healthEconnect ALASKA

healthEconnect Alaska's HIE Portal:

Two-Factor Authentication User Guide

V1.0 – September 20, 2021

CONTENTS

Background

As healthEconnect continues expanding our services, it is imperative that we ensure patient data is kept private and secure. A second factor for authentication (2FA) is required for login to the healthEconnect Portal to improve security via the Authy App (or other approve authenticators as they are added to the system).

To log on:

1. Go to https://hub.healthEconnectak.org and enter your username + password.
2. Enter your phone number to receive an activation text message (first time only).
3. Use the SMS text message link to download the Authy app.
4. Receive a push notification from the Authy app to approve log in.

Once activated, a push notification will appear on the user's cell phone via the Authy app to approve all future account login attempts. This user guide describes in detail the 2FA activation and login process, as well as how a user can login within cellular service or update outdated phone numbers.

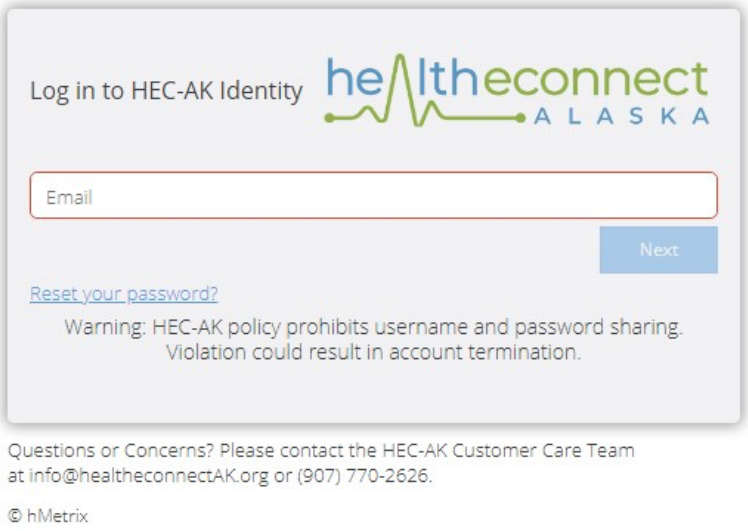
Note that as this portal is currently supported by our partners at CRISP, you will see CRISP support contact information and the CRISP logo when accessing Authy. This is intended. If you have any concerns or hesitation, always feel free to reach out to your Point of Contact to confirm. Remember to always check unfamiliar links or requests before accepting or clicking on them. The CRISP logo is shown below for reference.

