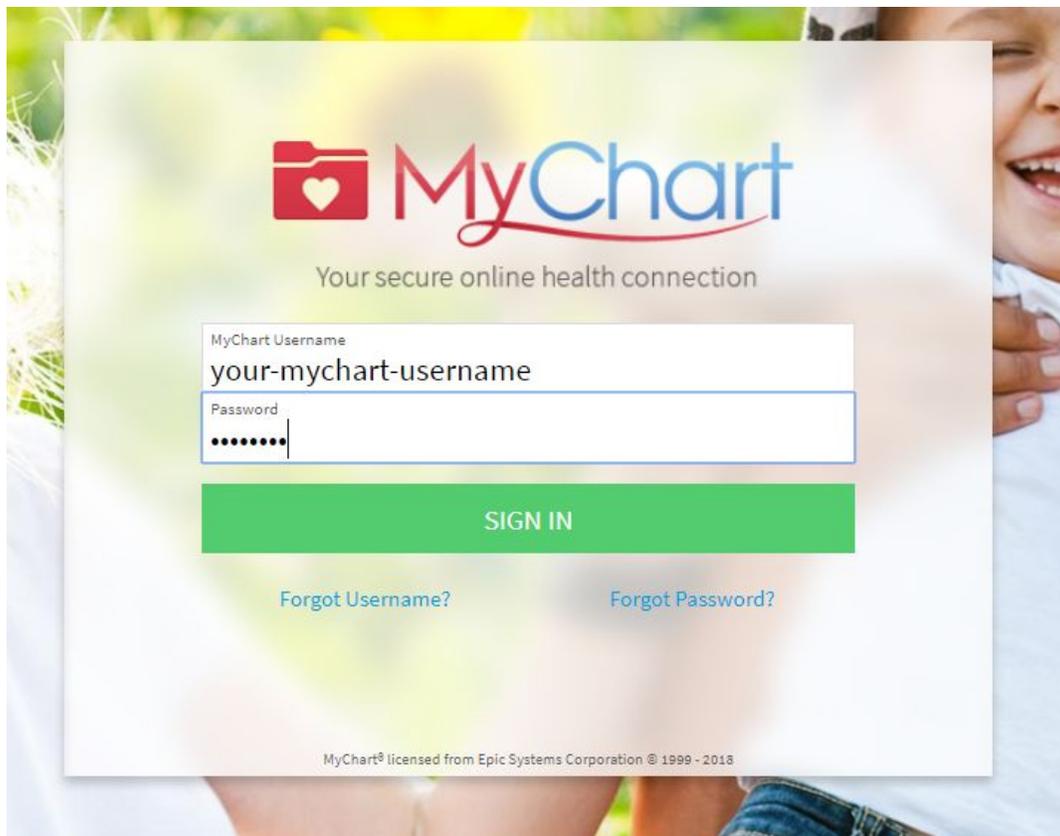


How to allow a third-party app to access your health record

Patients of providers that use Epic software are able to connect third-party applications (apps) to retrieve parts of their health record for their own personal use. Examples of data that can be pulled into an app include lab results, allergies, medications, and immunization history.

In order to authenticate an app to retrieve your health data, follow these steps (note that images may not reflect your healthcare organization's exact layout or content for each step in the process):

1. Make sure you have a MyChart (patient portal) account created for your healthcare provider organization. You will need your login credentials for the authentication process.
2. Access the application on your personal device. Carefully review the app's terms and conditions.
3. The app may ask you to select your healthcare provider from a list. Select your healthcare provider.
4. You will now be redirected to your provider's MyChart login screen. Enter your credentials to continue.



MyChart

Your secure online health connection

MyChart Username
your-mychart-username

Password
●●●●●●●

SIGN IN

[Forgot Username?](#) [Forgot Password?](#)

MyChart® licensed from Epic Systems Corporation © 1999 - 2018

Note: you should not share your password directly with another person or application. This page is designed to let you securely share your health record without disclosing your password. The logo and background image on this page might look different for your healthcare provider, but the general layout of the page should be similar with the Epic

