ASES
ADMINISTRACIÓN DE SEGUROS DE SALUD DE PUERTO RICO

Vital
Salud en tus manos
GOBIERNO DE PUERTO RICO

Interoperability Rule
2023- Vital

MMM
multihealth

What is the Interoperability Rule Set by the Centers for Medicare and Medicaid Services? (CMS)

It is a CMS mandate that provides for expanding patients' electronic access to their protected health information. All Medicaid and Medicare Advantage plans shall comply with this mandate

What's the purpose of the rule?

It is intended to facilitate the patient increased access to their personal health information (PHI), in order to help them be the center of their own health care decisions, thus minimizing the risk of duplicating tests and other inefficiencies.

This access to health information exchange (interoperability) helps to guarantee that providers are allowed to see an individual's medical history in order to make informed clinical decisions, which can lead to a better coordinated care.

What does this rule imply?

Our Beneficiary may download and register in an external application of their choice, and may direct such app to download and access the health information we have available

Before Proceeding, You Must Know!

MMM recommends to reconsider the use of apps that have not confirmed having basic privacy and security protection features, to take care of the confidentiality of your protected health information. If you are planning to use any external app to access your health information, make sure it is a safe application.

In an external application, and with your consent, your health information can be seen, exchanged or used by any person or entity, and can even be shared or sold at the extent that is permitted by Law. Your consent is required before accessing, exchanging or using and sharing your protected health information.

If you choose an external app for the management of your protected health information, it is important to make sure you can revoke or interrupt the access to your information through such app and determine how will the app delete your information after you revoke your consent.

The app should be able to protect your health information against risks such as loss or unauthorized access, use, change, destruction, disposal, or disclosure.

If You Are Considering to Choose a Third-party (External) Application or Website:

Remember that third-party apps or websites **are not** subject to HIPAA or other privacy laws, which generally protect personal health information. The app must have its own privacy policy, which should provide self-imposed limitations on how the app or website will use, keep, disclose and (probably) sell information about you.

We recommend to follow these tips when deciding which app to choose to be able to see your protected health information (PHI):

- **Use official app stores.** To minimize the risk of installing potentially harmful apps, only download apps from official app stores, such as your device manufacturer, or the app store of your operational system. In addition, you should make some research about the developer before installing an application.
- **You should know which information you will be able to access with the app.** Before downloading an app, read the app's privacy policy to see how will your data be used, or to see if your data will be shared. Is the policy unaccurate on how the app will share your data? If so, or if you are not comfortable with the way your information will be shared, you may find another app.
- **Take a look at permits**. To access information such as your location or contacts, or to access functionalities such as camera or mic, apps need your consent. Probably, you will be asked to give permission when you download the app for the first time, or when the app tries to access that information or function for the first time. Pay a lot of attention to permits requested by the app. For example: does it really need to access your location or pictures to do its job?

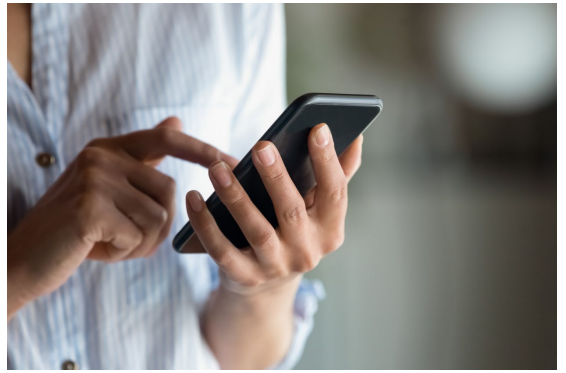
If You Are Considering to Choose a Third-party (External) Application or Website:

- **Public privacy policy**. That the App has a publicly available privacy policy that has been affirmatively shared with you prior your consent to access your protected health information through the App.

