API Task Force Recommendations

Overview

Introduction

Application Programming Interface (API) refers to technology that allows one software program to access the services provided by another software program. In its 2015 Edition of Health IT Certification Criteria (2015 CHIT), ONC established new criteria at §170.316(g)(7) that requires certified health IT to demonstrate the ability provide a patient-facing app access to the Common Clinical Data Set via an API.

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

In parallel, CMS included two objectives in Stage 3 of the Medicare and Medicaid Electronic Health Record Incentive Program (MU3) that reference the use of APIs:

- Objective 5: Patient Electronic Access to Health Information.
- Objective 6: Coordination of Care Through Patient Engagement

These MU3 objectives specify basic actions that a patient (or patient-authorized representative) should be able to take in respect to the patient's health information:

- View, Download, and Transmit (VDT) to a third party
- Access through an ONC-certified API that can be used by third-party applications or devices to provide patients (or patient-authorized representatives) access to their health information, within 24 hours of its availability to the provider.

Scope

The API Task Force was created in response to concerns expressed to ONC about privacy compliance and security of APIs. The Task Force was charged with the following scope:

- 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, identify 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.

Motivation for Limited Scope

Ultimately, the task force focused on needs specific to MU3 requirements and 2015 CHIT. Specifically, our recommendations focus on *read-only access to a single patient's record for disclosure to an app selected by that patient, and used to access data elements defined in the Common Clinical Data Set*.

Other "out of scope" issues include:

- Terms of Use
- Licensing Requirements
- Policy Formation
- Fee Structures
- Certifying Authorities
- Formulation of Standards
- Electronic documentation of consents required by law or policy
- Issues unique to writing new data into the EHR
- Issues unique to annotating data in the EHR

The aggregate ecosystem of consumer-facing apps includes apps that interact with health care data in ways that are beyond this scope. We expect developers to innovate and provide enhanced functionality through API technology.

Task Force Approach

The Task Force held virtual hearings on January 26 and 28, 2016. Panelists were represented from across both non-healthcare and healthcare industries. The Task Force reviewed written testimonies and public comments, and conducted analysis to summarize common themes. Additional information regarding the hearings can be located in the Appendix.

General support for APIs

Like any technology, APIs allow new capabilities and opportunities and, like any other technology, these opportunities come with some risks. There are fears that APIs may open new security vulnerabilities, with apps accessing patient records "for evil", and without receiving proper patient authorization. There are also fears that APIs could provide a possible "fire hose" of data, as opposed to the "one sip at a time" access that a web site or email interface may provide.

In testimony, we heard almost universally that, when APIs are appropriately managed, the

opportunities outweigh the risks. We heard from companies currently offering APIs that properly managed APIs provide better security properties than ad-hoc interfaces or proprietary integration technology.

While access to health data via APIs does require additional considerations and regulatory compliance needs, we believe existing standards, infrastructure and identity-proofing processes are adequate to support patient-directed access via APIs today.

Recommendations

- We recommend that ONC address other use cases in the future when the work can be informed by the lessons learned from experience with these initial use cases. For example:
    - Patient-directed APIs with Write and Update access to EHRs
    - Patient-directed APIs that access multiple patients (for example, aggregation of populations of patients)
- ONC should continue its pursuit of an API strategy as one important mechanism for enabling patient choice and promoting a more efficient healthcare marketplace.

Regulatory Oversight and Enforcement of APIs

Background

Depending on its functions and intended use, an app may need to comply with several federal laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Federal Food, Drug, and Cosmetic Act (FD&C Act), the Federal Trade Commission Act (FTC Act) and the FTC's Health Breach Notification Rule (as directed by the American Recovery and Reinvestment Act of 2009). The Task Force agrees this is a complicated framework, and it is not always intuitive as to which law applies at any given time. It is difficult for providers and developers to fully embrace API technology when there is uncertainty as to their respective rights, obligations and liabilities.

Many of the discussions within the task force centered around the notion that the patient-directed app of our purview supports the patient's HIPAA right to access his/her own PHI from a Covered Entity, as required under HIPAA § 164.502. This could be characterized in several ways: 1) the individual requesting access to their information, 2) an entity designated by the individual to receive a copy of PHI (as part of the individual exercising his/her right to access PHI), or 3) the medium on which the individual requests that PHI be provided or transmitted (as part of the individual exercising his/her right to obtain a copy of PHI). Alternatively, the patient-directed app may also be characterized as a third party formerly authorized by the individual to receive PHI, or a tool for engaging the individual in treatment. Each of these scenarios creates challenges when attempting to determine oversight of an app's behavior - there is not one clear solution.

Until authoritative guidance is available, we predict providers will align compliance practices to support the patient-directed app as closely as possible with their existing paper- or EHR-based

practices, likely with a very conservative approach, to mitigate the risk of unauthorized disclosures of PHI and thus avoid possible sanctions and penalties. Continued ambiguity in compliance requirements may result in providers adding unnecessary complexity and burden to their practices, which ultimately may chill support for and overall adoption of patient-directed data exchange.

Findings

FTC Oversight

Recognizing that health app developers are often confused about which legal requirements apply to them, FTC launched an online tool[1] to help health app developers determine which federal laws may apply to their mobile apps called The Mobile Health Apps Interactive Tool. The tool is interactive tool, leading the developer through a series of ten short questions about the app's functions. Based on the developer's answers, the tool indicates whether the developer may need to follow any of the laws when creating or administering the app. Once a developer determines which laws apply, the tool provides hyperlinks to access each agency's guidance.

Unfair or deceptive

As outlined in recent testimony to the U.S. House Committee on Oversight[2],

> The FTC's primary authority is Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce. If a company makes materially misleading statements or omissions about a matter, including privacy or data security, and such statements or omissions are likely to mislead reasonable consumers, they can be deceptive in violation of Section 5. Further, if a company's practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be unfair and violate Section 5.
>
> The FTC's Section 5 authority extends to both HIPAA and non-HIPAA covered entities, though generally this authority does not reach nonprofit entities. The FTC Act is currently the primary federal statute applicable to the privacy and security practices of businesses that collect individually identifiable health information where those entities are not covered by HIPAA.

Reasonable and appropriate data security practices

The FTC has also used its Section 5 authority to bring enforcement actions against companies that fail to maintain reasonable and appropriate data security practices regarding consumer

---

[1] The tool can be accessed here: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

[2] https://oversight.house.gov/wp-content/uploads/2016/03/2016-03-22-Rich-Testimony-FTC.pdf

data, including health data.

