Interoperability in Healthcare

Member Information

The Centers for Medicare and Medicaid Services (CMS) released the Interoperability and Patient Access final rule on May 1, 2020. This final rule requires Access Dental Plan to implement and maintain a secure, standards-based Patient Access Application Programming Interface (API). APIs allow members to easily access their claims and healthcare information including cost, specifically provider remittances and member cost-sharing, as well as a defined sub-set of their clinical information through third-party applications of their choice.

Generally, once health information has been transmitted to a third-party app, it is no longer protected by the Health Insurance Portability and Accountability Act (HIPAA) or Access Dental Plan's Notice of Privacy Practices. With this in mind, it is important for members to take an active role in protecting privacy and security of their health information. When deciding which third-party application to use, members should review the third-party app's privacy policy and 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, members should reconsider using the app to access their health information. Health information is very sensitive information, and members should be careful to choose apps with strong privacy and security standards to protect it.

What is Health Insurance Portability and Accountability Act of 1996 (HIPAA)?

The Health Insurance Portability and Accountability Act of 1996, or HIPAA for short, is a law that helps protect people's health information. The law sets rules for healthcare providers, health plans, and healthcare clearinghouses to follow when it comes to protecting the privacy and security of individual’s health information.

HIPAA requires these organizations to keep individual’s health information private, meaning it should not be shared with anyone who doesn't need to see it. The law also requires these organizations to use proper security measures to keep the health information safe.

HIPAA applies to various types of health information, including medical, dental and vision records, test results, and insurance information.

Additionally, HIPAA gives individuals certain rights when it comes to their health information. For example, individuals have the right to see and get a copy of their own health information, as well as the right to request that any errors in their health records be corrected.

HIPAA is important because it helps ensure that people's health information remains confidential, which can help protect them from discrimination and other negative consequences. If you have any questions or concerns about your own health information, do not hesitate to reach out to your healthcare provider or health plan.

HIPAA Covered Entities:

HIPAA applies to organizations and agencies that meet the definition of a covered entity. If an entity does not meet the definition of a covered entity, it does not have to comply with the HIPAA Rules. A covered entity includes but is not limited to healthcare providers, health plans, and healthcare clearinghouses. Generally, non-healthcare organizations, like fitness centers, gyms, and employers, are not subject to HIPAA. However, if these organizations provide wellness programs that collect health information, they may be subject to HIPAA rules.

How to Protect Your Protected Health Information (PHI):

Here are some steps you can take to keep your information safe:

- Don't share your health information unless necessary. Only share your health information with trusted healthcare providers or applications that you know are legitimate.
- Use strong and unique passwords for any applications you use that contain your health information. Avoid using the same password across multiple applications.

- Keep your applications and operating system up to date with the latest updates and security patches.
- Research any application you're considering using for secondary uses of your data. Make sure it has a good reputation for privacy and security, and that it clearly states its privacy and security practices.
- Review the privacy policy of any application or provider you entrust with your health data. Make sure you understand what information they collect, how it's used, and who has access to it.
- Be cautious when using public Wi-Fi to access health applications, as this can put your information at risk. Consider using a virtual private network (VPN) to encrypt your internet traffic.

Remember, protecting your health information is important to ensure your privacy, safety, and peace of mind.

Office for Civil Rights (OCR):

The Office for Civil Rights (OCR) is responsible for enforcing HIPAA rules. To submit a complaint to the OCR, you can use the OCR's online portal: https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf. You may also file a complaint by emailing OCRMail@hhs.gov or calling the OCR at 1-800-368-1019, TDD: 1-800-537-7697.

Federal Trade Commission (FTC):

The Federal Trade Commission (FTC) enforces rules related to consumer privacy and data security. You may file a complaint with the FTC if you believe a business has violated your privacy rights or provided inaccurate information about data breaches. To file a complaint with the FTC, you can use their online complaint form here: https://reportfraud.ftc.gov/#/ or call their Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357).

How to Contact Us:

If you have any questions about this Notice or need further information about matters covered in this Notice, please call the toll-free number on the back of your member ID card.

API Details

Avesis has implemented these functions from the Health Level Seven International - Homepage | HL7 International standards.

Base URL and access key will be provided as part of the enrollment process. Please contact FHIR_AccessRequest@avesis.com to initiate the enrollment process.

Once enrolled, to access the Avesis APIs you will need Internet access and can use any software tool capable of calling and processing API responses such as a customer developed applications, SoapUI or Postman.

Avesis implemented the standard Microsoft FHIR implementation, full technical details for can be found in this link: azure-docs/articles/healthcare-apis/azure-api-for-fhir/fhir-app-registration.md at main · MicrosoftDocs/azure-docs · GitHub