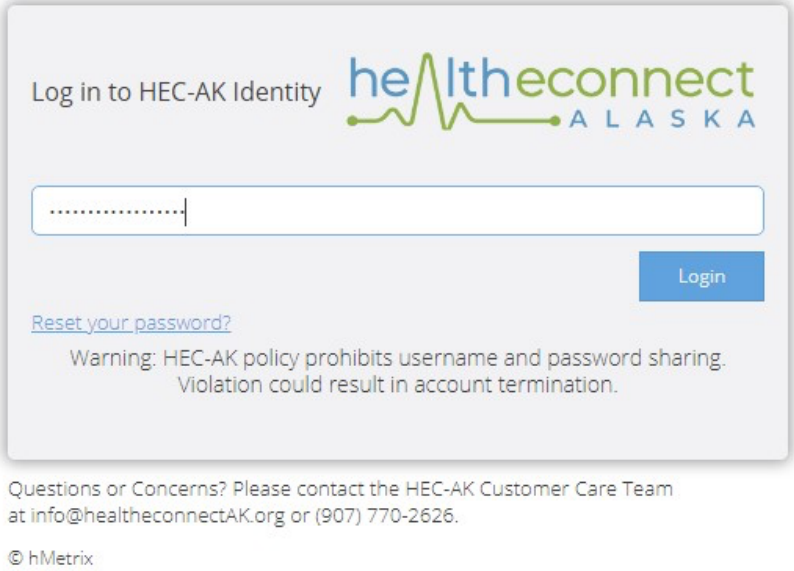
Figure 1: CRISP Partner logo

User Guide

Two-Factor Authentication Set Up

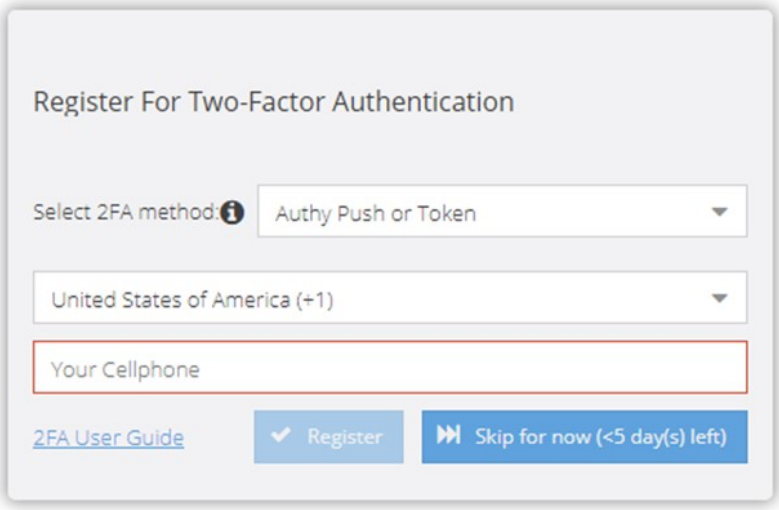
The two-factor authentication feature is enabled for all new and existing healthEconnect Portal users. You as a user will be prompted to set up 2FA on your next healthEconnect Portal Login. You can access the healthEconnect Portal by logging into https://hub.healthEconnectak.org with your User ID and password.





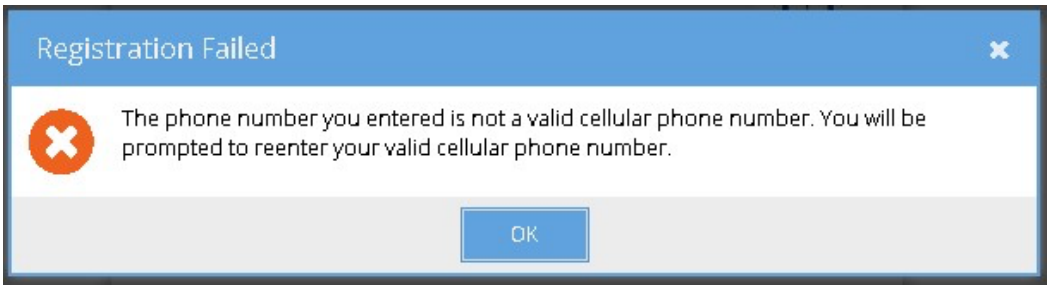
Authy and Other Authenticator Apps

Step 1. You will be presented with a prompt to register for Two-Factor Authentication as shown in the figure below. If you are not ready to activate 2FA, you may skip activation for the next 5 days. After 5 days the activation of 2FA is mandatory, and the skip button will disappear.



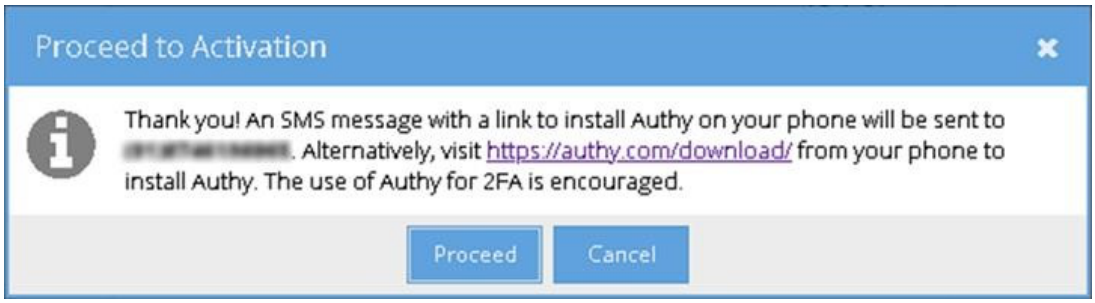
Step 2. Select 'Authy Push or Token' as the 2FA method from the dropdown list. The alternative of a security key (FIDO2) requires a hardware key. The security key option in discussed later in this guide.