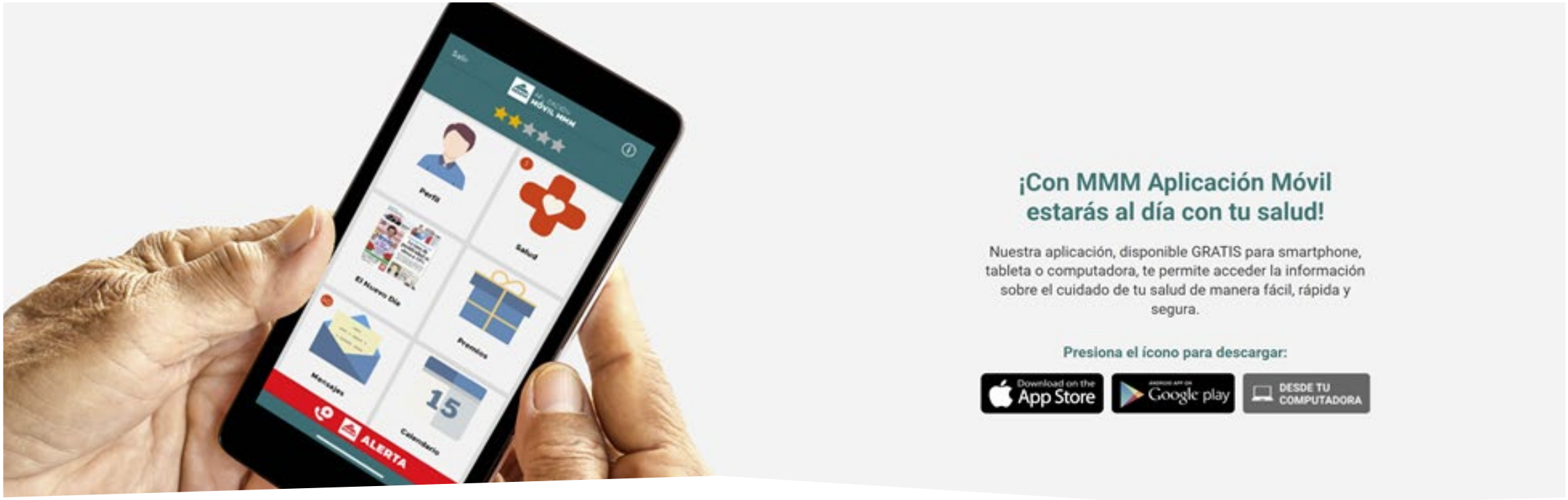
- **Minimum provisions in privacy policy**. That the App's privacy policy includes, at a minimum, the following provisions:
  - How your health information may be accessed, exchanged, or used by any person or entity, including whether your health information may be shared or sold as permitted by law;
  - The requirement for express consent from you before your protected health information is accessed, exchanged, or used and shared;
  - If the App will access any other information from your device and;
  - How you can revoke or discontinue the App's access to your protected health information and how the App will dispose/delete your information once you have withdrawn your consent.

- **Minimum safeguards.** That the app has safeguards to protect your protected health information against risks such as loss or unauthorized access, use, alteration, destruction or disposition, or disclosure.

What You Need to Know About a Third-party App or Website



- ¿Which health data does the app gather?
- Will the app gather non-health data from my device, such as location?
- Will my data be stored in a confidential or anonymous manner?
- How will the app use my data?
- Will the app disclose my data to third parties?
- Will the app sell my data on any reason, such as advertising or research?
- Will the app share my data on any reason? If so, with whom? What for?
- How can I limit the way the app will use and disclose my data?
- Which security measures does the app use to protect my data?
- How may others, such as my relatives, be affected when I share my data in an app?
- How may I access my profile and make corrections on the data retrieved by the app?
- Does the app have a process to gather and respond to users complaints?
- In case I do not want to use the app anymore, or if I do not want the app to keep having access to my health information, how may I end the app's access to my data?
- What's the app's policy to delete my data when access is ended? Should I do something else than just deleting the app from my device?
- How will the app inform the users of any changes in its privacy policy?



IMPORTANT: The third-party app or website you choose will have access to all your personal health information. This includes confidential health information about treatments, utilization, or sensitive information related to substance use disorder, mental health treatment, HIV status, and more.

For this reason, we recommend that you choose the option offered by your plan, which is free and safe, to have access to your health information! That's the MMM Mobile App.

IMPORTANT NOTE:

How to Report Identity Theft and Fraud

- If you believe an application that you've shared your data with is misusing that information in violation of their stated privacy policy, contact the Federal Trade Commission to investigate or call 1-877-382-4357. If you believe the privacy of your health care data has been violated, contact the federal Department of Health and Human Services Office of Civil Rights.