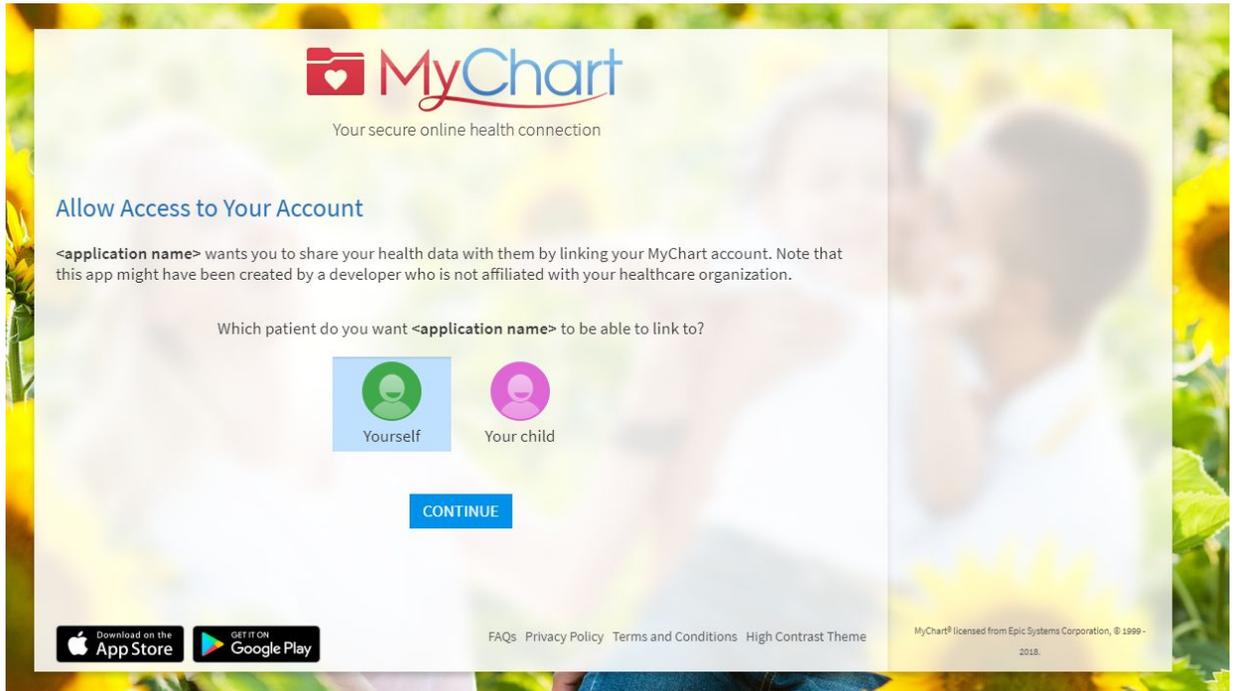
Systems Corporation copyright at the bottom of the screen.

You can also look at the URL at the top of the browser window to check that:

1. The website name is associated with your healthcare provider
2. The URL begins with <https://> or has the lock icon:



5. If you have access to another person's account, you will need to select to which account you are linking the app.



6. You may see a page with details about the application. These details come from a questionnaire that the app developer fills out and attests to, such as how the app is funded, whether it distributes your data to other parties, and whether you're able to delete or see records of the data the app collects. Review this information carefully and determine whether you would like the app to have access to your health information. If you would like to allow the app to access your data, check the "I have read the statements above" box, and then click "Allow Access".

Example of an app that has filled out questionnaire with useful information:

Allow Access to Your Account

<application name> wants you to share your health data with them.

What you need to know about <application name>

Before allowing <application name> to access your account, please be aware of the following important details. This information is provided by the creators of <application name>.

All mentions of the term "data" refer to the data from your electronic health record.



Who is offering the app?

This app is not provided by your healthcare provider, but is provided by <application vendor>, who must follow HIPAA federal health privacy laws.



Does the app developer allow you to obtain a record of the data that have been collected about you?

The app developer allows you to obtain a complete record of the data that have been collected about you.



How is this app funded?

This app is funded by advertisements. This app is funded by sale of your data to other organizations.



Does this app allow you to delete the data that have been stored about you?

This app allows you to delete all of the data that it has stored about you. Keep in mind that, even if the app has deleted your data, the app can't get back data provided to third parties.



Where does this app save your data?

This app can save your data locally on your device.

The app does not keep your data if you remove the app from your device and close your account. The privacy policy and statements of <application vendor> may contain more details.



Who has access to your data when you provide it to this app?

Other than you, the following people and groups may have access to the data that you provide this app, consistent with the privacy policy and statements of <application vendor>:

Researchers

Third parties affiliated with the app offerer

Companies to whom <application vendor> sells your data

You will specifically approve each time your information is accessed or shared.