Breach notifications

Pursuant to Section 13407 of the HITECH Act, the FTC's Health Breach Notification Rule[3] applies to vendors of personal health records and their third party service providers. Under the FTC Rule, companies that have had a security breach must: 1. Notify everyone whose information was breached; 2. In many cases, notify the media; and 3. Notify the FTC. FTC's Rule applies only to health information that is not secured through technologies specified by the Department of Health and Human Services. Also, the Rule does not apply to entities regulated under HIPAA. (In case of a security breach, entities covered by HIPAA must comply with the HHS' breach notification rule.[4])

FDA Oversight

Through guidance[5], FDA is focusing its oversight on mobile medical apps that present a greater risk to patients if they do not work as intended - specifically, apps that:

- Are intended to be used as an accessory to a regulated medical device; or
- Transform a mobile platform into a regulated medical device.

FDA intends to exercise its enforcement discretion for the majority of mobile apps, which pose minimal risk to consumers.

The FDA published guidance for effective cybersecurity management, which outlines recommendations that manufacturers should consider in order to protect patient information that may be stored on medical devices or transferred between wireless systems. The agency defines cybersecurity as "the process of preventing unauthorized access, modification, misuse or denial of use, or the authorized use of information that is stored, accessed or transferred from a medical device to an external recipient.

HIPAA Oversight

The HIPAA Rules apply only to Covered Entities and their Business Associates (Regulated Entities). When a Regulated Entity discloses PHI to a non-Regulated Entity (whether in accordance with or in violation of the HIPAA Rules), the HIPAA Rules do not govern the non-Regulated Entity's use or disclosure of the PHI. A Regulated Entity may choose to limit a non-Regulated Entity's use or disclosure of the PHI as a condition of releasing it, but those limitations would not be enforceable under HIPAA. Similarly, where an individual shares his or her health information with a non-Regulated Entity, the individual has no HIPAA-based privacy

[3] https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule

[4] 45 CFR §§ 164.400-414

[5] http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

rights (but may have rights based in contract, state privacy laws, or other relevant federal law).

HIPAA only governs the use and disclosure of PHI by Regulated Entities (Covered Entities and their Business Associates); PHI used or disclosed by a non-Regulated Entity is outside the scope of HIPAA.

An app developer is a business associate if it is creating, receiving, maintaining or transmitting protected health information on behalf of a covered health care provider. So an app developer that is providing services to a provider that involves PHI is a business associate of the provider.

The Office for Civil Rights (OCR) produced specific guidance including a set of scenarios describing when health apps require a BAA[6]. Based on OCR's presentation of these scenarios, the Task Force recognized a number of circumstances where no BAA is required. But relationships among healthcare organizations and health IT developers can be complex, and it is often difficult to map real-life circumstances into the OCR's prescribed scenarios.

OCR has also launched a platform for mobile health developers and others interested in the intersection of health information technology and HIPAA privacy and security protections. The website, monitored by OCR, http://hipaaqsportal.hhs.gov/ provides education and guidance, and allows users to submt questions or offer comments.

Recommendations

- ONC should coordinate with the relevant agencies and Congressional committees of jurisdiction where legislation is needed to give agencies the ability to effectively implement rules and regulations that ensure privacy and security of all health data.
- ONC should analyze the feasibility of a single, simple, comprehensive oversight framework mechanism that would address the needs of the patient-directed API ecosystem (for all health data shared with all organization types using any technology).
    - We recognize implementation of such a framework may require Congressional action; however, using its role as advisor for all things health IT, ONC should seek to harmonize conflicting, redundant and confusing laws that govern access to health IT.
- ONC should work with OCR to provide additional guidance to clarify whether a BAA is required in these scenarios.
- ONC should coordinate with the relevant agencies a single location for all API actors (EHR API developers, app developers, providers and patients) to access in order to become educated and understand the oversight and enforcement mechanisms specific to patient-directed health apps, as well as their specific rights, obligations and duties.
    - Patients should have one location to access to log complaints or to launch investigations regarding an app's behavior.
    - App developers should have one place to access to log complaints or to launch investigations regarding a provider or an EHR API developer's behavior

[6]http://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf

regarding information blocking.
    - Penalties for “bad actors” should be clearly communicated.
- We recommend that ONC coordinate with the relevant agencies to publish guidance as quickly as possible for EHR API developers, app developers, providers and patients, as to whether, from a HIPAA perspective, sharing data with a patient-directed application should be considered as an individual's access, or access by a third party, or as a tool for engaging in treatment (or a combination thereof), so the respective actors could anticipate how to meet HIPAA-specific requirements.
    - We note there may be a need for further distinction based on the nature of the app and its function, in a manner that affords the patient both the greatest flexibility and the highest protections.
- ONC should work with the relevant agencies to provide guidance to providers as to the patient-specific warnings and notices that can and should be made available via the portal prior to the app approval/authorization process.

Generic Use Case

We frame our discussion of API issues specific to our scope and charge through the use of a generic use case, described below.

> App Developer builds an app that can benefit from patient data accessed via an API-based connection to EHR data (Topic 1). App Developer registers App with Hospital or its EHR (Topic 2). Patient becomes aware of App (Topic 3), reviews App's data use and privacy policies (Topic 4) and decides to connect App to her EHR data at Hospital. Patient signs into Hospital’s portal, which displays an authorization screen. Patient agrees to share (Topic 5) some or all of her EHR data for some duration of time with App (Topic 6), and Hospital records this decision (Topic 7). Hospital’s portal sends Patient back to App, and App gets a unique, time- and scope-limited access token for Patient (Topic 8). App can use the token to access Patient's authorized EHR data for some duration of time in keeping with Patient’s approval (Topic 9).

We organize this document to correspond accordingly to topics raised in the use case:

> Topic 1: Types of Apps and the Organizations That Provides Them
> Topic 2: App Registration
> Topic 3: Endorsement/Certification of Apps
> Topic 4: Communication of the App’s Privacy Policies and Practices
> Topic 5: Patient Authorization Framework
> Topic 6: Limitations and Safeguards on Sharing
> Topic 7: Auditing and Accounting for Disclosures
> Topic 8: Identity Proofing, User Authorization, App Authorization

Terms used are defined in the Appendix Glossary.

