Creating Access to Real-time Information Now
through Consumer-Directed Exchange

The CARIN Alliance
Application Registration Guide

Initial Draft
Version 0.1
July 22, 2021

****This document is provided to the community as a draft and is meant to actively solicit stakeholder comments and feedback. Comments can be made on our website:**
https://www.carinalliance.com/about-us/contact-us/**

Table of Contents

1. Overview of This Guide

The purpose of this Application Registration Guide ("Guide") is to contribute guidance for payers required to implement provisions of the CMS Interoperability and Member Access Rule (CMS-9115-F or the "Rule"). The Guide includes guidance for implementing the app registration and member authorization experiences, with a focus on (i) the information payers can collect as part of an appropriate security risk analysis, (ii) delivering consumer education content that the Rule requires, and (iii) implementing a developer attestation process that incorporates the CARIN Code of Conduct, as encouraged in the Rule's Preamble. The Guide also includes recommendations for payers to provide developer-facing resources that API implementers in the wider technology community routinely provide at their API endpoints. This IG has been developed with the input of CARIN Alliance stakeholders, which collectively represent a cross-section of organizations involved in the health care information exchange community.

2. Intended Audiences

While the primary audiences of this IG are affiliated with payers that are subject to the Rule, a wider number of different organizations, and audiences within these organizations, can use this Guide. Table 2 lists the organizations, and audiences within these organizations, that the authors consider to be the Guide's intended audiences:

Table 2. Intended Audiences

Organizations	Audiences Within These Organizations
Payers that are required to implement and maintain open, FHIR-based APIs, consistent with the Rule.	Product managers Software engineers with FHIR-based experience Business leaders Regulatory compliance leaders
Other implementers of FHIR-based APIs, including open and proprietary APIs.	
Third-party app developers that want to establish connections with FHIR-based APIs, especially open, FHIR-based APIs.	

3. Goals of This Guide

We believe broad acceptance and implementation of the best practices described in this Guide can help improve interoperability and health care information access by:

1. Alleviating the costs and burdens of compliance on the payers subject to the Rule, which might otherwise develop independent approaches as they interpret relevant provisions of

the Rule, CMS guidance, and other resources identified by CMS in its Interoperability Roadmap.

2. Standardizing the workflows and processes that app developers experience at open APIs – not just of CMS-impacted payers, but all member-focused FHIR-based APIs – thereby alleviating the costs and burdens on app developers to develop robust API connection networks, and increasing overall app developer participation in health care information exchange.
3. Standardizing the delivery of the educational resources required by the Rule, and more broadly delivering contextually relevant content to members about steps they can take to protect the privacy and security of their personal health information.
4. Encouraging all HIPAA-covered entities and their business associates to adopt the same best practices when they implement API endpoints, thereby moving the health care industry forward in building an interoperable and sustainable API-based ecosystem.

4. Regulatory Background

Standardized APIs. Starting July 1, 2021, CMS-regulated payers are required by the CMS Interoperability and Member Access Rule (CMS-9115-F or the "Rule") to maintain application programming interfaces (APIs) that conform with the API technical standards finalized by HHS in the ONC 21st Century Cures Act Final Rule ("ONC Rule"). These APIs include an open, FHIR-based API that enables members to access their adjudicated claims and encounter data, formulary data, and member drug data through their choice of application (member access APIs). In addition, for payers that maintain clinical data in the USCDI standard as part of their normal operations, members must be able to access this data through open, standards-based member access APIs.

Registering Developers and their Applications. Under the Rule, CMS imposes requirements that significantly curtail the discretion of CMS-regulated payers to restrict third-party applications from establishing connections with their member access APIs. These restrictions distinguish the "open" APIs defined by the Rule from proprietary APIs, which may or may not be based on the ONC's technical standards but are not further specified by regulation. Under the Rule, payers can only deny access to an application or developer to open APIs, including the member access APIs, if these connections pose an unreasonable security risk to protected health information in their own systems. As described more fully below, the technical features of properly implemented FHIR-based APIs create a comparatively limited "blast zone" in terms of the security risks posed to payers' own systems. For this reason, developers registering to connect with open APIs should in most cases be approved. The app registration best practices described in this Guide recommend the types of information we believe can be requested of developers, consistent with the Rule and the HIPAA Security Rule, and how this information can be verified using publicly available or commercial services.

Educational Resources for Consumers. For the member access APIs, the Rule also requires payers to provide educational resources that help members become more informed about privacy and security-related factors to consider in selecting a particular application, help members determine if their app is subject to HIPAA, and explain how they can submit complaints to regulatory authorities. As described more fully below, we provide illustrative content and workflows for delivering general

consumer education about steps they can take to protect their privacy before members authorize a registered application to receive their personal health information. Payers can use this illustrative content and workflows as a prototype for developing their own content and workflows. Payers are reminded that the Rule requires general educational content to be accessible to their enrollees, beneficiaries, or members through all the mechanisms they use for communicating with these audiences, and not just within the API endpoint workflows.

Voluntary Attestation Process. In the Preamble accompanying the Rule, CMS encourages but does not require payers to ask third-party app developers to attest to having certain provisions in their respective privacy policies, and to establish a process that allows members to make decisions based on a developer's responses, or lack thereof. Otherwise, the Rule prevents payers from denying access based on their own determinations about a particular application's data practices and privacy protections. See 85 Fed Reg 25510, 25518 (May 1, 2021) ("While HIPAA covered entities and their business associates may notify members of their potential concerns regarding exchanging data with a specific third party not covered by HIPAA, they are not required to do so, and they may not substitute their own judgment for that of the member requesting the data be transferred."). In the discussion below and the prototype referenced above, we offer an approach for introducing a voluntary attestation framework that is aligned to the CARIN Alliance Code of Conduct.

5. Recommendations

Primary Use Cases. The best practice recommendations contained in this Guide are organized around five use cases. The objectives of these use cases are to help app developers to:

(1) Easily search for and find CMS-regulated payers' respective developer portals, which provide publicly accessible links to all resources needed for them to understand and develop software to interact with the Rule's required API endpoints (Section 5.1).

(2) Test the required APIs in a sandbox environment (Section 5.2).

(3) Register with a payer to establish connections with the required APIs in a manner that complies with the Rule (Section 5.3).

(4) Know in advance the information a payer will share with members about the developer's application privacy and security practices (Section 5.4).

(5) Understand in advance the payers' policies regarding session and refresh tokens, and other service level expectations (Section 5.5).

5.1. Developer Portal: Access and Resources

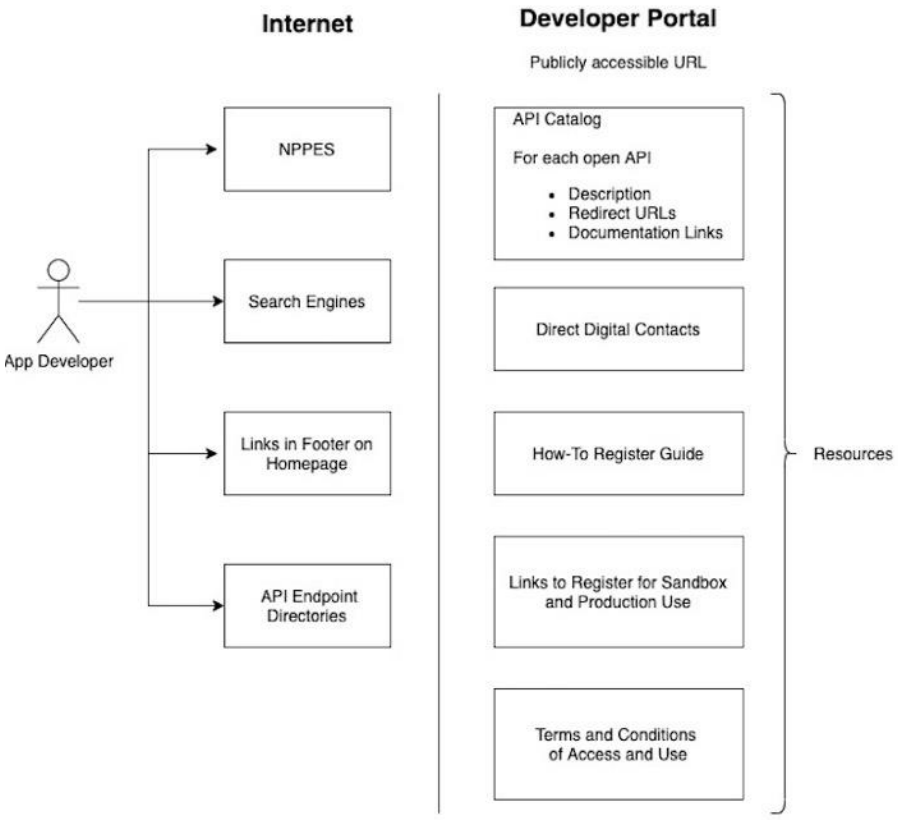
The Rule requires that the API endpoints subject to the Rule be "publicly accessible" by being posted directly on the payer's website or via publicly accessible hyperlink(s). Under the Rule, ''publicly accessible'' means that any person using commonly available technology to browse the internet can access the information without any preconditions or additional steps, such as a fee for access to the documentation; a requirement to receive a copy of the material via email; a requirement to register or create an account to receive the documentation; or a requirement to read promotional material or agree to receive future communications from the organization.

The Rule's public access requirement is consistent with approaches for establishing and sustaining API ecosystems in the wider technology community. To implement these requirements of the Rule and encourage a robust API ecosystem for member-directed health data, we also recommend that payers:

1. Implement and maintain a **developer portal**. A developer portal should minimally include: (a) a library with brief descriptions of all API endpoints that follow the SMART on FHIR protocol and any other external-facing open and proprietary APIs, (b) contact information for reaching the payer's API technical support team, (c) a how-to-guide that explains and provides navigation for all audiences to the resources available through the portal (including all business and technical documentation necessary to interact with the APIs), and what app developers in particular need to do to access and use these resources, (d) links to the page(s) where developers can begin registering to use the payers' respective sandbox environments (described below in Section 5.2) and production environments (described below in Section 5.3), and (e) terms and conditions of use ("terms") for the developer portal and other resources that link to the terms.
2. Add the developer portal URL to the directory of endpoints for health information exchange that CMS maintains using the **National Plan and Provider Enumerator System (NPPES)**, as described more fully by CMS in its NPPES documentation.
3. **Test common search engines** like Google, Bing, Yahoo!, and DuckDuckGo to make sure the developer portal's landing page is being indexed properly by these search engines.
4. Add the developer portal URL to the payers' profile in emerging **publicly accessible API endpoint directories**. See **Appendix A** for a non-exhaustive list of public and subscription-based directories.
5. Include a link to the landing page of the developer portal on the **homepage of the payer's public website**. The link can be included in the main footer, and should be accessible through the website's search tool.

