Frequently Asked Questions (FAQS)
VIVA HEALTH and VIVA MEDICARE Members

Question: What is interoperability?

Interoperability connects the health information systems of hospitals, urgent cares, outpatient clinics, and other health care facilities with insurance companies to share member health records, like claims, health conditions, prescribed drugs, and provider details. The sharing of this information helps health systems and providers (doctors and other health care professionals) deliver care more efficiently and effectively.

Interoperability creates a safe, electronic path for health records to be shared between health care organizations and insurance companies. The Centers for Medicare and Medicaid Services (CMS) — the government agency that runs Medicare — encourages the exchange of health care records, while making sure all member data is shared securely and only with the member's permission. The CMS Interoperability and Patient Access final rule requires health insurance companies and the developers creating the secure sharing of records to have certain privacy policies in place that ensure members attest and consent to their records being shared. Members must be given a clear explanation of how their records will be shared, what is covered in the attestation, and how to opt-out of sharing their records if they change their mind in the future.

Read more about Interoperability and CMS Patient Access final rule here.

Question: How does it work?

Interoperability enables members to access to their health information on a mobile device or other electronic devices in a secure way for personal use. As a member, you are in control of your health information. You can authorize the release of your data to a specified application (an app on your phone) so that you can view your data. VIVA HEALTH members are encouraged to use the VIVA HEALTH Member app or VivaMembers.com portal to view any information related to past medical and prescription claims history. The VIVA HEALTH Mobile App is available for download in the Apple App Store or Google Play Store.

To comply with CMS's regulatory requirements, VIVA HEALTH worked with 1UpHealth to make standards-based APIs available that will improve the electronic exchange of health care data. 1upHealth provides app registration and the vetting process on behalf of our members.

For a list of approved applications, please visit the 1Up Health App Gallery here.

Question: What third party apps are currently available to view my health information?

You can find a list of approved applications in Third-Party Applications in the 1upHealth Help Center.

Question: What kind of data is available?

The following types of member information will be available to third party applications developers:

- Adjudicated Claims/EOBs
- Clinical Data
- Formulary
- Provider and Pharmacy Directory
- Roster/Enrollment

Question: Is my medical information safe?

The privacy and security of member health information is a top priority for members and their families, health care providers and professionals, and the government. You can review how your medical information may be used and disclosed, as well as steps to protect the privacy and security of your health information here.

Are third party app developers 'vetted' for credibility?

Third-party applications that want to access the 1Up Health solution must complete the 1Up privacy and security attestation process. All published apps will be reviewed on an annual basis.

Apps that present active security threats, misuse, or abuse our APIs will have their access revoked and be blocked from API access until a thorough review is completed. 1Up Health will perform continuous monitoring of our API endpoints, have dashboards summarizing usage, and do routine log reviews.

Click here for more info on the Third Party App Vetting Process.

Benefits and Risks of Sharing Data

There are many benefits to this new ability to access and share your data. Some apps allow you to combine your data from multiple health systems to create a complete record of your visits with different doctors and hospitals, and combine it with the data that you generate on your own from wearable devices, such as glucose meters, pedometers, or heart rate monitors. Some other common uses include prescription drug management, chronic disease management, nutrition tracking, and care coordination. Data sharing empowers you to have greater ownership of and visibility into your health data, and has the potential to improve both your health and the quality of care you receive from the health care system.

As with any interaction over the Internet, these benefits are not without some level of risk. Your health plan takes your privacy and the security of your health information as seriously as you do. That's why your data is never shared without your permission. It's also very important to read the privacy and security policies for any application before you choose to share your data with it, to make sure that you understand how it is protected and used by that application.

Third Party App Developers

Question: As a third party app developer, how do I connect my application to CMS required VIVA HEALTH member information?

VIVA HEALTH has partnered with 1Up Health to provide an interoperability solution for our members using the FHIR/HL7 standards. This approach is outlined in: http://www.hl7.org/fhir/smart-app-launch/

Application Registration

- Third-party applications that want to connect their apps to the 1upHealth FHIR Server to send and receive health data, should begin by registering as a 1Up Health Developer. Click here to create a new account in the 1upHealth Developer Console and complete a new application.

- 1Up Health will then verify the information provided. 1Up Health seeks to ensure that the application and the company behind the application is providing a quality and secure application and that the company can meet all contractual requirements. Once the application is approved, client id's and, if necessary, client secrets (for confidential applications) will be issued and appropriate access to public keys established to ensure the confidentiality of communications and the signatures of access requests (public applications).