Variants on Use Case

Apps can be developed by various parties (e.g. provider organizations, insurers, patients, consumer technology companies, researchers, or criminals), and may or may not be “cloud” based. A few examples of apps include:

> **Personally-Controlled Health Record**. For example, Microsoft HealthVault. A site that is managed exclusively by a patient, storing information on the patient's behalf and making 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.

Use Case Topic 1: Types of Apps and Organizations Who Provide Them

Background

Within the framework of 2015 CHIT and MU3, patient data must be "available for the patient (or patient-authorized representative) to access using **any application of their choice that is configured to meet the technical specifications of the API** in the provider's CEHRT."[7]

Findings

During our testimony, we heard from panelists across the industry who described various health apps that will likely participate in the ecosystem. We heard about existing and potential apps developed by consumers themselves, or their friends and families (DIY movement); consumer companies; healthcare providers; insurers; clinical professional societies; HIT vendors; employers; medical device manufacturers; consumer device manufacturers; data aggregators; research organizations; health data platform companies; governments; and others.

The CHIT and MU3 regulations do not differentiate based on who has written an app, or the app's purpose or credibility. The key determinants of access appear to be **technical compatibility** and **patient choice**.

Recommendations

- ONC should coordinate with the relevant agencies and explicitly state in formal guidance that the type of app, and the kind of organization that developed it, are not considerations with respect to patient access. The only relevant concerns should be technical compatibility (app works with the API technical specifications) and patient

[7] https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications

choice.

Use Case Topic 2: App Registration

Background

The term "registration" designates some up-front technical process by which a client application is "introduced" to an API, and certain details are recorded within the API provider's system. For example, registration might convey: app name; app URLs; name and contact information for the app developer or other entities responsible for hosting the app.[8]

In some protocols, like OAuth 2.0, registration is a technical necessity; the registration process establishes the identifiers that an app will need when it asks for a patient's approval to access data. Although registration may be a technical necessity, it need not present a policy barrier. Web APIs often allow quick, frictionless registration of apps through two common patterns:

1. *Self-Service Registration Portal.* In this pattern, the API provider hosts a web site where developers can register a new client application by filling out a web form, perhaps providing some assurances or confirming details about their App. Generally registration is "automatic" in the sense that it requires no manual off-line review of evidence associated with the developer and imposes no artifical waiting period; but it may require the app developer to manually complete a Web-based form. Note that the mere act of registering the app does not share data with the app; data won't flow until a post-registration step called "app approval", where the API provider verifies the patient's identity and records the patient's decision to share. So registration itself is a low-risk activity.

2. *Dynamic Registration Protocol.* In this pattern, the API provider hosts a fully automated API for adding a new client application to a provider organization. For example, the OAuth Dynamic Client Registration Protocol[9] fills this role. This process can be entirely automated, with no manual form-filling and no waiting period. Note again that the mere act of registering the app does not share data with the app; data won't flow until a patient's decision to share. So registration itself is a low-risk activity.

An API provider can follow these patterns separately, or together. For example, an API provider can offer self-service registration *and* dynamic registration, which may be a particularly convenient way to suit diverse API developer needs.

In the 2015 EHR Certification Criteria, ONCs stated[10], "our intention is to encourage dynamic

---

[8] Note that some apps are deployed as a single, centralized service (e.g. HealthVault, Microsoft's personal health record platform), while other can be deployed multiple times, by different organizations and users (e.g. Indivo, an open-source personal health record). Apps can even be designed to have a separate "deployment" for every user. Registration is generally a once-per-deployment event, though it can be desirable for an API provider to know that a set of registrations all refer to different deployments of "the same app".

[9] https://tools.ietf.org/html/rfc7592

[10] https://www.federalregister.gov/articles/2015/10/16/2015-25597/2015-edition-health-information-technolog

registration and strongly believe that registration should not be used as a means to block information sharing via APIs". But ultimately ONC removed the strict requirement for dynamic registration, stating "from the comments received it was clear that our intention was not understood. Further, open source standards for dynamic registration are still under active development, there is currently no consensus-based standard to apply."

Findings

ONC's intention was to ensure that app registration procedures and policies did not limit a patient's ability to choose health apps. When ONC rejected the criterion of dynamic client registration, they apparently did not consider requiring self-service registration portals as an alternative.

When the final 2015 rule was published, ONC expressed concern that standards were still under active development; but in fact a finalized release of the OAuth 2.0 Dynamic Client Registration Protocol[11] was published by the IETF in July 2015 as the standards-track RFC 7591.

Confusingly, ONC appears to suggest that the 2015 certification criteria should suffice to allow application access without any registration process:

> *"a Health IT Module certified to this criterion [must] be capable of ensuring that: valid user credentials such as a username and password are presented … ; the provider can authorize the user ...; the application connects through a trusted connection... These certification requirements* ***should be sufficient to allow access without requiring further application pre-registration****." (emphasis added)*

Recommendations

- ONC should clarify that its goal is to ensure that when app registration is required, it does not impose an unreasonable barrier to patient choice.
- ONC should ensure that in scenarios where registration is a technical requirement, the registration process is frictionless and does not impose delays. For example, 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.
- ONC should further clarify that self-service registration portals and dynamic registration protocols are two complementary ways to ensure frictionless app registration. In subsequent rules, ONC should require both of these modes of app registration, since they address different developer needs, and it is easy to build a self-service registration portal on top of a dynamic registration protocol.
- 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) where registration is

---

y-health-it-certification-criteria-2015-edition-base#p-1071

[11] https://tools.ietf.org/html/rfc7591

sometimes a technical requirement.

- ONC should coordinate with the appropriate oversight agencies to ensure that API providers do not charge a fee for the app registration process, when registration is required. We note that HIPAA in general allows CEs to apply reasonable charges for a patient's access to data -- but such charges should not be applied to the registration process, before any data are flowing. ONC and OCR should clarify that "reasonable" charges in this context are vanishingly low, even to the point where levying the fee might cost more than the fee itself.
- ONC should coordinate with the appropriate oversight agencies to specify how app developers should report any "data blocking" issues that occur within a provider's app registration process.

Use Case Topic 3: Endorsement/Certification of Apps

Background

In a diverse health app ecosystem, some apps will be "more trustworthy" than others. Trustworthiness is a broad concept with many facets including:

- clinical (e.g. "does the app make safe recommendations?")
- privacy (e.g. "does the app propose to share my data in unexpected ways?")
- security (e.g. "are the app's servers well-guarded against attackers?)
- value (e.g. "is the app worth the money it costs?")
- stability (e.g. "will the app be around and well-supported in 18 months?")
- reputation (e.g. "what is known about the app's authors and their motivation?)