Figure 5.1 represents these recommendations in a process diagram.

Figure 5.1 Process Diagram - Developer Portal Search



Business and Technical Documentation. In addition to making API endpoints publicly accessible, the Rule (together with guidance expressed in the Preamble accompanying the Rule) requires payers to make all business and technical documentation that app developers would need to interact with these endpoints "freely and publicly accessible" so that any interested third-party application developer can easily obtain the information needed to develop applications that are technically compatible with a payer's open APIs. See 85 Fed Reg 25510, 25542 (May 1, 2022). As explained by CMS in the Preamble, "transparent" documentation helps third parties understand how to successfully interact with the organization's API, and how to satisfy any requirements the payer establishes for verifying the developer's identity and their applications' authenticity, consistent with the payer's security risk analysis and related organizational policies and procedures. It also helps prevent discrepancies between a payer's public documentation and its direct communications with app developers. Minimally, the Rule requires documentation to include the following information:

API syntax, function names, required and optional parameters supported and their data types, return variables, and their types/structures, exceptions, and exception handling methods and returns.

The software components and configurations an application must use in order to successfully interact with the API and process its response(s).
All applicable technical requirements and attributes necessary for an application to be registered with any authorization server(s) deployed in conjunction with the API.

A common practice in the wider software industry is to use OpenAPI (formerly Swagger) to document APIs, and to have OpenAPI documents be available to app developers in the Sandbox environment. **Appendix B** includes an example of the full OpenAPI specification as an aid to payers' development teams. Payers should also have a metadata endpoint that shows a server's capability statement. For more information, see Section 5.5.1 below.

Payers can also consult ONC's business and technical documentation requirements for guidance, as detailed in 170.404(a)(2) of the ONC Rule, and accompanying commentary in its Preamble. See 85 Fed Reg 25642, 25748 (May 1, 2020).

Under CMS' definition of public access, all business and technical documentation must be published without any preconditions or additional steps. For example, any visitor to the developer portal should be able to view and download all the documentation they might need to establish an API connection without having to pay a fee, provide an email, register with the site, create an account, agree to read promotional material, or agree to receive future communications. While not explicitly stated in the Rule, CMS' Preamble makes clear that payers cannot require app developers to sign a business associate agreement because the developers are providing services to consumers, and not to the payers impacted by the Rule. See 85 Fed Reg 25510, 25548-25549 ("We also note it would not be appropriate to require a member-designated third party to enter into a BAA with a payer as the API-facilitated exchange is taking place per the request of the member and not by, on behalf of, or service to, the payer.").

Terms of Service. The Rule does not explicitly address whether payers can condition access to their API technology on acceptance of relevant terms of service without violating the Rule restrictions on preconditions and additional steps. Although the Rule is silent on this issue, we believe payers should be allowed to condition access on terms of service that are reasonable for open APIs. For support, we look to Section 170.404(a) of the ONC Rule for guidance, even though Section 170.404(a) is not incorporated by reference into the Rule. Section 170.404(a) aligns with the Rule's requirements for all business and technical documentation to be published via publicly accessible hyperlink. In particular, Section 170.404(a)(2)(ii) requires HIT developers of certified API technologies to publish all terms and conditions applicable to API technology, including any restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

- Develop software applications to interact with the API technology.
- Distribute, deploy, and enable the use of software applications in production environments that use the API technology.
- Use software applications, including to access, exchange, and use electronic health information by means of API technology.
- Use of any electronic health information obtained by means of the API technology.

- Register software applications.

We believe it is appropriate for payers to publish terms of service for their open member-facing APIs because they advance transparency and mutual accountability between payers and developers. They provide the contractual mechanism for payers to exercise rights, including legal remedies, with respect to their online resources (e.g., suspending or terminating a registered app developer's access when their conduct creates a demonstrable security risk to payers' systems). Terms of service can also include acceptable use policies, which can include compliance with other payer-provided documentation. That way, for example, payers can establish a contractual basis for selectively limiting an application's ability to repeatedly call on open API endpoints due to the way the application is built, and thereby prevent service outages that could impact others connecting to these endpoints. For these reasons, we recommend that payers develop and publish terms and conditions for the Developer Portal and all the API-based resources available through it, and condition access and use of these online resources on developers' consent to these terms.

We recognize that each payer will likely establish a single Developer Portal for all of its external-facing APIs, which may include a payer's open and proprietary APIs. Care needs to be taken not to impose terms and conditions that are inconsistent with making APIs open. One approach we recommend is for payers to establish minimum terms of service that are generally applicable to all of a payer's open and proprietary externally facing APIs, similar to the terms represented in Appendix C. Payers can then apply specific terms of service that are only applicable to proprietary APIs, and include a provision allowing specific terms to take precedence when they are inconsistent or in conflict with the general terms.

Health Plan Directory. In order to achieve an ideal consumer experience, developers need access to information that (i) helps consumers to easily search for their health plan and payer using the application's search functionality, (ii) helps developers know whether data from a particular consumer's plan can be accessed through a FHIR-based data connection, (iii) directs developers to the appropriate Auth Server URL, and (iv) identifies the FHIR Server URL a developer should call using the authorization granted by the consumer.

Supporting this workflow can be as simple as typing a single recognizable company name or brand in a search feature, being directed to a single Auth Server URL where the consumer enters their SMART on FHIR credentials, and directing developers to the payer's single FHIR Server URL to initiate the call. In practice, considerably more information from payers is needed by developers to deliver a seamless consumer experience. Payer policies may not support data access via open member-facing APIs for all of their members, for example. For payers that utilize more than one organizational entity or brand in the marketplace, developers need to know which organization and/or brand names to display, and how to map these displays to the appropriate Auth Server URL(s) and FHIR Server URL(s), particularly when payers support multiple Auth Server URLs and/or FHIR Server URLs. Mappings between Auth Servers and FHIR Servers may also be required when multiple instances of these systems are in use for different lines of business, for example.

For these reasons, the business and technical documentation required by the Rule should include a dynamic health plan directory – as either a stand-alone API or part of the metadata on public-facing

Auth and FHIR Servers. Surfacing this information, including cardinal relationships, allows developers to configure their systems, so that a single member can easily search to determine whether their data can be accessed, be directed to the appropriate Auth Server URL, and quickly receive their data because the developer knows which FHIR Server URL to call for that member using that member's authorization token. We also recommend that Terms of Service explicitly grant permissions for developers to display the payers' applicable organizational names and brands in their search functionality, subject to payers' respective branding guidelines, so that third-party applications can deliver a better search experience for consumers looking to access their personal health information.

Notification of Documentation Updates. Section 170.404(a)(4) also requires HIT developers of certified API technologies to provide notice of updates to their documentation – including their terms of service – and a reasonable opportunity for API users to update their applications to preserve compatibility with the certified API technology and to comply with the applicable terms of service. ONC recommends posting the updates on the website (commonly done as a Change Log [see https://stripe.com/blog/changelog for a non-health care example]), as well as contacting registered users directly before updating the business and technical documentation, consistent with the ONC Rule. See 85 Fed Reg 25642, 25750 (May 1, 2020). We agree that this mode of direct outreach to developers is a best practice that payers should also implement. For further discussion, see Section 5.5.3, below.

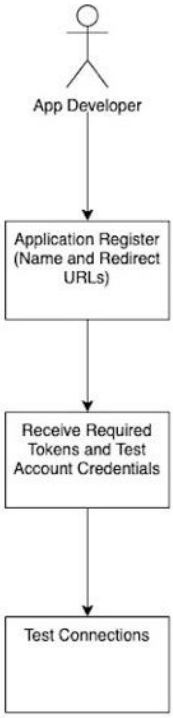
5.2. Sandbox Environment

The Rule does not require CMS-regulated payers to set up a sandbox environment, but sponsors of API ecosystems customarily offer sandbox environments as a resource to encourage developers to participate in these ecosystems. For this reason, we believe CMS-regulated payers should develop and maintain a sandbox environment for each of their supported APIs.

An API sandbox is an environment that replicates the current production environment for a given API. As a testing environment, the sandbox should not expose HIPAA-protected health information. For this reason, no HIPAA business associate agreement is necessary. The terms or conditions of access or use described in Appendix C should be sufficiently broad to cover an app developer's access and use of the payer's API sandbox to test its open APIs, before proceeding to register an application for the production environment.

Figure 5.2 represents the workflows and processes discussed in this Section 5.2.

Figure 5.2 Process Diagram - Registration for Sandbox Environment



Sandbox Accounts. In the wider development community, technology companies routinely require individual developers to create an account before granting access to a sandbox. Creating this account should be allowed to occur as a preliminary step before a user decides to register an app, for several reasons: (1) the individuals requesting access to a sandbox are technically-oriented developers or engineers whose roles and responsibilities may not include authorities to make the legal, business, or technical representations that are required as part of the registration process; (2) the development effort involved in building and testing connections usually occurs before an organization is ready to register an app for the production environment, or as updates to a registered app are being tested before general release; and (3) the organization might register more than one application, or add additional applications at a later time, some of which may require different representations to be made.

For this reason, we recommend that a developer be able to quickly register an account with only an email, password, and redirect URL. This would then generate a client ID and client secret that the developer can use to authenticate and test against the sandbox environment. An app developer could complete the full app registration process at a later time, using the same account if desired.

Test Data. Payers have a choice between populating the sandbox environment with de-identified or synthetic representations of member data. Either approach can work. Whichever approach is selected, payers are reminded that their use of de-identified data may not serve as a pretext for obligating app developers to sign a HIPAA business associate agreement. As CMS explains in its

Preamble to the Rule, "[i]t would not be appropriate to require a member-designated third party to enter into a BAA with payers as the API-facilitated exchange is taking place per the request of the member and not by, on behalf of, or in service to the payer." See 85 Fed Reg 25510, 25548-25549 (May 1, 2020). If payers wish to limit the scope of permitted purposes regarding de-identified or synthetic data, payers can include relevant provisions in the terms and conditions posted on their respective developer portals.

