MetroPlusHealth

Third-Party Applications

MetroPlusHealth is providing a secure electronic method via a patient access application programming interface (API) to members under the Interoperability Rule. This method will allow easy access to claims and encounter information including cost, as well as a defined sub-set of your clinical information. The API establishes an online connection between MetroPlusHealth, and any application authorized by you, our member. ensures that your information containing PHI is not only accessible but protected and secure under the Health Insurance Portability and Accountability Act (HIPAA) when it is transmitted to the application of your choice. However, once this information is transmitted, it may not receive the same level of protection covered entities, like MetroPlusHealth, are required to maintain.

It is important for members, like yourself, to take an active role in protecting their health information. To help assist in the selection of an application of your choice, we have created this guide to provide you with some helpful tips and address potential questions.

- **What is Protected Health Information (PHI)?**

  Protected Health Information is information about an individual that reveals something related to their health or allows the individual to be identified. PHI includes any identifiable information, including the member's name, address, date of birth, social security number, claims information, ID numbers and other information that is particular to an individual.

- **What is the Health Insurance Portability and Accountability Act (HIPAA) and how does it affect the privacy and security of my information?**

  The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires **covered entities** to:

  - Protect and secure the privacy of our member’s information (PHI), whether that information exists in a paper or electronic format.
  - Not disclose more than is necessary when providing or releasing information.
  - Allow members to access their information, provide information on how we use their information and how we disclose their information.

- **What are my rights under 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 your rights under HIPAA here: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-forconsumers/index.html

  HHS OCR also addresses HIPAA related FAQs here: https://www.hhs.gov/hipaa/for-individuals/faq/index.html

  We also provide this information annually to our members in our Privacy Notice. This document can be located here: https://www.metroplus.org/about-us/privacy-policies

- **What companies must follow the HIPAA rule?**

Covered Entities are organizations that must follow HIPAA. Examples of covered entities include health plans, health care clearinghouses, or health care providers. These organizations transmit member information in electronic form in connection with a HIPAA related transaction.

- **What companies do not need to follow the HIPAA rule?**

  Non-Covered Entities are organizations that **do not need to follow** HIPAA **but** have your information. Some examples of these include:
  - Life insurers
  - Employers
  - Worker's compensation carriers
  - Most schools and school districts
  - Many state agencies like child protective service agencies
  - Most law enforcement agencies
  - Many municipal office
  - Third-Party Applications

- **Is MetroPlusHealth a covered entity?**

  MetroPlusHealth is a health plan, which means it is a covered entity and must follow HIPAA. As a covered entity, the following rules must be in place to ensure your information is private and secure:
  - Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
  - Covered entities must have procedures in place to limit who can view and access your health information as well as implement training programs for employees about how to protect your health information.
  - Business associates of covered entities also must put in place safeguards to protect your health information and ensure they do not use or disclose your information improperly.

- **Are third-party applications covered by HIPAA?**

  Most third-party applications **will not** be covered by HIPAA. Most third-party applications 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 are important things I should consider before authorizing a third-party application to retrieve my health care data?**

  When using or downloading a third-party application, always look for the Privacy Policy (or Privacy and Security Policy) and Terms of Service to understand how the application works and how your information will be handled. The Privacy Policy should be easy to read and outline **at a minimum** how your data will be collected, used, shared, and protected. Terms of Service may outline how the site operates, what to expect, specific features including Authentication (registration and login), other third-party sites as well as Limitations of Liability.

<u>You should consider the following when selecting an application:</u>

- What health data will this application collect? Will this application 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 application use my data?
- Will this application disclose my data to third-parties?
    - Will this application sell my data for any reason, such as advertising or research?
    - Will this application share my data for any reason? If so, with whom? For what purpose?
- How can I limit this application's use and disclosure of my data?
- What security measures does this application use to protect my data?
- What impact could sharing my data with this application have on others, such as my family members?
- How can I access my data and correct inaccuracies in data retrieved by this application?
- Does this application have a process for collecting and responding to user complaints?
- If I no longer want to use this application, or if I no longer want this application to have access to my health information, how do I terminate the application's access to my data?
    - What is the application's policy for deleting my data once I terminate access? Do I have to do more than just delete the application from my device?
- How does this application inform users of changes that could affect its privacy practices?

- **What should I do if I believe my data has been breached or an application has used my data inappropriately?**

If you believe your data was breached or used inappropriately by an application, you may file a complaint to OCR or the FTC.

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://www.ftccomplaintassistant.gov/#crnt&panel1-1

- **Are there any other tips I should follow?**

Additional Cybersecurity Tips:

- Protect your data.
    - When prompted to enter data into a web portal, always look for two features first:
        1. Authentication. Create an account that will identify you, preferably using multi-factor for positive identification.

    2. Encryption. Always look at the web address to start with HTTPS://. This indicates the transmission of your data will be sent securely.

- Be suspicious of unsolicited contact.
    - phone calls, visits, or email messages from unknown individuals asking about you or any other internal information.
- If an unknown individual claims to be from a legitimate organization, always ask for identity directly with the company they claim to be representing.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).
- Pay attention to the Universal Resource Locator (URL) or Web Address of a website.
    - Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling, or a different domain found at the end of the URL (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.
    - Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
    - Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce unwanted or malicious traffic.
    - Understanding Anti-Virus Software: http://www.us-cert.gov/ncas/tips/ST04-005
    - Reducing Spam: http://www.us-cert.gov/ncas/tips/ST04-007