against unauthorized access of PHI through API endpoints. For example, covered entities and business associates may have to install commercial API management products, implement request data checking, and provide other safeguard mechanisms that protect against known API exploits.
  - How to respond to requests for data over an API endpoint that are too complex for regulatory reasons (e.g., implementing §164.524(a)(2) rules) or impractical over the chosen communication channel).
  - Review of existing breach procedures to include scenarios involving the unauthorized access of data accessed through API endpoints.

Appendix E

Use Case Technical Actors

Technical Actor	*Role*	*Operation*	*Rights / Responsibilities*	*HIPAA*
Patient	data requester	request Accounting of Disclosures (AoD)	no right for disclosures to self	Affected by HIPAA
		identify unauthorized access	no right for disclosures to self	
Provider (CE)	data provider	provide AoD	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	Regulated by HIPAA
		maintain audit records	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
		breach notification	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
EHR System	data custodian	generate audit records	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	Regulated by HIPAA
		maintain or forward audit records	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
		identify breach	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
EHR API Developer	not a CE or BA	provide read API functionality	meet FTC requirements	Not regulated by HIPAA.
			meet responsibilities as described in business contract	
EHR API Developer	CE or BA	provide read API functionality	meet responsibilities as described in business contract	Regulated by HIPAA
		generate audit records	meet requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
		maintain or forward audit records	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
		identify breach	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
App Developer	not a CE or BA	provide read operation	meet FTC requirements	Not regulated by HIPAA.

Use Case Technical Actors (cont.)

Technical Actor	*Role*	*Operation*	*Rights / Responsibilities*	*HIPAA*
App Developer	CE or BA	provide read operation	meet FTC requirements	Regulated by HIPAA
		generate audit records	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
		identify breach	meet legal requirements: HIPAA, HITECH, Meaningful Use, The Joint Commission, FIPPS, etc.	
API Provider	not a CE or BA	Distributor of the API used by apps to access healthcare data	meet FTC requirements	Not regulated by HIPAA.
API Provider	CE or BA	Distributor of the API used by apps to access healthcare data as service to CE	meet FTC requirements	Presumably regulated by HIPAA.
		generate audit records	?	