Test Cases. When developing the test data, care should be taken to include all data elements and classes that must be supported by the open APIs. Otherwise, app developers will not be able to create simulated responses for all foreseeable use cases. If the payer does not maintain clinical data in a USCDI-represented format as part of its normal business operations, payers should explain that clearly in their publicly accessible documentation. As a best practice, we recommend that payers include functionality in their sandbox environment that enables users to save, organize, and reuse the requests representing their test cases in Postman collections, or similar utilities.

5.3. App Registration

Information Collected from App Developers. When app developers register for connections to payers' production environments, payers are permitted to collect information that is relevant to their security risk analyses under the HIPAA Security Rule. However, payers cannot whitelist (that is, limit access to) applications based on the applications' respective data practices or privacy protections. See 85 Fed Reg 25510, 25548 (May 1, 2020) ("Payers cannot place additional constraints on apps, such as requiring a BAA, additional security audits, or requiring apps to make commitments about how it will or will not use the information members store on it"). Also, CMS declined requests from commenters to specify the information that can be requested and maintain compliance with the Rule. To address this gap, Section 5.3.1 offers recommendations about the information that payers can collect, and the role of that information in performing a security risk analysis to comply with the Rule's requirements.

Educational Resources. In addition, the Rule requires payers to provide general information to members in non-technical, simple, and easy-to-understand language about the steps members can take to help protect the privacy and security of their health information. This information is intended to help members understand when their data may not be protected under HIPAA, understand the different oversight responsibilities of the HHS Office of Civil Rights (OCR) and U.S. Federal Trade Commission (FTC), and explain how members can submit a complaint to OCR or the FTC. CMS points to its own experience with implementing Medicare Blue Button 2.0 for guidance. Section 5.3.2 considers CMS' Medicare Blue Button content and workflows and offers a prototype for communicating this educational content as part of a payer's OAuth workflow.

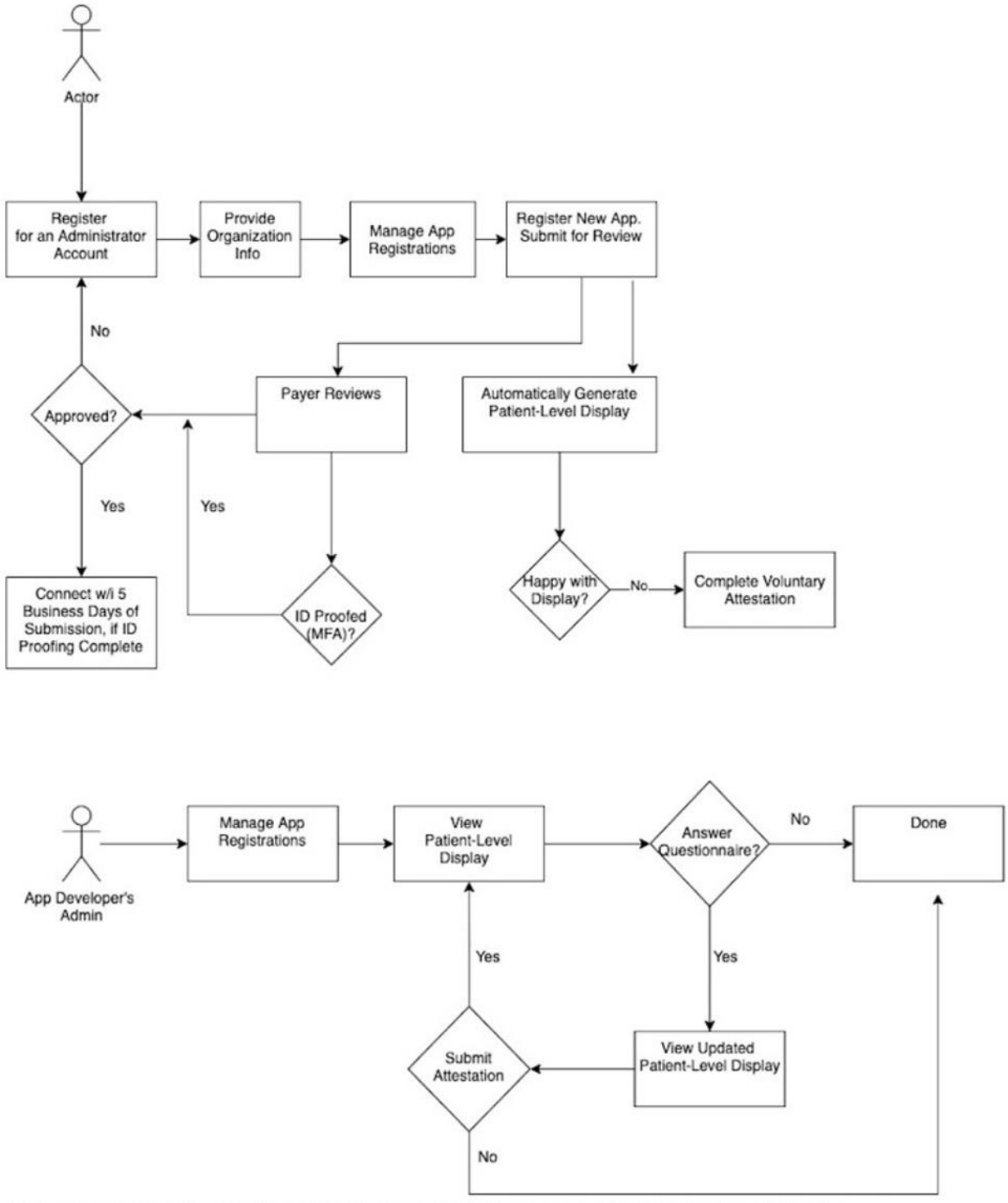
Attestation Framework. While not requiring it in the Rule, CMS encourages payers to implement a framework for asking developers to describe the data practice and privacy provisions of the apps they want to connect to open APIs. CMS believes an attestation framework would help payers educate members about their options when choosing a third-party app and recommends that payers turn to the ONC Model Privacy Policy and the CARIN Alliance Code of Conduct for guidance on setting up their own attestation models and workflows.

Section 5.3.3 offers suggestions for developing an attestation framework that is aligned to the CARIN Code of Conduct. As detailed more fully below, the suggested framework includes an assessment questionnaire that is modeled after the questionnaire that the CARIN Alliance uses as part of its voluntary attestation process on MyHealthApplication.com. As described more fully in Section 5.3.3, developers that have already voluntarily attested to the CARIN Code of Conduct, or that have undergone an independent third-party review by completing EHNAC TDRAAP Certification or Accreditation (which includes this attestation and other requirements) would be able to bypass detailed questions that they have previously answered as part of CARIN's voluntary attestation process.

For developers that have not voluntarily attested to or received independent certification of their compliance with the CARIN Code of Conduct, their responses to questions in our proposed Assessment Questionnaire, presented in Appendix E, can be used by payers to provide contextualized content about the areas where an application's data practices align to and differ from CARIN Code of Conduct data practices, assuming that the payer has already introduced educational resources about the CARIN Code of Conduct. As with the general educational resources presented in Section 5.3.2, we include links to a prototype that payers can reference to display application-specific content about a developer's data practices as part of their respective OAuth workflows.

We envision that data collection from app developers and the sharing of OAuth workflows with app developers will be integral to the app registration workflow, depicted in Figure 5.3. We describe this workflow in the discussion that follows the diagram, and in the commentary that follows in Sections 5.3.1 through 5.3.3.

Figure 5.3 - Process Diagram - Registration for Production Environment



For the app registration workflow, payers will collect personal data from any actor that self-identifies as the developer's representative (administrator) and grant a login credential that allows

the administrator to register the developer and its applications to the production environment. (The credential could be the same credentials authorized for a user that accesses the sandbox environment, but as discussed in Section 5.2, credentials for accessing the sandbox environment should be available to any developer, while app registration functionality should be limited to users that represent themselves as a developer's authorized representative.) Before establishing any API connection in the production environment, the user requesting access to the app registration workflow should be verified. Under the terms and conditions of use described in Appendix C, individuals holding themselves out as a developer's authorized representative agree that their digital representations have the power to contractually obligate the developer organization.

The developer's administrator is ultimately responsible for providing information about the developer's organization and the application(s) to be registered. The scope of information collected should be limited to what is needed to complete an appropriate and documented security risk analysis – as described below in Section 5.3.1 – and to populate some of the displays that members see when they participate in the OAuth process.

We believe a good practice in transparency is for these member-facing displays (described more fully in Section 5.3.2) to be presented to an app developer's registered users. That way, an app developer can correct mistakes before submitting a registration request and, as needed, communicate any concerns about the look and feel or content of displays to payers' technical points of contact.

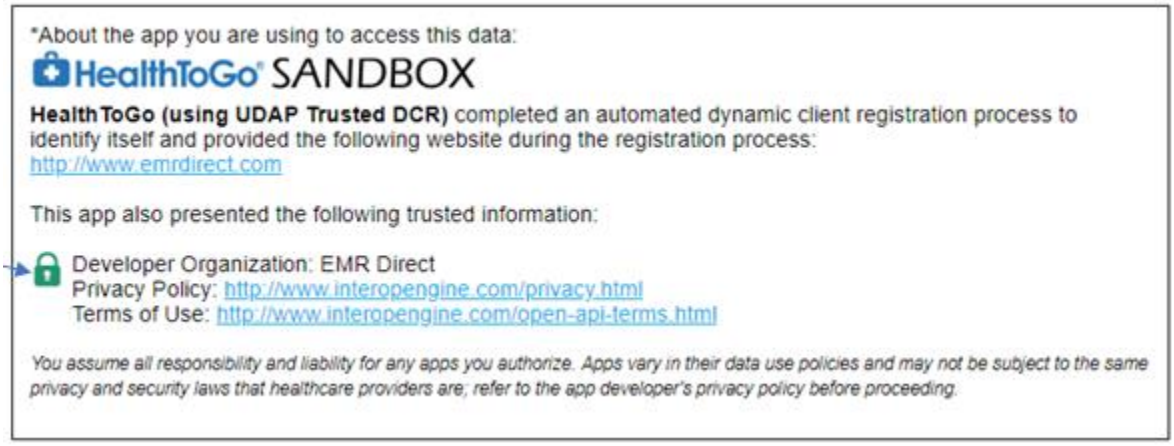
We recommend that the member-facing displays shared with developers during the registration process include links to the minimum educational resources required by the Rule (described more fully in Section 5.3.2), the name of the application, and a link to the application's terms of service and privacy policy (described below in Section 5.3.1).

