

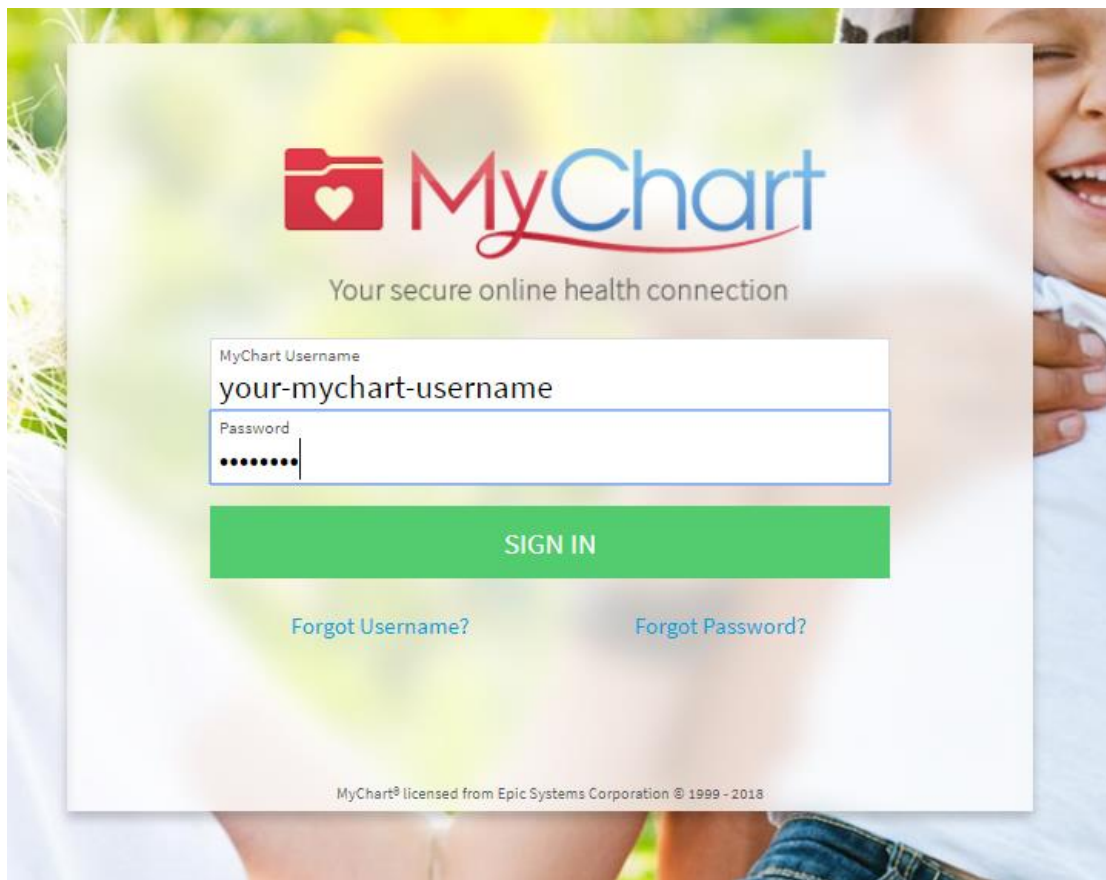
Patient Authentication

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

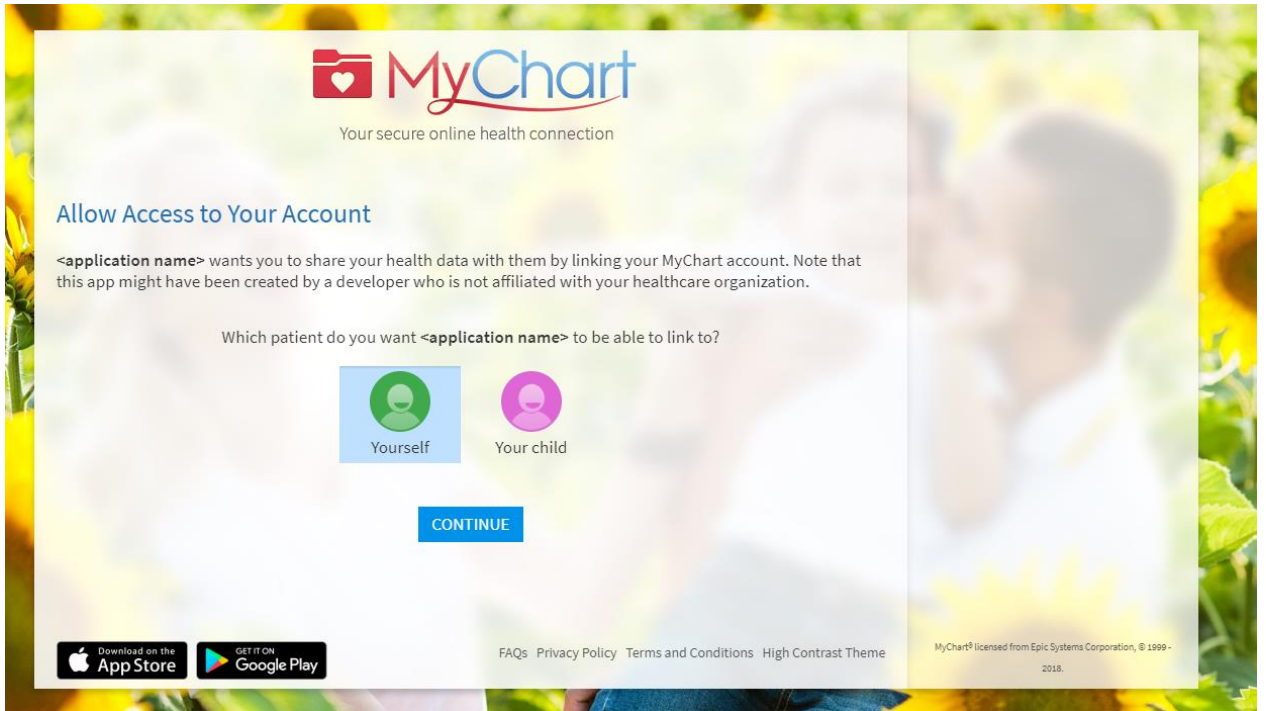
Patients of providers that use Epic software are able to connect third-party applications (apps) to retrieve parts of their health record for their own personal use. Examples of data that can be pulled into an app include lab results, allergies, medications, and immunization history.

To authenticate a third-party app to retrieve your health data from MyChart/your patient portal, follow these steps (images may not reflect your healthcare organization's exact layout or content for each step in the process):

1. Ensure you have a MyChart/patient portal account created for your healthcare provider organization. You will need your login credentials for the authentication process. Note: MyChart is an Epic-specific name. Your healthcare facility may use a different name for its patient portal.
2. Access the MyChart or patient portal app on your personal device. Carefully review the app's terms and conditions.
3. If prompted, select your healthcare provider from the given list.
4. You will be redirected to your provider's MyChart/patient portal login screen. Enter your credentials to continue.



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 (see image below). These details come from a questionnaire that the app developer completes, such as how the app is funded, whether it distributes your data to other parties, and whether you are 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".

Allow Access to Your Account

<application name> wants you to share your health data with them by linking your MyChart account. Note that this app might have been created by a developer who is not affiliated with your healthcare organization.

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" hereafter refers 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.



How is this app funded?

This app is funded by another healthcare provider.



Where does this app save your data?

This app does not save your data.



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

Only people who have access to this device could access the data.



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.

Want to dive deeper? Read more from the app developers of <application name>.

Allow or Deny Access

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



This app will have access to your information until
