Interoperability and Patient Access Final Rule

1. What is the Interoperability and Patient Access Final Rule and how does it work?

The law known as the "Interoperability and Patient Access Final Rule" was designed to allow people with Medicaid, Medicare Advantage, CHIP, and Federal Exchange health plans to easily access certain types of health information through mobile device applications ("apps"). This information includes the following:

- Claims and payment information for medical, dental, and pharmacy, including payments made both by you and by others on your behalf
- Certain types of health information submitted to IMCare (or other health plans) by health care providers
- Searchable provider information, including name, location, specialty, etc.
- A link to searchable pharmacy listings
- A link to prescription and over-the-counter drug information and pricing

The apps you use to access this information are **not** provided by IMCare. They are independent, third-party apps, and IMCare has no control over them. You choose the app you want to use and authorize sharing of your information. Then you can use that app to view your past 5 years of accessible information.

2. What information should be available in these apps?

When you access your chosen app, you will be able to see the claim information listed above that has been provided to IMCare. You may also be able to see other health information that providers have submitted to us. If you had another qualifying health plan within the last 5 years, you should also be able to see the information that health plan has submitted to the app.

3. What should I do if information is missing or wrong?

Some information may not show up in the apps. There are several reasons this might happen:

- Providers did not submit health information to IMCare.
- Providers did not submit claims to IMCare. Providers have up to 6 months to submit claims, so there might be a delay in getting the information.
- IMCare has received a claim, but it has not yet gone through our payment process.
- Claims were not submitted to a previous health plan.
- The app you are using has not collected information from a previous health plan.

If you feel that either health or claims/payment information in your record is wrong or missing, please contact your health care provider. IMCare is only able to share information that has been shared with us by providers.

4. Why would I want to download and share my health or claims/payment information?

Using these apps to access and download your information allows you to do the following:

- Review, track, and get control over your health and claims/payment information
- Easily share your health information with providers, caregivers, or anyone you choose
- Get help managing and improving your health

5. How do I protect my information?

Since you control access to your health information, it is your responsibility to take steps to keep it safe. Treat your health and claims/payment information the same way you would treat your banking or other confidential information. IMCare has no control over how these apps may use your information. Here are some important things to remember:

- Keep your login information private and secure.
- Choose a third-party app that follows the CARIN Code of Conduct. The CARIN Code of Conduct is a set of industry-leading best practices that the companies offering these apps have voluntarily adopted to protect and secure your health information. Visit **https://myhealthapplication.com** to see a list of apps that follow these best practices.
- Be sure you **read and understand the app's privacy and security policy before allowing the app to access your health data**. The apps may have different policies. Some may share your information with other entities, so be sure to check for that in their policies.

6. How do I access my information through the mobile app?

If you decide that you want to access your data through a mobile app, you will first need to be registered. Contact IMCare member services by calling 218-327-6188, toll free 1-800-843-9536, TDD 1-800-627-3529, or by emailing imcare.office@co.itasca.mn.us for help in registering.

7. What should I look for in a privacy and security policy statement?

Note: If the app's privacy policy does not clearly address the following questions, you should think about using a different app. Health information is very sensitive information. You should be careful to choose apps with strong privacy and security standards to protect it.

- Does the app have an easy-to-read privacy policy that clearly explains how the app will use my data?
  - If the answer to this question is no and the mobile app does **not** have a privacy policy, the app should **not** be trusted.
- What health data will this app collect?

- Will this app collect non-health data from my device, such as my location?
- How will this app use my data?
- Will my data be stored in a de-identified or anonymized form?
- 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 let users know of changes that could affect its privacy practices?

8. What are my privacy rights under the Health Insurance Portability and Accountability Act (HIPAA) and who must follow HIPAA?

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule. You can find more information about the following:

- **Patient rights under HIPAA and who must follow HIPAA**: **https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html**
- **HIPAA FAQs for Individuals**: **https://www.hhs.gov/hipaa/for-individuals/faq/index.html**

9. Are these third-party apps covered by HIPAA?

Most third-party apps will not be covered by HIPAA. Most third-party apps will instead fall under the jurisdiction of the Federal Trade Commission (FTC) and the protections provided by the FTC Act. The FTC Act, among other things, protects against deceptive acts (for example, if an app shares personal data without permission, despite having a privacy policy that says it will not do so).

The FTC provides information about mobile app privacy and security for consumers here: **https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps**

10. What should I do if I think my data has been breached or an app has used my data inappropriately?

If you feel that your data was shared without your permission or used in a way that you did not agree to, you can do any of the following:

- Contact the Office for Civil Rights (OCR) to file a complaint.
- Contact the Federal Trade Commission (FTC) to file a complaint.

If you are concerned that your privacy rights have been violated, you may file a complaint with IMCare. Contact the following:

HIPAA Privacy Officer
1209 SE 2nd Ave
Grand Rapids, MN 55744

Telephone: **1-800-843-9536**
TTY: **1-800-627-3529** or **711**
These calls are free.