The workflow would also invite (but not obligate) the administrator to complete a voluntary data use and privacy assessment questionnaire, as part of a CARIN Code of Conduct-based attestation framework that CMS encourages in the Preamble accompanying the Rule (described in Section 5.3.3). Opting for independent third-party privacy and security assessment through EHNAC TDRAAP Certification or Accreditation would be another way for client apps and servers to voluntarily signal a strong security posture and protection of member privacy.

Support for Scalability and Advanced Security. Payers are also encouraged to support the UDAP framework.[12] The UDAP framework introduces the concept of digital certificates issued to app developers and other ecosystem participants by third-party certificate authorities or "endorsers." Under this framework, payers select the endorsers they choose to trust. Endorsers assume the responsibility for validating the claims that app developers would otherwise make if they registered manually with an API endpoint. The digital certificates and assertions issued by trusted endorsers communicate validated attributes about the app developer, and the application underlying digital

[1] The profiles constituting the UDAP (Unified Data Access Profiles) framework are available at http://www.udap.org.
[2] Seib, A., Maas, J., Scrimshire, M., Maas, L., "Scaling Dynamic Client Registration and Endpoint Discovery for Open APIs," (February 2019), accessed July 12, 2021, provides an overview and some additional background about the UDAP framework.

certificate status information can also be dynamically discovered. Payers that support the UDAP framework would likely continue to support the manual app registration workflows, but in effect provide a faster "toll road" for app developers that present a trusted endorser's digital certificate or signed assertion. They would also be able to rely on an endorser's ongoing monitoring of an app's compliance with the endorser's policies for maintaining the certification or endorsement. UDAP-compliant systems display the UDAP green lock to indicate the verified attributes originating from a client app's digital certificate issued by a trusted endorser, or assertions validated with a trusted endorser's digital certificate, as in the screen shot provided below. App developers have the option as well of displaying the green lock before navigating a member to the payer's trusted FHIR endpoint, giving members confidence that they are not entering their credentials at a malicious server.



Supporting the UDAP framework also helps payers prepare their API endpoints for IAL2 compliant methods of consumer authorization and identity authentication. The UDAP framework includes a strategy for leveraging digital certificates to assert verified identity attributes, to sign these assertions, and to validate trust with the issuer of a digital credential at a specific identity and authentication assurance level. This step up to digital certificates for stronger endpoint identity assurance and dynamic discovery is a path that FAST, Carequality, CAQH and others in the health data interoperability community are pursuing for future scalability, security and efficient management of the health API ecosystem. More information can be found in the UDAP Implementation Guide for Registration and Authorization of Consumer Facing Health Apps, which is linked under the Authorization, Authentication and Registration section of the CARIN Consumer Directed Payer Data Exchange STU 1.1.0 ("CARIN Blue Button Implementation Guide").

Functionality for Multiple Users. While the app registration workflow needs to minimally support an administrator account, sponsors of API ecosystems in the wider technology community routinely permit an app developer's administrator to create and manage accounts for the developer's other organizational users. This functionality has multiple advantages for payers that support externally-facing open and proprietary APIs. It allows the administrator to designate an organizational user as the business owner, who would then be the authorized representative that consents to applicable terms of service. Likewise, the administrator could designate the organizational users with

appropriate knowledge of an application's (a) security practices and/or (b) privacy practices to view and complete the attestation process.

Management of Multiple Application Profiles. Payers should anticipate that the health care information exchange ecosystem will include app developers that build and maintain API connections for multiple applications and multiple organizations. For this reason, app developers should be able to manage multiple application profiles using the same login credentials for the sandbox and production environments.

5.3.1. Security Risk Considerations

The Rule in its final form only allows a payer to deny or discontinue a third party application's connection to the API if the payer --

1. Reasonably determines, consistent with its security risk analysis under the HIPAA Security Rule that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of PHI on the payer's systems, and
2. Makes this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers through which members seek to access their ePHI, including but not limited to criteria that may rely on automated monitoring and risk mitigation tools.

According to CMS, some commenters encouraged CMS to develop and/or further define guidelines for identifying "unacceptable risk" and establish a clearer standard for acceptable circumstances when API access can be restricted or denied. See 85 Fed Reg 25510, 25547 (May 1, 2020). CMS declined to establish this standard, observing instead that "it is the responsibility of payers to assess the risk to their system and act accordingly." See 85 Fed Reg 25510, 25548.

CMS explains in its Preamble accompanying the Rule that payers have limited discretion to deny registration applications from developers, due to a number of intersecting regulatory considerations, as follows:

- Individuals have a right of access to their data, and therefore have a right to choose the apps they wish to use for collecting their personal health information.
- CMS (and therefore the payers they regulate) do not have authority to regulate third party applications.
- Covered entities and business associates are not responsible for data after ePHI has been securely transmitted to the intended recipient under the HIPAA right of access; instead, app developers are accountable to members under their respective terms of service and privacy policy, and subject to the investigatory and enforcement authorities of the FTC and state agencies responsible for enforcing applicable state laws and regulations.
- Standards-based APIs are secure methods of data exchange, assuming they have been properly implemented.

- Nothing in the Rule alters payers' existing obligations under the HIPAA Security Rule to establish criteria and processes for assessing unacceptable risks to their systems, which include performing a risk analysis as part of their security management processes.

When conducting a security risk analysis, payers must consider the likelihood that their systems could be compromised by an app developer that is connected to payers' open, member access FHIR-based API endpoints. In turn, payers must consider inherent security features of these endpoints.

These endpoints are required to be implemented according to ONC's technical standards. If properly implemented, the vulnerabilities to payers' own systems can be significantly mitigated, due to certain security attributes. Among other attributes, (a) all transmissions between conformant open APIs and the app developer's interfaces are encrypted, (b) app developers connected to member access APIs lack access to the member's credentials, and (c) open APIs are only implemented as "read only" endpoints. The responsibility for mitigating these risks ultimately lies with the payers and their implementers. Accordingly, as long as payers' implementations of open APIs conform to the ONC's technical standards, in particular regarding the OAuth 2.0 Authorization Framework, the security risks to PHI in payers' own systems should be significantly reduced.

Given the ability of payers to mitigate risks, payers need to define the scope of information that is appropriate for them to collect from app developers during the registration process, consistent with an appropriately scoped security risk analysis. In our view, the scope of information collected should be dictated by three considerations, described below and listed in Table 5.3.1:

1. **Binding contract.** The payer should collect the minimum necessary information to make the terms of service legally binding, and to serve legal notice. For an individual, this information would include the registrant's full name, date of birth and residence. For a legal entity, this information would include the full legal name, entity status (LLC, Inc., etc.), the state where the entity is organized and a street address (not a P.O. box) for the developer headquarters or other place of business. The administrator should also provide the contact information for the primary technical and business points of contact, if different from the administrator.
2. **Nefarious domains and IP addresses.** Payers should collect the website URL for the app developer and all redirect URLs associated with a given application. Minimally, a security risk analysis would involve review of the corporate website URL and confirm the relationship between the developer and the redirect URLs. URLs or IP addresses could also be analyzed against suspicious URLs or IP in public or commercial threat intelligence registries as the ecosystem for member access APIs matures.
3. **Manage an application's connections.** Finally, as part of the registration workflow, an app developer should collect the minimum information needed to manage an application's connections and the member experience. This information should include the name of the app, relevant URLs (for non-mobile apps), links to the app's main page(s) in the Apple App Store and Google Play store (as applicable) and links to the application's terms of service and privacy policy. Also, because an app developer may be a service provider to another entity that offers the app to end users, the payer should request the legal name for the organization that offers the application to members. As a rule of thumb, this can be determined by the party named in the application's terms of service and privacy policy.

Table 5.3.1 - App Registration Workflow - Information Requested, and Verification Methods

Information Requested	Verification Methods
About the Developer	
What's the legal name for the developer requesting an API connection?	1. Check corporate information against public records. o Most jurisdictions support business entity search features through their respective corporation departments. 2. Use public or subscription-based business look-up services to validate legal existence. 3. Validate the developer's provided email address and phone number. 4. Use a recognized third-party legal entity verification service. The CARIN Alliance recommends using the Global Legal Entity Identifier Foundation (GLEIF) which is used and accepted globally across multiple countries, regulators, and industries. (https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei).
What type of legal entity is the requestor (e.g. corporation, partnership, LLC, sole proprietor)?	
Under the laws of what jurisdiction is the entity organized?	
What is the name, job title, phone number and email address for the registrant's primary business point of contact?	
What is the name, job title, phone number and email address for the registrant's primary technical/developer point of contact?	
What is a physical address for the entity (not a P.O. box)? (home address for a sole proprietor)	
What is the URL for the entity's corporate website?	
About the Application	
What is the name of the application?	1. Validate information against provided links. 2. Check domains and IP addresses for the application and redirect URL against blacklists of malicious domains that are associated with undesirable and/or illegal activity. o There are both commercial and public threat intelligence services available, o An example of one commercial service is offered by Anomali, https://www.anomali.com/marketplace/threat-intelligence-feeds.
If different from the developer, what's the legal name for the owner of the application, according to its terms of service and privacy policy?	
Redirect URLs	
As applicable, what is the application's: • Homepage URL? • iOS store link? • Android link? • Legal Terms of Service URL? • Privacy Policy URL?	

We selected the information in Table 5.3.1 because it can be verified through independent, objective and observable resources, without unreasonable effort, and, we believe, a low turnaround time. We note that ONC requires a five-business day turnaround time for registration decisions under Section 170.404 of the ONC Rule. However, CMS did not incorporate this requirement under its Rule. Payers should consult with their legal counsel whether to incorporate the five business day turnaround time as an organizational policy, or other time period. When setting that time period, payers should consider their concurrent obligations under the HIPAA right of access. Under proposed modifications to the HIPAA right of access, the proposed turnaround time would be reduced, for example.

5.3.2 Member Educational Resources

The Rule requires payers to develop member educational resources that helps members take an active role in protecting their health information. These resources are not just intended for consumption during the OAuth workflow. The Rule requires that these resources be easily accessible on payers' public website, and through the mechanisms ordinarily used to communicate with their current and former members, enrollees or beneficiaries.

