Best Practice Recommendations for HL7® FHIR® Based Deployment

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers and caregivers. We are committed to providing consumers and their authorized caregivers access to health information. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via the open HL7® FHIR® APIs in production today and the ability to use that information with any third-party application they choose. The ability to access and store clinical information in the application of one's choice is critical for many patients especially those who see many different providers, move frequently, or need to readily share their data.

In order for the CARIN Alliance's vision to become a reality, these consumer-facing applications need to be able to connect to as many providers and payers as possible across the country. This means the apps need to be able to easily discover and connect to all required HL7® FHIR® endpoints in production. For nearly eight years, the CARIN Alliance community members have been connecting to these APIs, and sharing experiences, tools, and resources with one another toward that collective vision. In 2021, the CARIN Alliance launched the HL7® FHIR® directory framework initiative, which was the first, fully crowdsourced payer HL7® FHIR® endpoint directory for stakeholders to use based on industry best practices. That same year, the CARIN Alliance released an Application Registration Best Practices guide for application developers looking to connect to these APIs.

The CARIN Alliance has also been collecting feedback and collaborating with members to develop a set of best practices for payers and electronic health record (EHRs) vendors on how to implement HL7® FHIR® APIs in their environments. With the anticipated release of the final CMS Advancing Interoperability and Improving Prior Authorization Processes Rule (CMS-0057) which will require HL7® FHIR® APIs to be implemented between providers and payers, we want to share the lessons we have learned with stakeholders regarding how to improve their current HL7® FHIR® infrastructure to make it easier for data holders to connect to each other.

The following represents the CARIN community's recommendations for how to improve the current HL7® FHIR® ecosystem to prepare the industry for implementing HL7® FHIR® at scale. We believe that if payers and providers adopt these recommendations, it will not only lead to a better exchange of data with each other, but will also lead to patient's having more access to their health data via an application of their choice.

CALL TO ACTION: We would request relevant actors under the health interoperability rules (*e.g.*, payers, health systems, EHRs, interoperability vendors) to examine these best practices and implement them as appropriate to improve the overall interoperability ecosystem. For the same reason, we would urge the Department of Health and Human Services to address the relevant obstacles in FAQs or policy making, not just for patient access APIs, but for the ever-

widening range of regulated APIs, including provider directory APIs, APIs for population services, payer-to-payer APIs, payer-to-provider APIs, and prior authorization APIs.

The following best practice recommendations are grouped by content area. If you have additional recommendations you would like to include, please let us know https://www.carinalliance.com/about-us/contact-us/.

I. Improving the Knowledge Base

1. Provide adequate resources to support delivery of Patient Access API capabilities and consistent application of actors' compliance obligations.
2. Publish a standard, publicly available site with clear and up-to-date information on third-party Patient Access application integration capabilities.
    a. Include documentation in a standardized format, such as FHIR API capability statements.
    b. Include up-to-date results of conformance testing from the Inferno test bed.
    c. Publish the site on Lantern and other open-source API directories.
3. Provide a comprehensive Developer Portal, such that application developers can self-start, being sure to include information about registration, standard operating procedures, error handling, token expiration, etc.
4. Publicly document detailed information for all available API endpoints using a standard format (*e.g.*, Patient Access Brands).
    a. Payers – list endpoints by plan (where applicable)
    b. EHR vendors – publicly available list of endpoints with for each individual provider or provider group; including more comprehensive provider to provider group affiliation in provider directory resources.
    c. Plans and Providers – should include identifying information such as logos, addresses, etc.
5. Publicly document standard code set mapping guide for included FHIR resources (*e.g.*, RxNorm, LOINC, SNOMED, etc).
6. Ensure Patient Access integration knowledge is adequately disseminated, distributed and documented within your organization, to support resilience if/when members of the API implementing team change roles or leave the organization, and to provide adequate support for third-party application developers throughout the registration, onboarding, and production lifecycle of a Patient Access integration.

II. Improving Application Registration

1. Wherever possible, application registration with payer and EHR vendor systems should support self-service registration for app developers.
2. Provide transparency about expected turnaround times and monitoring at each step of the registration, onboarding, and live production lifecycle. Make sure inboxes are assigned.

3. Provide easily understandable (*i.e.*, written in lay language) Terms & Conditions that conform with regulations.
4. Use standard and reasonable information requests/questionnaires that enable third-party app developers to attest to their relevant information security and privacy practices along with any additional PHI access and risk management practices as a part of the application registration process, consistent with applicable regulations.
5. Make contact information available to third party app developers for decisionmakers involved with revising and approving client ID requests.
6. Provide timely and relevant developer support during the integration and testing phases. Provide support staff that are easily reachable during the onboarding and registration process.
7. Actors should participate in conformance testing to ensure compliance with published specifications and should make these results public.

III. Improving Sandbox Testing

1. Provide no-cost lower environment/sandbox testing platform for all vendors.
2. Authorize access for testing platforms to all vendors; do not require a patient or member to first request access to their records through a particular app.
3. Do not terminate sandbox connections they should remain active over low volume for any app.
4. Provide testing platforms that mirror the production environment.
5. Provide test patient or member users with credentials and representative test data.
6. Include test data in the Production environment.
7. Make sure the test data covers all the resources available through the endpoint.
8. If consumer facing education is being provided, make it accessible to the app developer in lower-level environments.

IV. Improving Production Configuration & Release Management

1. Provide developers self-service capability to generate or obtain both a client secret and client ID if applicable.
2. Provide developers a pre-production final connection testing harness (*e.g.*, ping test).

Improving the Technical Infrastructure

1. Provide configurable API rate limiting capabilities, allowing applications to receive warmings about thresholds prior to inducing performance issues.
2. Provide certificate expiration alerts.
3. Document and use standardized definitions and practices for error codes.
4. Use a standard OAuth workflow consistent with the current regulations.
5. Provide a transparent user token expiration period consistent with regulations.
6. Provide tooling or a test patient to determine if the endpoint is active.

7. Do not require non-standard identifiers in transactions that require custom development by third party developers accessing the endpoint.
8. Do not require out of band consumer opt-in requirements.
9. Make sure the data available at endpoints is timely, consistent with applicable regulations.

V. Improving Integration and Onboarding

1. Provide a dedicated, responsive, and expert Onboarding team (Project & Technical) whose roles and responsibilities are clearly defined.
2. Provide a standard onboarding process and plan from integration request through Go Live.
3. Assign a business owner within the entity who will have accountability for a successful patient access integration.

VI. Improving Ongoing Support & Maintenance

1. Provide a contact information that will enable third-party application developers to connect with the Support point of contact to troubleshoot issues.
2. Provide responsive and expert Support team with clearly defined roles and responsibilities.
3. Document and use a standard issue management process and reasonable SLAs for resolution.
4. Provide designated developer contacts with clear, automated reminders about any ongoing connection requirements (*e.g.*, version control), security/privacy or third-party risk management processes that have an annual (or other frequency) renewal or update.
5. Provide release notes that can be subscribed to via email.