Patients will face an increasing number of choices in the marketplace; it is important to ensure the availability of tools and services that allow discovery of the best and most trustworthy apps.

Findings

We heard from a number of healthcare providers who shared concerns about allowing unknown patient-designated apps to connect to their APIs. These concerns included a worry that patient-designated apps might work against the patient's interest (e.g. leaking data), or that patient-designated apps might attempt to compromise the security of the provider's system. In general, we heard that providers would feel more comfortable in an environment where connections were restricted to well-vetted apps, through a process where apps obtained "certification" or a "seal of approval" or "endorsement". At the same time, we heard from patients and consumer representatives who expressed the concern that the expectation of app certification would unduly restrict consumer choice. We heard from consumer advocates that such restrictions would violate the patient's right to access.

Recommendations

- ONC should not require centralized certification or testing of apps. Instead, ONC should encourage 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 [12]) can "endorse" a given app through a distributed, publicly visible process, without centralized regulatory oversight. For example, an endorsement might take the form of openly published, cryptographically signed statement listing verified attributes of the endorsed app. Then, a consumer's evaluation of a given app could take such endorsements into account. This kind of infrastructure enables third-party app discovery services where consumers can filter apps based on criteria they consider most important (e.g. "only show me apps that Consumer Reports recommends", or "only show me apps that that promise not to share my personal data with advertisers, according to an analysis of their privacy policy conducted by the National Associate for Trusted Exchange"). This approach to endorsements avoids the pitfalls of defining a centralized certification process; and it avoids the difficulty of standardizing privacy policies; but still allows the consumer-facing discoverability benefits.
- ONC should ensure 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.
    - Provider organizations, however, should have the ability to present some of an app's endorsements to the patient at the time of app approval. For example, a provider could display endorsements from trusted sources (or conversely, if the app has none, the provider may display a warning and request extra patient confirmation).
- ONC should coordinate with the relevant federal agencies that are also holders of patient data to encourage the publication of federal app endorsement criteria, by which their patient populations would benefit.
    - For example, the Department of Defense may create a list of criteria by which apps that access the EHR data of active military would meet to indicate the app's trustworthiness.
- ONC should encourage a secondary market by which patients are able to share their experiences about an app.

Use Case Topic 4: Communication of the App's Privacy Policies

Background

Risks associated with disclosures of protected health information (PHI) using well-known mechanisms are fairly well understood and mitigated in today's healthcare environment. We heard from providers concerned that patient-directed API technology may introduce risk owing to variables beyond the provider's control (e.g. when disclosed information is subsequently used

[12] This does not necessarily apply a business associate agreement between the app and provider. See OCR guidance.

or accessed inappropriately).

As entities regulated by HIPAA, providers are familiar with the HIPAA Notice of Privacy Practices for Protected Health Information and have oriented their compliance practices accordingly. The portals by which patients access the API are provided by HIPAA-regulated entities, yet it will be common for a patient's data to be disclosed to an app that is not regulated under HIPAA.

While HIPAA is a starting point for the disclosure, once the disclosure is made to a non-HIPAA regulated entity, it is not clear which laws prevail and how privacy issues must be identified and enforced, nor who is responsible for what actions (provider, API developer, app developer) when a patient's privacy rights are violated. Providers are concerned they will miss making the necessary updates to their risk and compliance processes to assess these unknown situations and may be held liable or penalized for an unexpected outcome that may or may not be within their control.

Findings

The Task Force heard from commenters who were concerned the typical patient is not savvy enough to understand the information presented enough to navigate the complex privacy landscape.

The Task Force recognizes the patient must have a fundamental level of "privacy literacy" in order to make an informed decision about whether an app is allowed to access their health data, which requires patients to be aware of the app's privacy practices for the access, collection, use and disclosure of their health information.

The Task Force also recognizes that many elements contribute toward whether a patient can be considered "aware" of the app's privacy practices. For example, the usability and readability of the privacy notices may be complicated by small font size or a language inappropriate for the actual consumer (English, Spanish, etc.), or the user may have needs specific to one or more disabilities. Further, patients may click "I Accept" yet not actually read the provisions.

There are several existing Model Privacy Notices we can draw on for reference.

- ONC Voluntary PHR Model Privacy Notice (currently under revision)
- OCR HIPAA Model Privacy Notice
  http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

There are several existing best practices for transparent communications to consumers:

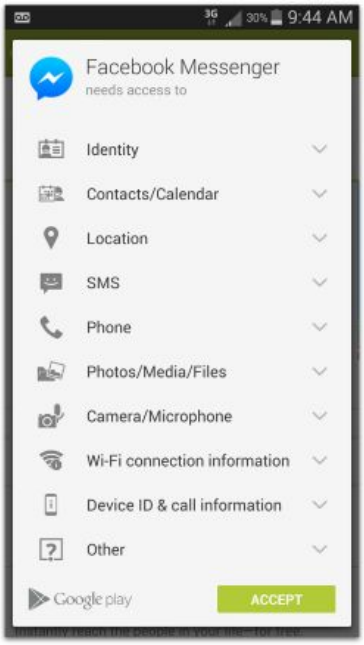
- FDA Nutrition Facts Label and the Schumer Box for credit card disclosures

There are several practices and industry guidelines we can draw on for reference.

- Future of Privacy Forum Best Practices for Mobile App Developers

https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf

- HealthKit's requirement for an app to have a privacy policy (refers to OCR & ONC MPNs) and accessed at https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/
- Google (accessed at https://developers.google.com/terms/#your-api-clients) - sections of interest:
    - Section 3d. User Privacy and API Clients: You will comply with all applicable privacy laws and regulations including those applying to PII. You will provide and adhere to a privacy policy for your API Client that clearly and accurately describes to users of your API Client what user information you collect and how you use and share such information (including for advertising) with Google and third parties. Apple - Developers must provide clear and complete information to users regarding collection, use and disclosure of user or device data. (Section 3.3.10 of the iOS Developer Program License Agreement) Apps should have all included URLs fully functional when you submit it for review, such as support and privacy policy URLs. (Section 3.12 of the App Store Review Guidelines) Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used. (Section 17.1 of the App Store Review Guidelines)
- Android - "If users provide you with, or your app accesses or uses user names, passwords, or other log-in or personal information, you must make users aware that this information will be available to your app, and you must provide legally adequate privacy notice and protection for those users." (Section 4.3 of the Android Market Developer Distribution Agreement) "It is important to respect user privacy if certain parameters, such as demographics or location, are passed to ad networks for targeting purposes. Let your users know and give them a chance to opt out of these features."
- Facebook - "You will have a privacy policy that tells users what user data you are going to use and how you will use, display, share, or transfer that data and you will include your privacy policy URL in the Developer Application." (Section II(3) of Facebook Platform Policies)
- Short form notices use a limited number of characters that highlight the key data practices disclosed in the full privacy policy.