Monday April 15, 2019, 9:50 AM



Allergies



Problems



Primary Care Provider



Procedures



Demographics



Immunizations

If you have concerns with any one of the points listed above, please deny <application name> from accessing your account.

If you want to grant access, please proceed by confirming you have read the statements above. You can find further information within the app's privacy policy and statements. I have read the statements above

DENY ACCESS

ALLOW ACCESS




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


MyChart
Your secure online health connection

Allow Access to Your Account

<application name> wants you to share your health data with them by linking your MyChart account. Note that this app might have been created by a developer who is not affiliated with your healthcare organization.

 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.


We recommend that you deny access to your account.

 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

Allow or Deny Access


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




This app will have access to your information until
Monday February 25, 2019, 5:36 PM




Allergies




Primary Care Provider




Demographics



Problems



Procedures




Immunizations


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.

If you want to grant access, please proceed by confirming you have read the statements above. You can find further information within the app's privacy policy and statements. I have read the statements above

DENY ACCESSALLOW ACCESS



Download on the
App Store



GET IT ON
Google Play

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

MyChart™ licensed from Epic Systems Corporation, © 1989-2019.

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, and the text 'Your Name Log Out' is visible on the right. Below the navigation bar, the page title is 'Manage My Linked Apps and Devices'. Underneath, there is a section titled 'Services Accessing My Account' with the subtext 'You've given the following apps permission to access your data.' A table-like structure shows one entry: '<application name>' with a 'REMOVE ACCESS' button and a 'View Permissions' link. Below this is a section titled 'My Linked Devices' with the subtext 'You've added the following devices as trusted devices.' A large grey box contains the message 'You have not authorized any devices.' At the bottom center, there is a 'BACK TO HOME PAGE' button.