Best Practices for Payers and App Developers

The Centers for Medicare and Medicaid Services (CMS) released the Interoperability and Patient Access final rule on May 1, 2020. This final rule requires most CMS-regulated payers – specifically, Medicare Advantage (MA) organizations, Medicaid Fee-For-Service (FFS) programs, CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs), excluding issuers offering only Stand-alone dental plans (SADPs) and QHP issuers offering coverage in the Federally-facilitated Small Business Health Options Program (FF-SHOP) - to implement and maintain a secure, standards-based **Patient Access Application Programming Interface (API)** (using Health Level 7® (HL7) Fast Healthcare Interoperability Resources® (FHIR) Release 4.0.1) that allows patients to easily access their claims and encounter information, including cost (specifically provider remittances and enrollee cost-sharing), as well as a defined sub-set of their clinical information through third-party applications of their choice.

This rule also requires MA organizations, Medicaid FFS programs, CHIP FFS programs, Medicaid managed care plans, and CHIP managed care entities to make provider directory information publicly available via a FHIR-based **Provider Directory API** accessible through a public-facing digital endpoint on the payer's website.

In this document you can find links to useful information and best practices to help you build and maintain a FHIR-based API, as well as best practices for payers and third-party app developers.

HL7 FHIR – Getting Started:

- Welcome to FHIR: https://www.hl7.org/fhir/
- FHIR Starter: https://wiki.hl7.org/FHIR_Starter
- Training on FHIR: https://wiki.hl7.org/FHIR_Teaching
- Resources for FHIR Implementers: https://confluence.hl7.org/display/FHIR/Implementers
- FHIR Tools Registry: https://confluence.hl7.org/display/FHIR/FHIR+Tools+Registry

Privacy and Security Tools:

- Privacy, Security, and HIPAA: https://www.healthit.gov/topic/privacy-security-and-hipaa
- Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- OAuth 2.0:
    - https://oauth.net/2/
    - http://hl7.org/fhir/smart-app-launch/
- OpenID Connect:
    - https://openid.net/what-is-openid/
    - http://openid.net/specs/openid-connect-core-1_0.html

API Testing Tools:

- Inferno: https://inferno.healthit.gov/

Implementation Guidance for the Patient Access API and Provider Directory API:
https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

Best Practice for Payers: Multi-person Enrollment Groups

The CMS Interoperability and Patient Access final rule applies to Qualified Health Plan (QHP) issuers on the individual market Federally-facilitated Exchanges. We recommend that issuers explore ways to minimize the risk of the claims information of other members of an enrollment group from being unexpectedly shared with a third-party app when one member of an enrollment group requests that the payer share his or her claims information with an app. This could include storing and making accessible claims information for each non-minor member of an enrollment group separately.

Developing Third-Party Apps

The CMS Interoperability and Patient Access final rule provides app developers with an opportunity to find innovative ways to help patients access their health information and provider directory information. With this unprecedented opportunity comes an important responsibility. Here we provide information to help app developers give patients access to their health information in a way that protects their privacy and keeps their data secure.

Start by reviewing the standards payers will use to make these data available via APIs:
https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

Privacy and Security:

As a first step, it is important to know what laws may impact an app. A great place to start is the Federal Trade Commission's (FTC's) Mobile Health Apps Interactive Tool. Generally, once health information has been transmitted to a third-party app, it is no longer protected by the Health Insurance Portability and Accountability Act (HIPAA). To better understand an app's relationship to HIPAA, see the Office for Civil Rights' (OCR's) HIPAA Q's Portal for Health App Developers.

Third-party apps are subject to the FTC Act. Additional FTC resources developers may find helpful include:

- Start with Security: A Guide for Business
- Mobile Health App Developers: FTC Best Practices

In addition to these federal laws, state laws may also apply.

Beyond an app developer's legal obligations, we strongly recommend app developers follow industry best practices to protect patient privacy and secure their health information.

Privacy Notice

Protecting patient privacy requires a strong privacy policy and an accessible, easy-to-read, comprehensive privacy notice. We strongly recommend that all third-party app developers clearly explain to patients that their data are no longer covered by HIPAA once the patient directs their data to be exchanged with most apps. Payers required to provide patients their data via the Patient Access API may also ask third-party developers to attest to having certain privacy provisions in place should a patient wish to use the developer's app. For instance, they may ask if the app has a publicly available privacy policy, written in plain language, that has been affirmatively shared with the patient prior to the patient authorizing app access to their health information. When we say "affirmatively shared," we mean that the patient had to take an action to indicate they viewed the privacy policy, such as click or check a box or boxes. Payers can ask if the privacy policy includes important information, such as, at a minimum:

- How a patient's health information may be accessed, exchanged, or used by any person or other entity, including whether the patient's health information may be shared or sold at any time (including in the future);
- A requirement for express consent from a patient before the patient's health information is accessed, exchanged, or used, including receiving express consent before a patient's health information is shared or sold (other than disclosures required by law or disclosures necessary in connection with the sale of the application or a similar transaction);
- If the app will access any other information from a patient's device; or
- How a patient can discontinue app access to their data, and what the app's policy and process is for disposing of a patient's data once the patient has withdrawn consent.

We strongly urge developers to follow industry best practices when developing a privacy policy and consult relevant resources, such as:

- CARIN Alliance Code of Conduct: https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/
- ONC Model Privacy Notice: https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn

For more information visit https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index