Screen capture of Facebook Messenger App short form notice. Note that here, the decision is "all-or-nothing", and that a user must make the decision ahead of time. More recent Android releases allow the user to make fine-grained decisions, and allow the user to delay some decision-making until after an app has been installed (e.g. access to contacts might be requested only when the user attempts to look up a friend).

There are several existing applicable laws and regulations that address transparent communications to consumers regarding privacy and security practices:

- From Jan. 2016, the FTC's 2015 Privacy and Security Update shed's light on the FTC's authority over privacy and security matters and examples of actions they've taken in recent years:
    - *"The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain*

privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule. To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.

- The FTC's other tools include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before the U.S. Congress and commenting on legislative and regulatory proposals that affect consumer privacy, and working with international partners on global privacy and accountability issues." (https://www.ftc.gov/reports/privacy-data-security-update-2015)
- Of particular note is the list of actions they've taken against orgs. such as TRUSTe (a certification body) and PaymentsMD (a health billing portal) that are related to some of the API Task Force's discussions (https://www.ftc.gov/reports/privacy-data-security-update-2015#enforcement)
- Some of the rules listed, including the health breach notification rule, also seem relevant for enforcement authority. (https://www.ftc.gov/reports/privacy-data-security-update-2015#rules)
- The FTC also keeps a large list of press releases for privacy related actions that may help to give an idea of it's reach (https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises)
- The FTC published a guide titled "Marketing Your Mobile App: Get It Right From the Start" to guide app developers on what truth-in-advertising and privacy principles apply to their products. (https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start)
- Other non-privacy enforcement actions of the FTC:
    - *"The Federal Trade Commission (FTC) protects consumers from unfair or deceptive acts or practices as well as false or misleading claims. Where mHealth is concerned, it has focused on the claims companies have made about the effectiveness of their devices or apps. The FTC also has jurisdiction over health data breaches when the entities involved are not HIPAA-covered entities. The FTC has already been active, taking enforcement action against several mobile health app marketers that have not met the requirements of the FTC. The FTC collaborates closely with both the FDA and FCC on areas where there is jurisdictional overlap." (http://cchpca.org/mhealth-laws-and-regulations)*

- HIPAA - national privacy standards for the protection of individually identifiable health information for certain regulated entities.
- Children's Online Privacy Protection Act of 1998 (COPPA) Sets forth rules governing the online collection of information from children under 13 years of age, including restrictions on marketing to those under 13 years of age.

Recommendations

- We recommend that ONC coordinates with the relevant agencies to pursue a concept of "privacy literacy," similar to what is known as "health literacy." This would include defining the basics of privacy literacy, and outlining strategies and techniques for the government either to action directly - or through providers and app developers - to improve privacy literacy at the community and organizational level.
    - Privacy literacy is the degree to which individuals have the capacity to obtain, process, and understand basic privacy information needed to make appropriate decisions regarding the sharing of personal information, including health data.
- We recommend that ONC supports a Model Privacy Notice for app developers.
    - The MPN should clearly define who is responsible for what (individual, app developer, provider, API developer), including example indemnification clauses where applicable.
    - The MPN should provide standard definitions and terms.
    - To facilitate easy review and a user-friendly experience, a short-form privacy notice may be valuable, with a link to access the full notice or more detailed information. ONC should provide guidance in its MPN for the minimum data set required for short form notices.
    - The MPN should allow for the download - or other electronic "save" - of the privacy notice (or otherwise saved electronically).
    - The MPN should ensure a "just in time" communication when the patient accesses the app.
    - Users must be informed when the app's practices change
    - Privacy policies must be easily accessible in the app for later review
    - Where the patient has choice and control, the app should provide meaningful controls such as opt-outs.
    - Contact information regarding how a patient can contact the app developer if there are problems are concerns.
- We recommend that 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.

- We recommend that ONC collaborate with FTC to provide ongoing support to app developers to ensure the app's privacy practices align with the app's marketing practices according to Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information.
- We recommend that ONC evaluates methods by which a consumer is able to compare the privacy policies of two or more apps.
- We encourage ONC to pursue enforceability of "click through" agreements specific to health information.
- We encourage the private market to develop standards specific to the usability of consumer apps, and until such time, app developers should be encouraged to consult Web Content Accessibility Guidelines (WCAG) for a wide range of recommendations to make apps more usable to more types of users.
- We encourage the development of private-market endorsements to indicate those apps that strive to make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photosensitivity and combinations of these.

Use Case Topic 5: Patient Authorization Framework

Background

We hold the fundamental assumption that the *APIs by which patient-directed apps gain access to patient data are "logically" administered by providers who are Covered Entities under HIPAA* (that is, even if the Covered Entity does not run and maintain the hardware and software stack, this functionality is provided *on behalf of* the covered entity, by a Business Associate).

As noted in Regulatory Oversight and Enforcement of APIs, there is no existing official guidance as to whether sharing data with a patient-directed app is defined as individual access, or authorization to share data with a third party, or as tool for engaging the consumer in treatment.

We recognize, however, that providers will have existing HIPAA practices (implemented as a Covered Entity or via a Business Associate) specific to patient consent, patient authorization to disclose to third parties, and access to the individual's own record. Each of these pathways indicates terms specific to what essentially represents the patient's go-ahead for the app to receive his/her data (referred to as consent, authorization, approval, or request for access), and has downstream effects, such as requirements for notification of breach and accounting of disclosures. Throughout this document, we try to use the correct term in its correct context.

Generally, we refer to this process as the patient's "authorization."

- We note that the term "authorization" as used in this section is specific to HIPAA patient authorizations for disclosure, not the term used when referencing the technical protocol that allows users to approve an application to act on their behalf (eg, OAuth) as referenced in Use Case Topic 8: Identity Proofing, User Authorization and App Authorization.
- The need for the provider to document the patient's authorization is a critical component which we further discuss in Use Case Topic 7: Auditing and Accounting for Disclosures.