Mechanisms. To comply with these provisions of the Rule, payers should first take an inventory of the mechanisms they ordinarily use to communicate with their current and former members, and then provide appropriate content or links to the payer's authoritative educational resources. Examples of mechanisms to include in that inventory can include:

- The footer on a payer's public home page.
- An online Privacy Center or similar collection point for relevant disclosures about payers' data practices, including its HIPAA notice of privacy practices.
- Member portals.
- The terms of use, and associated privacy policy, that are linked to a payer's OAuth workflow.
- The payer's HIPAA notice of privacy practices, under disclosures pertaining to individual rights.
- Periodic print mailings of payers' privacy policies.

Educational Content. Under the Rule, all educational resources need to be communicated in non-technical, simple and easy-to-understand language. The Rule also requires information about steps a member should consider taking to help protect the privacy and security of their health information, including factors to consider in selecting an application including secondary uses of data, and the importance of understanding the security and privacy practices of any application to which they will entrust their health information. In addition, the Rule requires payers to provide an overview of the types of organizations or individuals that are likely to be HIPAA covered entities, as well as information about the oversight responsibilities of the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC), and how a member can submit a complaint to The HHS Office for Civil Rights (OCR) (https://ocrcas.ed.gov/); and The Federal Trade Commission (FTC) (https://www.ftc.gov/news-events/press-releases/2020/10/ftc-announces-new-fraud-reporting-platform-consumers).

In the Rule's Preamble, CMS suggests that payers turn to Medicare Blue Button 2.0 as an informative resource for developing their educational resources. In follow-up sub-regulatory guidance to payers about educating members, CMS also lists a number of questions that payers can encourage members to ask themselves regarding a third party application's data practices. By way of example, CMS recommends asking members to consider the following questions --

- What health data will this app collect?
- Will this app collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
- How will this app use my data?
- Will this app disclose my data to third parties?
- Will this app sell my data for any reason, such as advertising or research?
- Will this app share my data for any reason? If so, with whom? For what purpose?
- How can I limit this app's use and disclosure of my data?
- What security measures does this app use to protect my data?
- What impact could sharing my data with this app have on others, such as my family members?
- How can I access my data and correct inaccuracies in data retrieved by this app?
- Does this app have a process for collecting and responding to user complaints?
- If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data?
- What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?
- How does this app inform users of changes that could affect its privacy practices?

We note that the CMS Medicare Blue Button 2.0 resources do not provide an exact match of all the information required by the Rule. In light of these considerations, we have created an interactive prototype that demonstrates how to communicate these educational resources within the OAuth workflow: https://bit.ly/CARIN-Payer-OAuth. A flow diagram of this OAuth experience is presented in Appendix F and a video walkthrough of the prototype is available at https://bit.ly/Patient-Education-OAuth-Demo.

5.3.3. Voluntary Attestation Process

Appendix D lists informative resources for developing an attestation framework. Because CMS encourages payers to consult the CARIN Alliance Code of Conduct, this Guide offers an approach for implementing an attestation framework that aligns to the CARIN Code of Conduct. This approach begins with the data use and privacy assessment tool attached hereto as **Appendix E**.

The questionnaire in Appendix E is a modified version of the CARIN Alliance Member-Facing Implementation Guide, v.6.0 ("PFIG v6"), which the CARIN Alliance uses to collect representations from developers that wish to voluntary attest to the CARIN Code of Conduct. Developers that voluntarily attest to the CARIN Code of Conduct are listed on the CARIN Alliance's MyHealthApplication.com website. They can also earn the privilege of publishing a CARIN Attested trustmark on their website and in app stores like Apple App Store and Google Play.

The questionnaire offers a way for developers that have already voluntarily attested to the CARIN Code of Conduct to bypass questions they would have already answered from the PFIG v6 if they voluntarily attested to the CARIN Code of Conduct. Remaining developers answer these questions as part of a payer's own attestation workflow.

If feasible, we believe a good practice for a payer's attestation workflow is to include a real-time, auto-generated update to the member-facing displays, based on responses provided in their attestation workflow. Incorporating this transparency allows developers to confirm that their questionnaire responses in are accurate before submitting their attestation, communicate any concerns about the updated display to the payer's technical points of contact, and ultimately decide if they want to participate in a payer's attestation process, or decide later. This approach also allows app developers to submit new attestations over time as they update the terms of service and privacy policies of their applications.

When designing member-facing displays, payers should exercise care not to design displays that materially discourage members from connecting their choice of application with their open APIs. It's also important not to penalize developers that either (a) choose not to complete the attestation workflow or (b) have not already voluntarily attested to the CARIN Code of Conduct through CARIN's MyHealthApplication.com. The decision for a developer to participate in the attestation workflow should be voluntary. The app registration workflow should be designed so that the attestation is informative to developers and regarded as a "nice to have", rather than a "must-have". If developers choose not to submit an attestation, the general information required by the Rule should be perceived by developers as a neutral, acceptable alternative.

The display should also make clear that the developer is the source of information presented. That way, payers do not interpose themselves between members and the developer of the applications they use.

Another consideration for payers, which will influence developers' acceptance of any attestation process, is whether the updated member-facing displays fairly and accurately characterize an application's particular data practices, and not attempt to summarize these practices. By way of example, the display should not assume that the developer responsible for registering an application is also the application's sponsor. Payers should anticipate that other HIPAA covered entities will contract with an app developer to build and maintain white-labeled applications. Accordingly, the developer – and not the white-labeled sponsor for an application – is likely to complete the app registration workflow, answering questions about the application's data practices on behalf of the sponsoring entity. A good rule of thumb is to include the application's name, rather than the application developer, in the member-facing display. If the display does include an organization's name, make sure that the entity listed is the same one that has a contractual relationship with the member under the application's terms of service and privacy policy.

These considerations reinforce the need for transparency throughout the app registration process, since the developers are best equipped to know whether language in the member-facing displays provide an accurate representation of the data practices for a given application. Transparent workflows provide developers with a mechanism to communicate concerns or other feedback

concerning the display with the payers' technical team points of contact. Finally, payers can manage their compliance risks more effectively by obtaining developers' consent to the member-facing displays as part of the attestation submission process.

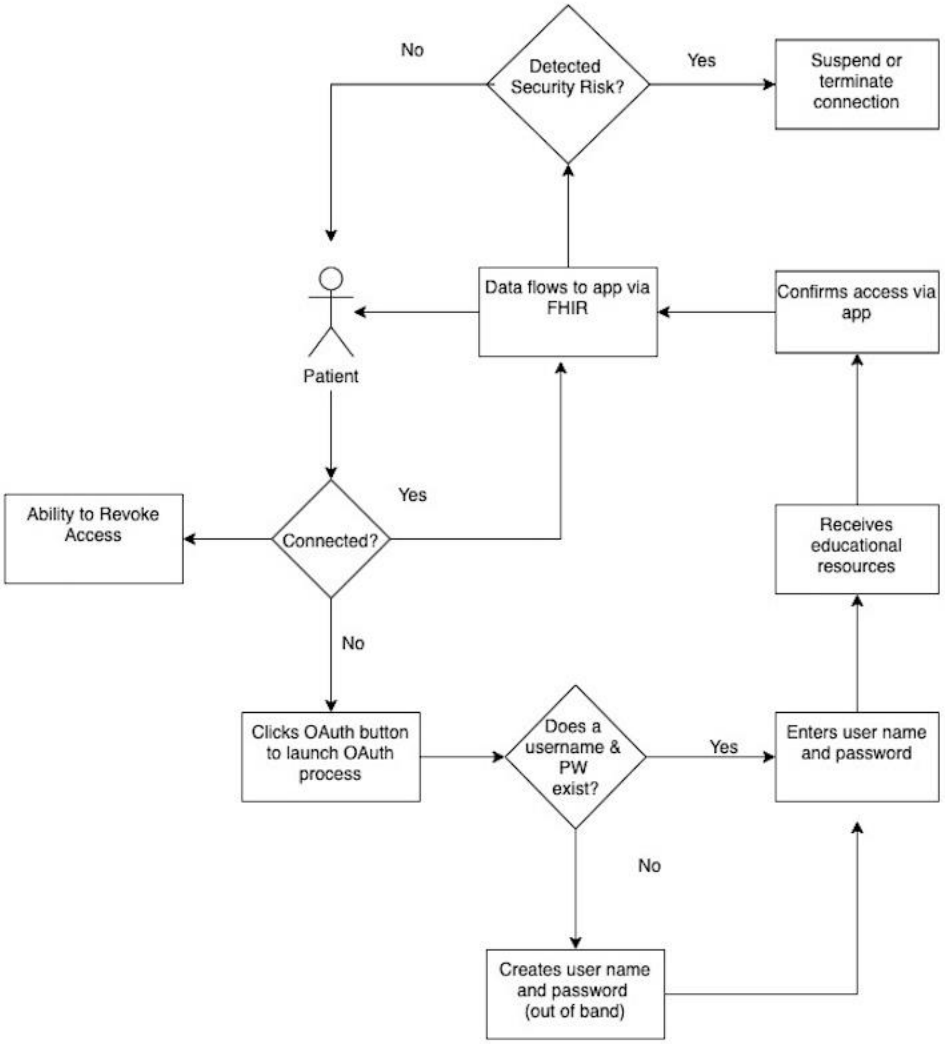
5.4. Member Experience

The Rule requires the SMART on FHIR workflow to be supported, for educational resources to be shared with members, and for payers to conduct routine testing and monitoring of their open API endpoints. The Preamble also permits payers that implement a voluntary attestation framework to provide contextual information about a given application's data practices and privacy protections. The Rule also permits payers to suspend or revoke an application's access when it presents an unacceptable security risk to the payer's own systems. Otherwise, the Rule is silent about the member workflow.

Notably, the Rule is silent about policies that payers should adopt when members use applications that are not capable of storing a client secret. Likewise, the Rule is silent about the duration of refresh tokens when members use applications that are capable of storing a client secret. A payer's policies about these issues can dramatically increase or decrease the ease (or "friction") with which a member can receive ongoing streams of their personal health information, and thereby impact a member's perceptions about a given application. Another topic where the Rule is silent concerns revocation.

We consider these and other policy questions in the following discussion. We start by walking through a process diagram of the member experience, as detailed in Figure 5.4.