How does the app developer use your data?

The app developer does not use data about you beyond providing direct services.

<application vendor>'s privacy policy and statements may have more details on how and when the app uses your data.



How long will the app have access to my information?

This app will have access to your information for 1 hour(s) and 0 minute(s), until Wednesday April 15, 2020, 1:24 PM

Allow or Deny Access

<application name> wants your permission to access the following information:



Allergies



Documents



Health Goals



Implants



Lab Results



Problems



Procedural and Diagnostic Orders



Appointments



Clinical Notes



Referrals

Back

Deny Access

Allow Access



Example of an app that has neglected to fill out the questionnaire:



The image shows a screenshot of the MyChart mobile application interface. At the top, the MyChart logo is displayed with the tagline "Your secure online health connection". The main heading is "Allow Access to Your Account". Below this, a red warning banner states: "This app's developer has NOT yet submitted to us how they plan to use your data. Once your data has been shared with <application name>, it could be made public and you may not be able to revoke access to it." A red warning icon (a triangle with an exclamation mark) is shown next to a list of missing Terms of Use items: "What type of organization is offering this app", "How the app is funded", "How your data will be stored", "Who will have access to your data when it is provided to the app", "If this app tells you about the data it has collected about you", "How your data will be retained", and "How your data will be used". Below this, a clock icon is next to the question "How long will the app have access to my information?" and the answer: "This app will have access to your information for 1 hour(s) and 0 minute(s), until Wednesday April 15, 2020, 1:26 PM". The next section is "Allow or Deny Access", which lists various data types: Allergies, Documents, Health Goals, Implants, Lab Results, Problems, Procedural and Diagnostic Orders, Appointments, Clinical Notes, and Referrals. A red warning message states: "Because the app's developer has not informed us of how they plan to use your data, we recommend that you deny access to your account." At the bottom, there are three buttons: "Back" (blue), "Deny Access" (red), and "Allow Access" (green). The footer includes "Download on the App Store" and "GET IT ON Google Play" logos, along with links for "Interoperability Guide", "FAQs", "Privacy Policy", "Terms and Conditions", and "High Contrast Theme". The MyChart logo and "2020" are also present in the bottom right corner.

MyChart
Your secure online health connection

Allow Access to Your Account

<application name> wants you to share your health data with them.

This app's developer has NOT yet submitted to us how they plan to use your data. Once your data has been shared with <application name>, it could be made public and you may not be able to revoke access to it.

This app's developer has not shared any of the following Terms of Use:

- What type of organization is offering this app
- How the app is funded
- How your data will be stored
- Who will have access to your data when it is provided to the app
- If this app tells you about the data it has collected about you
- How your data will be retained
- How your data will be used

How long will the app have access to my information?
This app will have access to your information for 1 hour(s) and 0 minute(s), until **Wednesday April 15, 2020, 1:26 PM**

Allow or Deny Access

<application name> wants your permission to access the following information:

- Allergies
- Documents
- Health Goals
- Implants
- Lab Results
- Problems
- Procedural and Diagnostic Orders
- Appointments
- Clinical Notes
- Referrals

Because the app's developer has not informed us of how they plan to use your data, we recommend that you deny access to your account.

[Back](#) [Deny Access](#) [Allow Access](#)

Download on the **App Store** GET IT ON **Google Play**

[Interoperability Guide](#) [FAQs](#) [Privacy Policy](#) [Terms and Conditions](#) [High Contrast Theme](#)

MyChart® licensed from Epic Systems Corporation
2020.

7. You can review and remove app access to your health data at any time by navigating to the 'Manage My Linked Apps and Devices' page in MyChart.

The screenshot shows the MyChart Epic Medical Center interface. At the top, there is a navigation bar with icons for 'You', 'Health', 'Visits', 'Messaging', 'Billing', 'Resources', and 'Profile'. The 'Profile' icon is highlighted. To the right of the navigation bar, the user's name and a 'Log Out' link are visible. The main content area is titled 'Manage My Linked Apps and Devices' and includes a print icon. Under the heading 'Services Accessing My Account', there is a sub-heading 'You've given the following apps permission to access your data.' Below this, a placeholder box shows '<application name>' with a 'REMOVE ACCESS' button and a 'View Permissions' link. The 'My Linked Devices' section has a sub-heading 'You've added the following devices as trusted devices.' and a message box stating 'You have not authorized any devices.' with a 'BACK TO HOME PAGE' button.