There are some challenges in applying certain HIPAA processes to the patient-directed API. For example, under HIPAA, individuals may request access to their PHI and a Covered Entity is required to provide such access if the PHI is maintained in a designated record set and no grounds for denial exist (providers may deny a patient's request to access his/her own PHI in whole or in part ; HIPAA § 164.524 stipulates grounds and requirements for denial of access). Under current HIPAA regulations, providers have no later than 30 days to respond to an individual's request to access his/her information. Recognizing the "on the fly" nature of patient-directed apps, it is not feasible to assume a site administrator can manually mitigate patient requests for access to their individual information within this framework. Additionally, the HIPAA designated record set contains a broader set of data than what EHRs implement to support the CCDS; for example, the HIPAA designated record set contains data related to enrollment and payment.

Recommendations

- We recommend that until clear guidance is available, providers should proceed in defining practices for their EHR portals in a manner that focuses on ensuring the patient is in possession of all essential information in order to give his/her valid, informed go-ahead for the provider to enable the patient-directed app access to the patient's data. While we expect this is no different than what a patient is already asked to agree to for use of the portal given its ability to view, download and transmit, this ensures the authorization represents the patient's control to direct the disclosure (or use the app to make the request).
- We recommend that ONC coordinate with the relevant agencies a model authorization form with resuable/referance-able language, that contains the following information:
    - The name of the patient whose records will be shared
        - The relationship of the authorizer to the patient (eg, guardian, parent)
        - We note the legal challenges inherent in releasing information to and on

behalf of minors. We do not provide comment on this topic and recommend ONC coordinate appropriate guidance.

- The name of the app requesting information
- A description of the information that identifies the information in a specific and meaningful manner, such as listing the data categories the app is requesting access to (scope of permissions)
    - While we recognize the need to provide more granularity in access permissions as capabilities evolve, we note ONC should be clear in its guidance that there is no expectation to support granular permissions beyond data categories for the 2015 CHIT Edition API requirements. For example, Grant "Access to My Meds," not "Access to My Diabetes Meds."
- A statement as to whether the app can or cannot change information currently in the EHR. (Note that the task force scope is read only access.)
- 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)
    - Note the task force is not commenting on best practices for e-signature; however, this information should be readily obtainable from a web interface (clicking on buttons or typing) and should not require offline processes (such as a faxed signature) or special software.
- "Save as" or "Email a copy to" Option: The patient must be provide a mechanism to email or otherwise electronically save the authorization for his/her own records.
- Access to the policies regarding the API developer and the provider's obligations to disable access to an app (such as through the provider's obligations to respond to threats under the HIPAA Security Rule), as well as the patient's ability to be made aware of the reasons for which an app is disabled (and any related appeal process).
    - We recommend additional guidance to determine whether there are grounds and specific requirements to support the provider to deny the patient's request to authorize a patient-directed app, such as those specified in 164.524.

- As we expect patients will be managing access to their data across multiple EHR APIs from multiple provider portals, use of a model authorization form will help patients be

aware of and navigate inconsistencies. We recommend that ONC encourage a standardized mechanism by which a patient can compare authorization requirements for two or more providers.

- We recommend that ONC continue advancing work in support of standardized machine computable consent. At the same time, we emphasize that a lack of granular, comptable consent standards should not be viewed as a barrier to exchanging data through APIs. Generally, standardized machine computable consent may be helpful for the "to what" aspects of the disclosure. Supporting the request of the API through a standardized, computable process could facilitate the response matching the request as accurately and completely as possible, and consistently across multiple systems.
    - In the Interoperability Roadmap, ONC referred to computable privacy as "the technical representation and communication of permission to share and use identifiable health information, including when law and applicable organizational policies enable information to be shared without need to first seek an individual's permission. Once implemented effectively, using technology for privacy compliance saves time and resources, and can build trust and confidence in the system overall." Standards for computable privacy will go a long way to address automating the complex legal, regulatory and policy landscape for patient-directed exchange of health information via apps.

- We recommend that ONC coordinate with the relevant agencies to publish guidance to providers on best practices for patient-directed API authorizations, which includes We recommend the provider include the following statements, which are typical of HIPAA authorizations, to notify the individual of the following:
    - The individual has the right to revoke the app authorization, and provide a description of the process to do so.
    - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on the authorization.
    - The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by HIPAA.
        - We recommend that, where feasible, the provider should be required to disclose its relationship to the app and indicate whether the app is covered by HIPAA.
    - A statement directed at the patient to the effect of, "Please ensure you refer to the app's terms of service and notice of privacy practices for further details." (See Use Case Topic 4: Communication of the App's Privacy Policies.)

Use Case Topic 6: Limitations and Safeguards on Sharing

Background

Three parties must come together to enable the flow of data into a patient-selected app: the patient, the API provider, and the application. All three parties must agree before data can be shared between systems. Questions about the circumstances in which each party can impose limitations on access to data include:

1. *API Provider.* Under what circumstances can the API provider limit access to patient data? For example, can an API provider prevent certain applications from registering, or disable access to apps that have already been approved by a patient?
2. *Patient*. When a patient decides to share data with an application, what limitations can the patient impose on this decision? Any limitations (e.g. of duration, or scope of access) must be "supported" by the API provider in a technical sense, in order to have an actual effect. In this model, the patient and API provider together define a policy for access, and the API provider implements that policy with respect to a given application.

Findings

We heard from consumer health technology firms and healthcare providers who host APIs today. In general, many API providers impose restrictions at app registration, limiting registration to apps that fall under the API Provider's terms of use guidelines. API providers sometimes dictate the terms by which a third party app may use data from the API, for instance to prevent the downstream sale of data to third-parties, or to prevent use in advertising. API Providers also impose limitations on rate of access and security-related details, such as requiring encrypted connections and the and expiration/refreshing of access tokens.

API certification can provide a level of assurance and stability that certain standards and requirements are being met - both for the interfaces that are being supported and for the security and permissioning capabilities.

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 believe that there will be an evolving set of services around patient record locator services that will enable a patient or a provider to find the sources of data and links and/or coordinates to access the APIs for that information.

We heard from patients who would like to share their data with apps and services on a long-term, ongoing basis, with minimum friction. We also heard about use cases for limited sharing, such as an app that helps a patient search for better medication prices: such an app would not necessarily be expected to require access to a patient's entire data set (e.g. lab tests, immunizations, problem list).

