Florida Blue
Your local Blue Cross Blue Shield

May 2021

CMS Rule Provides Consumers Access to Protected Health Information Using Mobile Applications

A new Centers for Medicare & Medicaid Services (CMS) mandate puts consumers at the center of their health care by requiring CMS-regulated payers to implement and maintain a secure application programming interface (API)* for consumers to access their health information through third-party applications (apps).

The CMS Interoperability and Patient Access final rule impacts Medicare Advantage organizations and Qualified Health Plan issuers on the Federally Facilitated Exchanges. This includes Florida Blue Medicare Advantage and the health plans we offer through the Health Insurance Exchange℠ (Marketplace).

This requirement implements key provisions of the 21st Century Cures Act and Executive Order 13813 by improving the quality and accessibility of information consumers need to make informed health care decisions while minimizing reporting burdens on health care providers and payers. There are three required APIs:

1. **Provider Directory API:** Payers must enable an open API for third-party developers to access provider directory information. This API does not require member credentials.
2. **Patient Access API**: Payers must enable an open API for third-party developers to access members' clinical data, claims and payment information as well as pharmacy information.
3. **Payer-to-Payer API:** Requires CMS-regulated payers, at the member's request, to exchange specified data. Payers must implement a process for this data exchange across payers that will allow consumers to take their information with them when they move between health plans to different payers' systems. Payers must enable an open API for other payers to access member's clinical data upon request. (This API requirement is not effective until Jan. 1, 2022.)

Please note: While the mandate became effective Jan. 1, 2021, there is a six-month non-enforcement period. Our Provider Directory API will be accessible May 3 to our Medicare Advantage members and those with an individual under 65 Marketplace plan. The Patient Access API will be accessible after June 19 to the same members. We may expand the Patient Access API to additional members in the future.

On the following page are descriptions of each type of required API.

104179 0321

Provider Directory API	Patient Access API	Payer-to-Payer API

• Consumers access the data via the app of their choice
• API provides access to:
  ○ Provider data including name, address, phone number, specialty and network participation
• Pharmacy data including name, address, phone number, number of pharmacies in network and pharmacy type (i.e. retail)
	• Patient-directed exchange
	• Consumers access the data via the app(s) of their choice
	• API has ability to provide covered members access to:
	  ○ Their claims, payment and clinical data using a standard format: Fast Healthcare Interoperability Resources® (FHIR)
	  ○ Formulary information, including eligible drug lists, copay tiering and utilization management requirements
		• Requires CMS-regulated payers, at a patient's request, to exchange specified data, including the USCDI v1 data set and coverage decisions
		• Payers must implement a process for this data exchange across payers that will allow patients to take their information with them when patients move between health plans to different payers' systems

When your patient requests a copy of their personal health information (PHI) through the specific app they have chosen to download, we will electronically provide all their claims, encounter and clinical information back to Jan. 1, 2016 through that app. The health information we provide is limited to what we or our vendors maintain on behalf of our members.

We are required by CMS to provide the patient's information, but we are unable to specify how these apps will use this information. This PHI may include sensitive medical information. We cannot withhold this information when responding to a PHI access request through an app, even at the member's request.

Educating our Members

We are letting our members know about this new mandate and encouraging them to research the different apps available. Members should carefully consider and review the privacy and security settings and policies of the app developer before requesting their PHI through the app. They should look for an easy-to-read privacy policy that clearly explains how the app will use their PHI. If an app does not have a privacy policy, members are encouraged to reconsider using the app.

Members are responsible for ensuring their desired app is appropriately registered with Florida Blue before they make a request to access their PHI using that app. We will have a list of registered apps available on our website after May 3. This list will be updated weekly.

Frequently Asked Questions

What do I need to do?

There is nothing you need to do but be aware. Once the APIs are accessible – provider directory API in May and patient access API in June -- you may receive questions from your patients regarding their clinical and claims information as well as information included in the provider directory transmitted via the app.

What do I do if the information my patient has in the app is incorrect?

Because the information is collected from a variety of sources, your patient will need to contact the app's customer service area for assistance.

Can my patient choose which information they want transmitted through the app?

At this time, we cannot withhold information when responding to a PHI access request through an app, even at the member's request. This PHI may include sensitive medical information, such as treatment or diagnosis information pertaining to mental health, substance use disorders, sexually transmitted diseases and other sensitive information. If a member wants to limit the amount or type of PHI Florida Blue transmits through an app, they should reconsider using any app to obtain their PHI in this manner.

Who oversees these apps and their content?

Most third-party apps are not created by -- or affiliated with -- covered entities, therefore app developers are likely not subject to the HIPAA privacy and security protections. These apps may be regulated by the Federal Trade Commission (FTC) and the protections provided by the FTC Act. The FTC Act, among other things, protects against deceptive acts (e.g., if an app shares personal data without permission, despite having a privacy policy that says it will not do so). The FTC also enforces the promises that are made in an app's privacy policies, which is why it is important for members to review an app's privacy policies before using it to request PHI from Florida Blue.

Here is FTC information about mobile app privacy and security for consumers.

As always, members can request a copy of their PHI in accordance with the Florida Blue Notice of Privacy Practices. A copy of Florida Blue's Notice of Privacy Practices can be found here.

The data included in third-party apps may not be reliable. Providers should use caution in relying on such information when making diagnostic and treatment decisions.

*An application programming interface is a software intermediary "messenger" that makes it possible for application programs to interact with each other and share data. It is a standard industry practice to share data so app developers don't have to "reinvent the wheel." Anytime a consumer uses a health care portal to communicate with their provider or request their records from their provider electronically, they are using an API. Other common examples include:

- Visiting a travel site to book a hotel. The API collects data from hotels in the area you selected.
- Purchasing an item online and getting an estimate of the shipping costs. The API collects the shipping rates for select carriers and provides options based on the purchase.