Figure 5.4 - Process Diagram - Member Experience



Member-Facing Displays. As described in Section 5.3.3, payers should exercise care not to design displays that materially discourage members from connecting their choice of application with their open APIs. Some early implementations of open member access APIs include red box or black box "warnings" that are problematic because they interpose the implementer's judgment about the risk to members of connecting using a specific application and could implicate rules prohibiting information blocking when these rules apply. Our recommendation is that payers and other implementers design a user experience that is neutral and focuses on consumer education. The general education required by the Rule can be enriched detail that surfaces through an attestation workflow, but developers should not be penalized for participating in the payer's attestation workflow. As described above in Section 5.3.3, the choice to participate in a payer's attestation framework should be regarded as a net-positive to developers. If developers choose not to submit an attestation, the general information required by the Rule should be perceived by developers as a neutral, acceptable alternative. Also, any displays containing information about a developer's data

practices and privacy protections should make clear that the developer is the source of information presented. That way, payers do not interpose themselves between members and the developer of the applications they use.

Health Plan Directories and Limited Branding Rights. Sharing with developers the information described in Section 5.3.1 as a health plan directory will also help alleviate friction.

Use of Multifactor Authentication (MFA). Payers should prompt the member to enter in a MFA credential if MFA has been enabled on the member's account. This prompt should take place directly after the user enters in their username and password combination during the authentication flow. In addition, the CARIN Alliance has also recommended the use of the FIDO2 specifications which includes the use of the W3C's Web Authentication (WebAuthn) specification and the FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP) which eliminates the need for user names and passwords.

Proxy Implementation. Payers can optionally choose to implement in handling for proxies. If proxies are enabled, when a user is going through authentication flow, they would then be shown a screen after authentication and education screens where they'd select the user who's information they're looking to connect to the consumer application. Once selected, the application would only be able to access information associated to the user selected with that access/refresh token.

Endpoint Connections - Duration of Refresh Tokens. From a member's perspective, the starting point is whether the member's chosen app is currently connected to the open, member-facing API endpoint. If so, then new data will flow into the member's application, without interruption or manual intervention.

Refresh tokens are commonly used in health care and other industries to provide seamless integration of systems with other applications, while reducing the need for the burdensome process of re-authentication and re-authorization. At open APIs, the ability to revoke refresh tokens gives payers an important tool for protecting their systems if connections with a particular app presents an unacceptable security risk to their own systems. Absent a reasonable determination of this risk, the Rule does not authorize payers to set a time limit on refresh tokens but does reference the ONC rule on this topic. The ONC rule states:

§ 170.315 2015 Edition health IT certification criteria.

(10) Standardized API for member and population services.

(v) Authentication and authorization—(A) Authentication and authorization for member and user scopes—

(1) First time connections—(i) Authentication and authorization must occur during the process of granting access to member data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b). (ii) An application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months.

(2) Subsequent connections. (i) Access must be granted to member data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. (ii) An application capable of storing a client secret must be issued a new refresh token valid for a new period of no less than three months.

Setting time limits on refresh tokens will require members to re-authenticate and re-authorize at a high frequency, which could inhibit member access. For this reason, payers need to consider their compliance obligations under the Rule before imposing unreasonable time limits on refresh tokens, as detailed in Section 5.3.1 above. Specifically, policies to set time limits on refresh tokens would need to be based upon a reasonable determination consistent with the ONC Rule guidance above and a security risk analysis under the HIPAA Security Rule. This determination would need to be made using objective, verifiable criteria that are applied fairly and consistently across all applications and developers.

In most cases, arguments for setting time limits for refresh tokens due to security concerns can be mitigated with the implementation of revocation API endpoints or via developer portal in the case that an app developer's app is compromised. It's recommended that you allow for developer's to easily handle revocation in the event that they become aware of such as compromise.

Consumer Revocations. When members are connected, they should also have the flexibility to revoke access. The Rule does not specifically address revocation patterns or incorporate relevant provisions of the ONC Rule that requires developers of certified API technology to demonstrate that their technology can revoke refresh tokens where appropriate. In the absence of affirmative regulatory requirements, we make the following recommendations:

- At minimum, payers should provide functionality that allows members to revoke access through their own systems.
- Optionally, the educational resources provided to members can include advice that members understand how to revoke access through their chosen applications.
- Additionally, payers can ask developers to attest that their applications give members the ability to revoke access, if they implement an attestation process.

When members initiate a revocation through the payer, members should receive a confirming email of the member's receipt of the revocation request, and as needed, a follow up email when the revocation request has been implemented. Payers should also provide a contemporaneous notification to app developers' organizational users. We recommend that these notifications be displayed in the dashboards that an app developer's registered users see when they are logged into a payer's app registration environment. Consistent with Fair Information Practice Principles and the CARIN Alliance Code of Conduct, we would also expect app developers to provide accessible mechanisms for members to revoke an application's access to their personal health information, but these expectations lie outside the scope of this Guide. Readers are directed instead to the CARIN Alliance's App Developers UX Compliance Guide, accessible at https://carinuxguide.arcwebtech.com/.

SMART on FHIR (OAuth 2.0) Connection. If members are not connected, they'll need to initiate the OAuth process. From a member experience perspective, the OAuth process appears as a workflow within a registered application, but much of the OAuth workflow is managed by payers. App developers implementing the OAuth process will probably navigate members to a "health data connection" resource within their application, where members will be presented with a directory, drop down or similar feature that allows member to view the names of the payers with which the application has established API connections. Members would also be able to select the payer(s) with which they'd like to establish data connections using the application. These payer lists should include the familiar trade names of payers. If a payer operates under multiple names or DBAs, payers' documentation should let developers know how these names should be listed, and for the avoidance of doubt, grant a license in the general terms of service that allows registered applications to list these names in their application and related materials for this purpose. Payers should also facilitate access to this information to app developers in a programmatically digestible way.

Since the Rule only applies to a subset of payers' lines of business (e.g. Medicare, Medicaid and QHPs, but not commercial business lines), payers' documentation should clearly specify which lines of business are supported at their open member access API endpoints. That way, app developers can incorporate these business conditions into their application workflows and provide appropriate expectations for their member end users like which lines are supported and which are not currently for these connections.

Once members have selected a payer for a health data connection, the application will need to validate/pull the payer's authorize endpoint from the metadata endpoint (for more information about metadata endpoints (aka capability statements, see Section 5.5.1). The application would then build a request to this endpoint that contains the following information:

- Client ID
- Response type
- Redirect URL (to be validated against ones on file)
- Scope
- State
- Aud Claim (Audience)

Once a request URL is built, the application will direct members to the payer's authorization page. At this page, members will be prompted to enter their username and password, to authenticate against the payer's identity server. If a member doesn't have a username and password (or doesn't remember their login credentials), payers can redirect the member to their identity server, where members can securely create or reset their credentials.

After a member submits their credentials, and the payer authenticates them, the payer will direct members to the educational resources required by the Rule and described in Section 5.3.2. This would also be the point when payers would present information obtained from developers about their data practices and privacy protections through a voluntary attestation framework, as described in Section 5.3.3.

After members consume a payer's educational resources, they'll be asked to confirm the application's authority to access and receive their personal health information. After confirming this access, the payer's server will make a request back to the app developer's redirect URL passed in the initial request containing the originally passed state variable and the generated authorization code.

The application would then make one additional request to the authentication/token endpoint using the

- Authorization code
- Client ID
- Client secret

This request will generate the actual access token, token expiration time, refresh token, and member id (full list including optional parameters available at http://hl7.org/fhir/smart-app-launch/index.html#step-3-app-exchanges-authorization-code-for-access-token) which can then be used going forward for all subsequent FHIR API calls in scope along with being able to exchange this token for a new one via the refresh token process.

5.5 Service Level Expectations

The Rule provides that CMS-regulated payers must perform routine testing and monitoring, to ensure proper functioning of their API endpoints. To be consistent with expectations in the wider API technology community, we recommend that payers voluntarily commit to provide support and other services reasonably necessary to enable the effective development, deployment, and use of their open APIs in production environments. These service level agreements (SLAs) should be included with the business and technical documentation that payers publish and make publicly accessible on their Developer Portal.

These SLAs should address topics that address the duration of session tokens (as discussed in Section 5.4 "Endpoint Connections - Duration of Refresh Tokens), planned downtime, unplanned downtime notifications, and security considerations that justify status changes in an app developer's API connections, and permissible status changes, such as session tokens of time-limited duration, API rate limiting, suspension or termination.

5.5.1. Use of Metadata/Capability Statement Endpoint

As APIs access continues to expand with new APIs and payers continue to update their systems it's important to keep third party applications aware of changes that have taken place programmatically. This is accomplished through the use of the FHIR metadata endpoint (sometimes referred to as the Capability Statement) which provides information such as

- The URLs of the authorize and token endpoints
- APIs which are available to be accessed

This information can then be used programmatically by the third party applications to make sure the application is always using the correct URLs and taking advantage of all of the latest and greatest APIs available to it. This URL endpoint should not be secured behind the SMART on FHIR authorization flow that protects other endpoints and should be available without any authentication.

NOTE: It's important that the location of the metadata endpoint never change once set. If a metadata endpoint is changed, this needs to be broadcasted to the app community along with substantial notice for the switch (ideally with both old and new metadata endpoints existing together).

5.5.2. Routine Testing and Monitoring

If routine testing and monitoring surface conditions that could change the status of an app developer's connections, payers should provide advance notice of those changes, unless a delay would present an unacceptable security risk to payers' own systems. Any such notice would need to be fairly and consistently applied across all applications and developers, using objective, verifiable criteria.

5.5.3. Updates to Business and Technical Documentation

Payers should provide notice of changes to their business and technical documentation – including their terms of service – and a reasonable opportunity for third party app developers to update their applications to preserve compatibility with payers' API technology, and to comply with applicable terms and conditions. We recommend that this notice be provided through multiple mechanisms, including the website via a CHANGELOG and the email addresses provided for the app developer's designated administrator. The metadata endpoint shall also need updates corresponding to the changes that have been made to the actual API endpoints.

5.5.4. Support

Payers' business and technical documentation should specify the mechanisms that app developers should use to report issues in the sandbox or production environments. We recommend that these mechanisms include a toll-free telephone number, online support form and monitored email, and that support concerns be logged as part of payer's obligations to perform routine testing and monitoring of their open API endpoints. Documentation should also specify the business hours and days of operation for receiving support.