Note: ONC's 2015 certification program requires that an API provider offer access at the

"data category" level (e.g., lab results, or immunizations), but there is not currently a requirement that patient be allowed to define a sharing policy at the category level. In other words, the 2015 certification criteria allow an API where a patient's only choice is to share "all or nothing" with an app; and it would be entirely up to the app to decide which categories of data to access, after receiving blanket approval.

We heard testimony that authorization standards have mechanisms for capturing such limitations as an explicit set of permissions at app approval time (e.g., OAuth 2 has a "scopes" mechanism for this purpose).

Recommendations

- ONC should clarify that while API Providers may impose security-related restrictions on app access (e.g. rate-limiting, encryption, and expiration of access tokens), it is inappropriate for API providers to set limitations on what a patient-authorized app can do with data downstream.
    - Given the nature of patient access rights, the provider is not in a legal position to prevent the registration of apps that would aggregate or share data, for example (though the provider might certainly decide to warn the patient, or endeavor to educate and explain these issue to the patient, as part of the provider-hosted app-approval workflow).
- 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[13], or appears to have been compromised, or if the app poses a threat to the provider's own system. However, patients must be able to override this suspension (except in the case where an app poses threat to the provider's own system or violates allowable terms of service).
- ONC should coordinate with the relevant agencies the threshold of proof by which an app may be disabled in order to avoid considerations of Information Blocking.
- ONC should update the HIT certification requirements to ensure that API providers enable patients to share data with certain (coarse-grained, for now) limits, rather than "all or nothing". Under the updated requirements, 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.
- ONC should require that CHIT enable patients to share data with apps at the category level.
    - While we believe in the value of fine-grained permissions, we also recognize that implementing many narrowly-scoped access control policies would require a costly and difficult re-design of existing systems. Therefore in the near-term we propose a pragmatic approach that ties back to the capabilities described in the

[13] We need clarification about where ToS (between app and provider) end, and HIPAA begins. What are acceptable terms of service? Can these terms impose limits like “no more than X requests per minute”? Does it depend on X? What about “No more than 1 request per week” → this seems obviously unreasonable. We also need clarification on where complaints should go.

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), ONC should ensure that patients can approve access at this same level.

Use Case Topic 7: Auditing and Accounting for Disclosures

Background

Multiple parties participate in the API ecosystem - the patient, the provider (Covered Entity), the app developer, and the EHR API developer - and each of these parties plays an important role in bringing to light unauthorized accesses to personal health information (PHI). Further, there are several existing oversight mechanisms that contribute to overall auditing and accounting for disclosures practices. Effective auditing is a crucial tool to detect system intrusion attempts, to track disclosures of PHI, to provide forensic evidence during investigations of a security incident, and to ensure policies are being followed.

Patient: Providing individuals with an accounting of disclosures fosters transparency and patient trust. When patients review these accountings, they inherently assist providers to ascertain weakness in privacy and security practices by identifying possible unauthorized disclosures and detecting possible breaches. HIPAA provides individuals with the right to view an accounting of disclosures made by a Covered Entity; however, this does not include disclosures made to the individual, to a third party specified by the individual, or to any entity for treatment, payment or healthcare operations purposes.

Provider: Must meet the requirements of various sources specific to auditing needs and accounting for disclosures. For example, HIPAA, HITECH, Meaningful Use, The Joint Commission, and so on.

EHR API Developer: Responsible for enabling both the auditing of the disclosure and auditing the authorization of disclosure—i.e. the event where the patient authorizes the disclosure of his/her PHI to the app. The EHR API developer must comply with the ONC CHIT audit related criterion.

App Developer: Responsible for auditing what is done with the data by the application, including any further disclosures. Realistically, the app developer is the only one that has enough context to provide a meaningful record of what happened after the initial disclosure made by the API. Apps are not certified, so there are no requirements for apps comparable to the ONC CHIT audit related criterion. There are various sources of

guidance available for app developers specific to privacy and security.

Findings

We analyzed whether patient-driven, read-only APIs introduce risks that we would not expect to be addressed in existing audit and accounting for disclosures practices under ONC CHIT and HIPAA.

CHIT Auditing Requirements

We assessed the 2015 CHIT certification rule and relevant companion guides to understand audit requirements intended to address Read access to PHI from third-party apps via API: § 170.315(d)(10) ‘‘auditing actions on health information’’or § 170.315(d)(2) ‘‘auditable events and tamper resistance.’’ The CHIT must track actions pertaining to electronic health information in accordance with sections 7.2 through 7.4, 7.6, and 7.7 of the ASTM E2147-01 standard, and the actions and information should be captured in a manner that supports the forensic reconstruction of the sequence of changes to a patient’s chart.

- 7.2 Date and Time of Event—The exact date and time of the access event and the exit event.
- 7.3 Patient Identification—Unique identification of the patient to distinguish the patient and his/her health information from all others.
- 7.4 User Identification—Unique identification of the user of the health information system.
- 7.6 Type of Action (additions, deletions, changes, queries, print, copy)—Specifies inquiry, any changes made (with pointer to original data state), and a delete specification (with a pointer to deleted information).
- 7.7 Identification of the Patient Data that is Accessed—Granularity should be specific enough to clearly determine if data designated by federal or state law as requiring special confidentiality protection has been accessed. Specific category of data content, such as demographics, pharmacy data, test results, and transcribed notes type, should be identified. For example, the ability of the audit log to record that the user accessed a patient’s medication list would be sufficient; it is not necessary for the audit log to record the specific medication.

We are satisfied that the above CHIT auditing requirements address the needs of Read access by a consumer-direct app to the EHR API.

We note there are potential challenges inherent in auditing app accesses to the API, such as a

high frequency of occurrences flooding the audit with so much noise it is difficult upon review to discern what actually happened based. To this end, we anticipate practices and services will evolve to address these challenges and are not compelled to comment.

HIPAA - Accounting of Disclosures

Patients have the right to receive an accounting of their PHI under § 164.528 (Accounting of disclosures of protected health information). Specifically, an individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures to individuals of protected health information about them.

There is no individual right under HIPAA to receive an accounting of disclosures made to an app at the direction of the individual. If an individual requests a Covered Entity to release his/her PHI to an app, that is the equivalent of releasing PHI to the individual directly and, as such, no accounting of disclosures is required. An individual also does not have a right to an accounting of disclosures made by a Covered Entity pursuant to an individual's authorization.

