CMS INTEROPERABILITY AND PATIENT ACCESS FINAL RULE

MEMBER EDUCATION

According to the Centers for Medicare and Medicaid Services (CMS), the "*Patient Access Rule puts patients first by giving them access to their health information when they need it most, and in a way they can best use it.*" As a result of this Rule, Magellan is required to implement and maintain a secure Application Programming Interface (API) website that allows patients to easily access their claims and encounter information, including cost, as well as some types of clinical information through 3rd Party applications of selected by the patient. Magellan is also required to make provider directory information publicly available through a standard website. More information is available at https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet.

FAQs

1. **What is API?**
   - API means Application Programming Interface.

2. **What is a 3rd Party application?**
   - An application that was not created by Magellan.

3. **How will I get the 3rd Party application?**
   - You can choose from different applications available in our Member Access Portal.

4. **Can I get it on my smart phone?**
   - Yes.

5. **Do I need to do anything?**
   - You do not need to do anything different unless you want to give your consent for 3rd Party applications to get your health information from the Magellan API.

6. **Why do you need my consent/permission?**
   - The law allows patients to choose which 3rd Party application is best for collecting all or part of the patient's electronic health information (EHI).

7. **What is the consent/permission for?**
   - When you give Magellan your consent, it means that Magellan can disclose or release your electronic health information to another 3rd Party API that you selected.

8. Can I remove/revoke my consent?

- Yes. A member may login to the Member Access Portal and on the dashboard you may click on the revoke access button, to remove/revoke consent given to applications for accessing (EHI).

9. Are you tracking who I gave consent to?

- Yes. You may see which applications you have given consent to in the Member Access Portal.

10. Can my caregiver get access to my data using this?

- No, unless you give them your consent to act on your behalf as your authorized representative.

11. What type of information is available and shared if I give my consent?

- Claims and claims adjudication information, explanation of benefits, provider and practitioner related information, eligibility, and patient history.

12. Can I see the information?

- Yes, by using 3rd Party applications you have provided consent to.

13. Can I get a copy of all the information available through the API?

- Yes, by using 3rd Party applications you have provided consent to.

14. Can my doctor or I use the API site to ask for prior authorizations?

- No.

15. How do I access the provider directory?

- The 3rd Party applications will have access to the Provider Directory API. You will not need to provide consent for a 3rd Party application to access the Provider Directory API.

16. How is this provider directory different?

- The Provider Directory API has been created by Magellan to provide data for the 3rd Party applications to use.

17. Who should I contact if some of the information about my health information is not correct?

- Contact Magellan's Member Services at:
    i. Bucks County: 1-877-769-9784
    ii. Cambria County: 1-800-424-0485
    iii. Delaware County: 1-888-207-2911
    iv. Lehigh County: 1-866-238-2311
    v. Montgomery County: 1-877-769-9782
    vi. Northampton County: 1-866-238-2312

18. Who should I contact if I have general questions about this FAQ?

- Contact Magellan's Member Services at:
    i. Bucks County: 1-877-769-9784
    ii. Cambria County: 1-800-424-0485
    iii. Delaware County: 1-888-207-2911
    iv. Lehigh County: 1-866-238-2311
    v. Montgomery County: 1-877-769-9782
    vi. Northampton County: 1-866-238-2312

19. Who should I contact if I have questions about technical support?

- Contact Interoperability@magellanhealth.com

20. Did Magellan get any notice or attestation from all the 3rd Party applications listed on the Magellan API website?

- No, but Magellan requires all 3rd Party applications listed on the Magellan Portal to abide by CARIN code of conduct, set forth by CARIN alliance. It is in the Member's best interest to be fully aware of the risks associated with releasing data to these 3rd Party applications. Magellan strongly recommends each Member Consent document to be reviewed by the Member/authorized representative to grant consent to these 3rd Party applications.

21. What are important things I should know or consider before I give my permission to a 3rd Party application (App) to collect my health information?

According to the Centers for Medicare and Medicaid Services (CMS),[1] it is important for patients to take an active role in protecting their health information. Patients should look for an easy-to-read privacy policy that clearly explains how the App will use their data. If an App does not have a privacy policy, we recommend that you do not use the App. Patients 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, patients should reconsider using the App to access their health information. Health information is very sensitive information, and patients should be careful to choose Apps with strong privacy and security standards to protect it.

22. What are a patient'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/guidance-materials-for-consumers/index.html

Information about the HIPAA FAQs for individuals is available here: https://www.hhs.gov/hipaa/for-individuals/faq/index.html

---

[1] See Page 2 for the source of the information @ https://www.cms.gov/files/document/patient-privacy-and-security-resources.pdf

23. Are 3rd Party applications covered by HIPAA?

Most 3rd Party applications will not be covered by HIPAA. Most 3rd Party applications will instead fall under the jurisdiction or authority 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

24. **What should a patient do if they think their data have been breached or an App has used their data inappropriately?**

If you think your data may have been breached or an App has used your data inappropriately, please contact our internal privacy office at Compliance@MagellanHealth.com.

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