We also encourage payers to implement a framework for characterizing and prioritizing incoming requests for technical support, and minimally commit to responding to support requests within specified time periods that are proportionate to the severity of reported support concerns. A representative framework might look something like this:

Severity Levels	Description	Initial Response Targets	Update Frequency
Critical	Production or sandbox system is unavailable; data compliance issues; fatal errors; substantive data loss; widespread impact to all connected members or all an app developer's registered applications; a major component of payer's open API environment is unavailable.	2 Business Hours	Every 3 Business Hours
Major	Production or sandbox system is available, but users cannot perform a substantive task; no workaround exists; issue is substantially impactful to multiple members or applications.	1 Business Day	Every Business Day
Medium/Low	Production or sandbox system is available; normal business operations are minimally restricted. App developer is requesting information about an inconvenience or a cosmetic issue, questions regarding notices or member-facing displays	2 Business Days	Every 2 Business Days

5.5.5 Uptime

Payers' business and technical documentation should include reasonable uptime commitments for their sandbox or production environments. As the ecosystem of open member access APIs expands and matures, we would expect these uptime commitments to float upwards. As a starting point, we recommend adopting a standard methodology for defining uptime, like the following:

Uptime Percentage = (Hours of Operation - Downtime) / Hours of Operation, where

"Downtime" means the period of time per month that the sandbox (or production environment, as applicable) is unavailable (excluding scheduled maintenance periods or times the environment is severely impacted or unavailable due to causes beyond a payer's reasonable control.

"Uptime Percentage" for each month shall be specified by the payer

"Hours of Operation" should be expressed as 24 hours per day, 7 days per week.

5.5.6. Scheduled and Unscheduled Maintenance

Payers' business and technical documentation should include commitments that payers will use their commercially reasonable efforts to notify registered users of their sandbox and production environments of schedule and unscheduled maintenance when maintenance is expected to make the applicable environment unavailable to the user or members.

6. Authors

The CARIN Alliance would like to thank the entire CARIN community for their input, participation, and support as we worked together to gain consensus on the content of the Application Registration guide. We especially want to thank our Primary and Secondary authors for their leadership and the incredible amount of work they put in to help us create this initial draft.

Primary

- Philips Johnson (b.well Connected Health, Inc.) – philips.johnson@icanbwell.com
- Jill DeGraff (b.well Connected Health, Inc.) – jill.degraff@icanbwell.com
- Nathan Hall (b.well Connected Health, Inc.) – nathan.hall@icanbwell.com
- Mark Marciante (Highmark Health Solutions, Inc) – mark.marciante@hmhs.com
- Beverly Buckta (Pfizer) – beverly.buckta@pfizer.com

Secondary

- David Lee (Leavitt Partners / CARIN Alliance) – david.lee@leavittpartners.com
- Ryan Howells (Leavitt Partners / CARIN Alliance) – ryan.howells@leavittpartners.com
- Rosalie Blacklock (Leavitt Partners / CARIN Alliance) – rosalie.blacklock@leavittpartners.com
- The CARIN Alliance Board
- The CARIN Alliance Blue Button® Implementer's Forum
- The CARIN Alliance Application Forum
- The CARIN Alliance Trust Framework Workgroup

7. Revision History

Draft Version 0.1 released for public comment on July 22, 2021.

Appendices

[Content Continues on Next Page]

Appendix A - (Non-Exhaustive) List of Public and Subscription-Based API Directories

1. The "Lantern" API endpoint registry that MITRE Corporation is building under a contract with the ONC (For more information about this open-source project check out https://github.com/onc-healthit/lantern-back-end).
2. CAQH Endpoint Directory: https://www.caqh.org/solutions/caqh-endpoint-directory
3. Change Healthcare's Marketplace and Endpoint Directory: https://marketplace.changehealthcare.com/catalog/ALL

Appendix B - Links to Reference Technical Documentation

Twilio – https://www.twilio.com/docs/api

Slack – https://api.slack.com/

Swagger (f/k/a OpenAPI) – https://swagger.io/specification/

Argonaut R4 OpenAPI Spec – http://build.fhir.org/ig/argonautproject/R4/branches/master/us-core-server.openapi.json

Humana Developer Portal – https://developers.humana.com/

Appendix C - Minimum Recommended Terms or Conditions of Use or Access

[Legal Disclaimer – Provided AS IS with all faults. Offered for Informational and Illustrative Purposes Only.]

Terms and Conditions of Access	
Date Published Effective Date Prior Versions	
Welcome	Welcome. By accessing or using any resource of [Name of Payer] ("we," "us," or "our") that links to these terms and conditions of access ("Terms"), you must agree to these Terms. BY REQUESTING, RECEIVING AND USING AN ACCOUNT, YOU AGREE TO BE BOUND BY THESE TERMS. IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, DO NOT REQUEST OR USE AN ACCOUNT. THESE TERMS ARE NOT INTENDED FOR CONSUMERS. FOR THE TERMS OF SERVICE AND OTHER LEGAL CONDITIONS APPLICABLE TO CONSUMER END USERS, PLEASE GO TO _____. IF YOU ARE NATURAL PERSON AGREEING TO THESE TERMS ON BEHALF OF A LEGAL ENTITY, YOU REPRESENT THAT YOU ARE LEGALLY AUTHORIZED TO CONTRACTUALLY OBLIGATE THAT LEGAL ENTITY TO THESE TERMS. IF YOU MISREPRESENT YOUR AUTHORITY TO CONTRACTUALLY OBLIGATE THAT LEGAL ENTITY TO THESE TERMS, YOUR ACCESS TO SERVICES MAY BE SUSPENDED OR REVOKED BY US. BE ADVISED: THESE TERMS INCLUDE A BINDING ARBITRATION AGREEMENT AND CLASS ACTION WAIVER. IT AFFECTS HOW DISPUTES ARE RESOLVED. We reserve the right to modify these Terms at any time, or suspend any service that links to these Terms ("Services"). If we modify these Terms, we will notify you through your account and by email to the address you have provided us in your account. These notifications will include a link to the updated Terms.

Consent to Electronic Transactions	We collect legally binding consents and other agreements using electronic signatures that are binding per 15 U.S.C § 7001-7006 (the federal E-SIGN Act). You agree that these electronic signatures, represented by the unique identifiers and passwords associated with your account, will bear the same legal authority as your written signature and will be binding per 15 U.S.C § 7001-7006.
Account Creation	To create an account, you will be asked to provide certain information (including identification and contact details) as part of the registration process. You represent and warrant that any registration or identity verification information given to is accurate, complete, and up to date. You must inform us promptly of any updates. Account login credentials (**"Credentials"**) issued by us to you, or your agents or employees are intended to be used only by them on your behalf. These Credentials are not intended for use by multiple individuals. You are responsible for ensuring that individuals granted access to Credentials maintain their confidentiality, and agree not to provide them to any third party. You are responsible for all statements made and acts or omissions that occur while your Credentials are being used. You are responsible for any breach of security caused by your failure to maintain the confidentiality of your Credentials. You agree to notify us immediately in the event of loss or theft of your Credentials, or if you believe the confidentiality of your Credentials has been compromised in any way. We reserve the right to suspend or revoke Credentials and/or access to Services at any time without prior notice for failure to comply with these Terms, or where we reasonably determine that your continued access would present an unacceptable level of risk to the security of our systems.
Minimum Service Requirements	To access Services, you will need access to the internet, a device that connects with the internet and Credentials. You understand that you must, at your own expense, provide all internet, telephone and other equipment and services necessary to access and use our services. We are not responsible for the fees that you incur from unrelated third parties. You agree that the phone number you provide for receiving text messages is registered in the name of your authorized users ("Authorized Users"). You agree that we are not responsible for the security of transmissions of text messages to mobile phones or other devices that do not support password protection or encryption, or which are shared with others.

Conditions of Access	The rights granted to you by us under these Terms are further conditioned upon your compliance with the following terms and conditions. You and your Authorized Users will not: (A) Sell, rent, lease, sublicense, redistribute, or syndicate access to your account; (B) Use your account to access tools, services or documentation in violation of any law or regulation; (C) Access tools, services or documentation in any manner that – (i) Compromises, breaks, or circumvents any of our technical processes or security measures, (ii) Poses a security or privacy vulnerability to customers or users of our Services, or (iii) Tests the vulnerability of our systems or networks; (D) Attempt to reverse-engineer or otherwise derive source code, trade secrets, or know-how from us; (E) Permit the international transfer of personal data; or (F) Delete or in any manner alter the trade names, trademarks, service marks, logos, domain names, and other branding. Further, you must promptly notify our technical support team via email of any known or suspected security or privacy incident.
Ownership	We grant you the right to access and use Credentials, subject to your compliance with these Terms. We further grant you the limited right to display or refer to the Brands listed in Schedule X for the limited purpose of identifying the fact that your application is capable of interfacing, accessing or otherwise interacting with the application programming interfaces covered by these these Terms, subject to your continuing compliance with the branding guidelines referred to in Schedule X. No intellectual property rights are assigned, transferred or conveyed by either party hereunder.
Disclaimers	The Services are provided or made available “As Is,” “As Available,” and with all faults. Information obtained by you will not create any warranties. You assume all risks associated with your access and use of the Services.

Term; Termination	These Terms are effective until terminated by either party. If you no longer agree to be bound by these Terms, you must cease your use of your account. If you breach any provision of these Terms, then you may no longer use your account. If these Terms are terminated for any reason, then these Terms will continue to apply and be binding upon you in respect of your prior use of your account.
Survival	Upon termination of this Agreement, the terms under the following Headers shall survive: Conditions of Access; Ownership, Disclaimers, Limitations of Liability, Indemnification and Entire Agreement; Interpretation.
Limitations of Liability	WE SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM ANY LOSS OF USE, LOSS OF DATA, LOSS OF PROFITS, BUSINESS INTERRUPTION, LITIGATION, OR ANY OTHER PECUNIARY LOSS, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE, OPERATION OR PERFORMANCE OF SERVICES, WITH THE DELAY OR INABILITY TO USE THE SERVICE, ANY DEFECTS IN THE SERVICE, OR WITH THE PROVISION OF, OR FAILURE TO MAKE AVAILABLE, ANY INFORMATION, SERVICES, PRODUCTS, MATERIALS, OR OTHER RESOURCES AVAILABLE ON OR ACCESSIBLE THROUGH THE SERVICE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
Indemnification	You hereby agree to indemnify, defend, and hold us harmless from any liability, loss, claim, and expense (including reasonable attorneys' fees) related to or arising out of your violation of these Terms.