There is no individual right under HIPAA to receive an accounting of disclosures made to an app by a Covered Entity (or by a Business Associate at the direction of a Covered Entity) for treatment, payment, or operations purposes. In the limited circumstance in which an accounting might be required (i.e., disclosures for public health purposes), note that the obligation to account for disclosures falls on the Covered Entity, not the Business Associate, even if the Business Associate made the disclosure.

App developers not acting as Business Associates are not regulated by HIPAA. An app developer that is not acting as a Business Associate and thus not regulated by HIPAA does not have to comply with HIPAA and would not have to provide an accounting of any disclosures TO OR FROM the app. However, this activity may be governed by terms of use that an individual may agree to when using the app.

Although providers must have audit controls that record and examine activity involving PHI (§ 164.502(a)(1), there is no general right granted to the individual to request these audit records.

The supporting CHIT requirements for Accounting of Disclosures are as follows:

- § 170.315(d)(11) - Accounting of Disclosures - Record disclosures made for treatment, payment, and health care operations in accordance with the standard

specified in § 170.210(d).
    - § 170.210(d) - The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.
    - Note: There is no requirement to make the Accounting of Disclosures available via the portal.

While an app developer may or may not be subject to HIPAA audit requirements, it is not only important for CHIT to audit access to the API, but apps should have some level of audit as well to enable consumers better control and review of their data use and sharing.

Recommendations

- We recommend that ONC expand certification criteria to require CHIT to make API access audit logs available to patients through an Accounting of Disclosures via the portal.
    - Show patients a list of all app authorizations in the portal
    - Include the ability for the patient to revoke any app authorization
    - Show patients a list of which apps have accessed their data via the API (including relevant details like source IP, location, and scope of data accessed)
        - Working with the appropriate authorities, ONC should provide guidance to the EHR API developer regarding the information that should be logged to detail the disclosure by the API to the app, in terms of the “of what” information relevant to both the Accounting of Disclosures and the audit that may be used to meet requirements of the HIPAA Security Rule.
        - We recommend that ONC review the task force’s recommendations for patient authorization requirements in *Use Case Topic 5: Patient Authorization* to ensure CHIT audit capabilities sufficiently support an artifact that represents such patient authorization.
    - The patient should be informed of the process which he/she needs to follow in order to flag any of the displayed disclosures as potentially inappropriate, which then could trigger an investigation by the provider.
        - The patient flagging process should be supported electronically through the portal and not require any manual processes (such as faxing a signed complaint).

- We recommend ONC coordinate with the relevant HHS agencies to publish patient-facing guidance that explains to patients what their rights are when the app developer is not covered under HIPAA as a Business Associate (and therefore not required to provide an accounting of disclosures).
- While apps are not covered under ONC's certification program for health IT and we are not suggesting that they should be, we do recommend ONC should provide guidance regarding voluntary best practices of audit capture and accountings for disclosures to developers offering apps that are intended to interact with CHIT.
- We recommend ONC coordinate with the appropriate authorities, including states, to provide an easy-to-use educational resource that details for all API ecosystem actors (patients, providers, app developers and EHR API developers) the rules and responsibilities specific to breach notifications across all enforcement mechanisms (eg, HIPAA, FTC).

Use Case Topic 8: Identity Proofing, User Authentication, and App Authentication

Background

When healthcare data flow from a HIPAA-covered entity into a patient-selected app, there are several points where identity assurances are required. These include:

- *Registration Time.* API Provider may need assurance about the identity of the application developer.
- *App Approval Time.* The API Provider needs assurance of the patient's (or authorized representative's) identity in order to enable that individual to make a data-sharing decision. The patient may need assurance of the app's authenticity (e.g. "the app that I'm using is the one hosted at https://my-app.com") to make an informed decision.
- *Data Access Time*. The API Provider may need assurance of the app's authenticity in order to permit access.

Findings

We heard testimony from health care provider organizations indicating that procedures have been developed and widely deployed to enable patients to access their own data online today that have been in operation for a long time (up to a decade in some cases) and deployed to millions of consumers. These procedures have spread across the healthcare delivery system as incentivized by MU2 patient access objectives, and they involve different combinations of in-person proofing (e.g. during an office visit, the patient gets a one-time "registration code" to sign up for portal access), postal mail-based proofing (e.g. portal sign-up instructions are sent to the patient via the US Postal Service), or online identity proofing (e.g. patients complete an

automated identity proofing process relying on knowledge based responses to consumer specific content derived from financial records). While these practices are diverse, they are not unique to APIs, and existing solutions have enabled patients to access their data through online portals in the MU2 era.

We heard testimony from API providers in the consumer space where app registration is offered on a self-service basis (e.g. registering an app with Google via https://developers.google.com). In such cases, the API provider verifies some attribute about the app developer (e.g., e-mail address and the app's URL), and requires the app developer to agree to terms of service. At approval time and data access time, a combination of the app's domain and (in some cases) app credentials is used to verify the identity of the app.

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 View, Download, Transmit.
    - Specifically, a provider organization must have an appropriate level of assurance of a patient's identity, and must authenticate the patient through an appropriate mechanism. But the same sign-up and login process that's used for portal access can and should be used to bootstrap API access.
- ONC should recommend that standards like OAuth can used to allow patients to leverage existing portal account infrastructure as the means for approving access to an app.
- ONC should indicate that API Providers must not impose patient identify-proofing or authentication barriers for API access that go beyond what's required for View, Download, Transmit access.
- ONC should collaborate with the appropriate agencies to provide clear and distinct API developer and API appropriate usage privacy and security standards in order to encourage API development and adoption.
- ONC should clarify that for registering patient-authored apps, existing patient identity proofing and authentication is sufficient: in other words, 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 other apps, ONC should clarify that identity proofing of developers must be non-onerous and automatable (e.g. e-mail address or domain verification would be reasonable; a review of tax records or inspection of facilities would not).
- 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, and that providers must ensure that app approval and data access can occur without active involvement from the API Provider or app developer.
    - In other words, the only person who should have to take action to approve an

app's access to patient data is the patient (or representative).

- ONC should establish that an API provider's portal-based identity proofing and patient authentication procedures (i.e. the ones capabilities they use to enable access to patient portals) are deemed sufficient for granting an app access to the API.
    - Any process that presents a substantially greater burden to the patient for API access approval should be considered Information Blocking.