Interoperability FAQs – Resources Regarding Privacy and Security

What are important things members should consider before authorizing a third-party app to retrieve their health care data?

It is important for members to take an active role in protecting their health information. Helping you know what to look for when choosing an app can help you make more informed decisions. You should look for an easy-to-read privacy policy that clearly explains how the app will use your data. If an app does not have a privacy policy, you should not use the app.

You should consider:

- What health data will this app collect? Will this app collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
- How will this app use my data?
- 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 inform users of changes that could affect its privacy practices? If the app's privacy policy does not clearly answer these questions, you should reconsider using the app to access their health information. Health information is very sensitive information, and you should be careful to choose apps with strong privacy and security standards to protect it.

Prior to connecting to the IO Station, third party apps are asked to attest to certain privacy policies. If the third party app attests negatively or doesn't respond to the request, a warning will display when you log in for each app that you use. After reviewing the warning, you can decide to change your mind about sharing data to the third app. If you choose to move forward after reviewing the warning, your data will be shared with the third party app.

It is very important to review and understand the privacy and security practices of the app before you use it.

What should a member consider if they are part of an enrollment group?

Some members, particularly members who are covered by Qualified Health Plans (QHPs) on the Federally-facilitated Exchanges (FFEs), may be part of an enrollment group where they share the same health plan as multiple members of their tax household. There may be times when the primary policy

holder (subscriber) and other members, can access information for all members of an enrollment group unless a specific request is made to restrict access to member data. You will only be able to access your own data through the app. If you would like to access data for family members, you must obtain authorization from your family member in order to access their information. Contact Customer Service at 888-327-0671 and ask for the for the appropriate forms. Note, if you are the parent of a minor (age 14 or under), you may be able to access the minor's information through the app. Contact Customer Service for more information. Note that if you share a tax household but you do not want to share an enrollment group, you have the option of enrolling individual household members into separate enrollment groups, even while applying for Exchange coverage and financial assistance on the same application; however, this may result in higher premiums for your household and some members, (i.e. dependent minors, may not be able to enroll in all QHPs in a service area if enrolling in their own enrollment group) and in higher total out-of-pocket expenses if each member has to meet a separate annual limitation on cost sharing (i.e., Maximum Out-of-Pocket (MOOP)).

What are a member's 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 patient rights under HIPAA and who is obligated to follow HIPAA here: https://www.hhs.gov/hipaa/for-individuals/index.html

You can also find more information in the HIPAA FAQs for Individuals found here: https://www.hhs.gov/hipaa/for-individuals/faq/index.html

Are 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 (e.g., 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

What should a member do if they think their data have been breached or an app has used their data inappropriately?

You can file a complaint with the McLaren Privacy Office. Complaints can be sent by mail or email.

You can send it by email to MHPCompliance@mclaren.org

Or you can mail it to the following:

ATTN: Privacy Officer
McLaren Health Plan
P.O. Box 1511 Flint, MI 48501-1511

In addition, you can submit a complaint to OCR or FTC, as appropriate.

To learn more about filing a complaint with OCR under HIPAA, visit:
https://www.hhs.gov/hipaa/filing-a-complaint/index.html

Individuals can file a complaint with OCR using the OCR complaint portal:
https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

Individuals can file a complaint with the FTC using the FTC complaint assistant:
https://reportfraud.ftc.gov/#/