	A. Agreement to Arbitrate This Dispute Resolution by Binding Arbitration section is referred to in these terms as the "Arbitration Agreement." You agree that any and all disputes or claims that have arisen or may arise between you and us, whether arising out of or relating to the terms (including any alleged breach thereof), the services, any advertising, any aspect of the relationship or transactions between us, shall be resolved exclusively through final and binding arbitration, rather than a court, in accordance with the terms of this Arbitration Agreement, except that you may assert individual claims in small claims court, if your claims qualify. Further, this Arbitration Agreement does not preclude you from bringing issues to the attention of federal, state, or local agencies, and such agencies can, if the law allows, seek relief against us on your behalf. You agree that, by entering into the terms, you and we are each waiving the right to a trial by jury or to participate in a class action. Your rights will be determined by a neutral arbitrator, not a judge or jury. The Federal Arbitration Act governs the interpretation and enforcement of this Arbitration Agreement. **B. Prohibition of Class and Representative Actions and Non-Individualized Relief** You agree that each of us may bring claims against the other only on an individual basis and not as a plaintiff or class member in any purported class or representative action or proceeding. unless both you and we agree otherwise, the arbitrator may not consolidate or join more than one person's or party's claims and may not otherwise preside over any form of a consolidated, representative, or class proceeding. also, the arbitrator may award relief (including monetary, injunctive, and declaratory relief) only in favor of the individual party seeking relief and only to the extent necessary to provide relief necessitated by that party's individual claim(s), except that you may pursue a claim for and the arbitrator may award public injunctive relief under applicable law to the extent required for the enforceability of this provision.
Relationship of the Parties	These Terms shall not be interpreted as a joint venture, partnership, agency relationship, or formal business organization of any kind.
Third-Party Beneficiaries	There are no third-party beneficiaries to these Terms.

Notices	When you send emails or other electronic messages to us or in connection with the Service, you are communicating with us electronically and consent to our review and analysis of such messages and to receive return communications, if any, from us electronically. You agree that all agreements, notices, disclosures and other communications that we provide to you through the email address and mailing address you provide through the Service satisfy any legal requirement that such communications be in writing.
Modifications to the Service	The Services are still evolving. For this reason, we reserve the right to discontinue, modify, or change the Services, the information we make available, or the systems and services we use to deliver the Services, at any time and from time to time, with or without notice to you. In such circumstances, we will have no liability or obligation to you.
No Waiver	Our failure to exercise or enforce any right or provision of these Terms shall not constitute a waiver of such right or provision.
Entire Agreement; Interpretation	These Terms constitutes the entire and exclusive understanding and agreement between us and you regarding the Service. These Terms supersede and replace any and all prior oral or written understandings or agreements between us and you regarding the subject matter hereof. Titles and headings of sections of these Terms are for convenience only and will not affect the construction of any provision of these Terms. In the event the following agreements are signed by the partiers, and a conflict or inconsistency exists among the following documents, the order of precedence for purposes of interpretation will be: [Insert Order of Precedence for Agreements Applicable to Proprietary APIs].
Severability	If any provision of these Terms is determined to be invalid under any applicable statute or rule of law, such provision is to that extent to be deemed omitted, and the balance of the Terms shall remain enforceable.
Assignability	Either party may assign, delegate, or otherwise transfer these Terms, in whole or in part, without the other party's consent. Subject to the foregoing, these Terms will be binding on each party and each party's successors and assigns.

Appendix D – (Non-Exhaustive) List of Informative Resources for Developing Educational Resources

CMS Medicare Blue Button and Blue Button 2.0

https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn

https://www.carinalliance.com/who-we-help/consumers-caregivers/

Appendix E – CARIN Code of Conduct: Assessment Questionnaire

Name of Application[3]:

Name of Organization Offering the Application[4]:

Name of App Developer, if different from above:

Instructions for Completing Questionnaire

The individual completing this questionnaire should have an understanding of (1) federal and state laws and regulations applicable to the health data and the Organization offering the Application, (2) the Application's data practices, and (3) the Application's terms of service and privacy policy.

Completed by:

{Name}

{Title}

{Date}

{Phone Number}

{Email Address}

1. Is the organization offering the Application[5]–

   ☐ A HIPAA-covered entity

   ☐ A HIPAA business associate

   ☐ Not a HIPAA-covered entity or a HIPAA business associate

[3] An application can include any consumer-facing application, including a technology-enabled platform, service or tool
[4] List the organization who offers the application to consumers under the Terms of Service and Privacy Policy. Do not list the app developer if consumers do not have a direct contract relationship with the developer.
[5] The U.S. Department of Health and Human Services Office of Civil Rights offers guidance to help developers determine whether their data practices are subject to HIPAA. See https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf

2. Do the Application's data practices follow the CARIN Alliance Trust Framework and Code of Conduct[6]?

   ☐ Yes

   ☐ No

   ☐ Not sure (Complete Questions 4-11, below)

3. Has the Application been registered on the CARIN Alliance's MyHealthApplication.com?

   ☐ Yes (Skip to Question 12, below)

   ☐ No

4. Transparency –

   a. The Organization includes a publicly accessible link to the Application's Privacy Policy on its website and through the Application.

      ☐ Yes

      ☐ No

   b. The Privacy Policy covers collection, use, and disclosure of Personal Data.

      ☐ Yes

      ☐ No

   c. The Privacy Policy covers collection, use, and disclosure of De-identified Information.

      ☐ Yes

      ☐ No

   d. The Organization provides updates when Privacy Policies have changed, and provides individuals with the option to re-affirm consent or to withdraw consent.

      ☐ Yes

[6] https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/.

☐ No

e. The Privacy Policy is clear about what happens to Data when Consent is re-affirmed or withdrawn.

☐ Yes

☐ No

f. The Privacy Policy is clear about what happens to Data if the Application has a change in ownership or the Organization (or Application Developer, if different from the Organization) goes out of business.

☐ Yes

☐ No

5. Questions about Data Collection

a. The Privacy Policy is clear about the scope of information collected by the Application.

☐ Yes

☐ No

b. The Application only collects Personal Data through external data connections with users' consent.

☐ Yes

☐ No

c. The Application only collects Personal Data with users' consent.

☐ Yes

☐ No

d. After collecting Personal Data from an external source, the Application:

☐ Continues to collect new Personal Data as it becomes available until the user revokes consent.

☐ Requires consent each time before collecting additional Personal Data from that source.

6. Questions about Data Uses by the Application

   a. The Privacy Policy is clear about the scope of permitted Uses of Personal Data.

      ☐ Yes

      ☐ No

   b. The App Developer (if different from the Organization) and all other third-party service providers are contractually obligated to follow the Privacy Policy.

      ☐ Yes

      ☐ No

   c. The Organization prohibits Uses of Personal Data and De-identified Information except with Consent from the individual.

      ☐ Yes

      ☐ No

   d. The Organization collects a separate Consent before marketing third-party goods or services to an individual.

      ☐ Yes

      ☐ No

7. Questions about Disclosures of Data to Third Parties

   a. The Privacy Policy is clear about the scope of permitted Disclosures, when the Application will collect an informed, proactive Consent before sharing a user's Data with third parties and when Disclosures are permitted without an informed, proactive Consent (for example, as required by law or in connection with the business transfer).

      ☐ Yes

      ☐ No

b. The Privacy Policy requires the Application to collect a separate Consent if the purpose of Disclosure is to facilitate the marketing of goods or services to the individual.

☐ Yes

☐ No

8. Questions about Individual Rights

a. The Application supports the right of users to access their Data.

☐ Yes

☐ No

b. The Application supports the right of users to easily change their Consent options.

☐ Yes

☐ No

c. The Application supports the right of users to close their account and delete their Data and is clear about situations when data deletion may not be feasible.

☐ Yes

☐ No

d. The Application supports the right of users to send Personal Data to the destination of their choice.

☐ Yes

☐ No

9. Questions about Data Security

a. The Organization and App Developer (if different from the Organization) protects identifiable health information by implementing security safeguards including encryption of data in transit and at rest and internal accountability measures such as access controls and audit logs.

☐ Yes

☐ No

b. The Organization and App Developer (if different from the Organization) comply with applicable breach notification laws.

☐ Yes

☐ No

c. The Organization and App Developer (if different from the Organization) use provider portal credentials (compliant with SMART on FHIR standards) or a digital identity credential that meets NIST assurance level 2.

☐ Yes

☐ No

d. The Organization and App Developer (if different from the Organization) prohibit re-identification of De-Identified/Anonymized/Pseudonymized Data.

☐ Yes

☐ No

10. Question about Accountability

a. The Organization and App Developer (if different from the Organization) comply with all applicable federal and state laws.

☐ Yes

☐ No

b. The App Developer regularly trains its workforce on compliance with the data practices covered by the CARIN Code of Conduct.

☐ Yes

☐ No

11. Questions about Consumer Education[7]

    a. The Application includes educational resources to help users understand the Application's data practices, and steps they can take to protect their privacy and the confidentiality of their Personal Data.

    ☐ Yes

    ☐ No

12. Questions About Certifications

    a. In the last 12 months, the Application's data practices has been reviewed by an independent assessment organization for compliance with the Application's Privacy Policy and AICPA Privacy Principles, and is documented by a written SOC-2 certification report.

    ☐ Yes

    ☐ No

    b. In the last 12 months, the Application's data practices have been certified by an independent assessment organization for compliance with the HITRUST CSF.

    ☐ Yes

    ☐ No

    c. The developer will immediately suspend the Application's connections with the API endpoints if its data practices are not consistent with its applicable SOC-2 or HITRUST CSF certifications.

    ☐ Yes

    ☐ No

    ☐ Not applicable

13. Questions About Other FHIR-Based API Connections

[7] The CARIN UX Compliance Guide, accessible via https://carinuxguide.arcwebtech.com/, offers guidance for delivering education to consumers about safeguarding their health data and informing themselves about an application's privacy practices.

a. The Application has been approved by the U.S. Centers for Medicare and Medicaid Services for access to Personal Data through the CMS Blue Button 2.0 APIs.

☐ Yes

☐ No

b. The Application has been approved by U.S. Veterans Administration for access to Personal Data through the VHA's Lighthouse APIs.

☐ Yes

☐ No

c. The Application is currently registered to access Personal Data from other health care organizations, through open (non-proprietary) or proprietary FHIR-based APIs.

☐ Yes

☐ No

d. The Organization or App Developer has not been permanently banned from connecting with the FHIR-based APIs of any health care organization.

☐ Yes

☐ No

Appendix F - Process Diagram - Educational Information Workflow

Attached is an illustrative example of how member educational information could be provided.