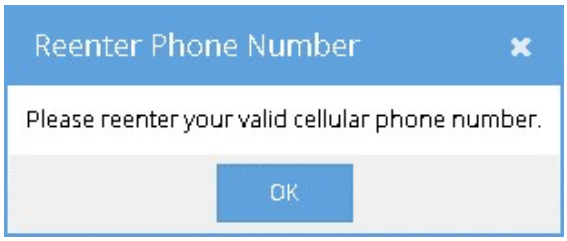
Step 3. You may enter your cellular phone number and register phone number with 2FA by clicking the Register button. When you click the Register button, the healthEconnect Portal will validate that the phone number entered is a cellular phone number. If it is not a cellular phone number, a message is displayed, and you will be prompted to enter your cellular phone number once again. You can click Ok button and reenter the phone number.



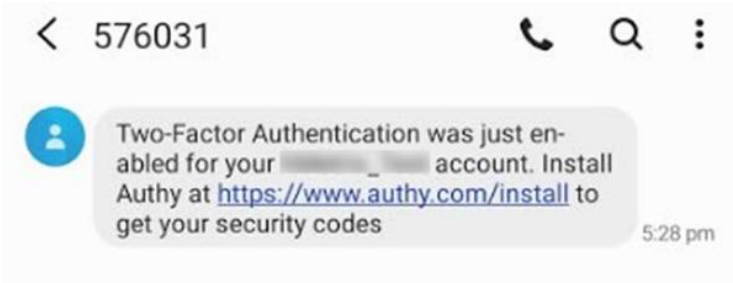
Step 4. After the phone number has been validated, the Proceed to Activation screen shown in the below figure will be displayed. On clicking Proceed, an Authy account will be created with the given phone number and you

will be taken a screen to 'Activate 2FA'. If you click the 'Cancel' button a message will be displayed and will return you to the 2FA Activation screen.

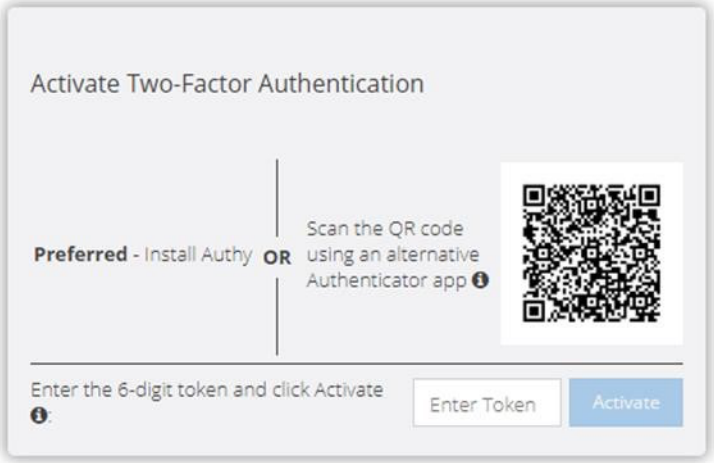




Step 5. Authy will send an SMS text message like the one shown below. Authy will autodetect the device type and redirect you to the appropriate download link. Clicking the link will prompt you to download the Authy application onto your registered device.



Step 6. Use of Authy app is strongly preferred. You can also use an alternative authenticator app, such as Google Authenticator or Microsoft Authenticator. The alternative authenticator app can be used by scanning the QR code in below figure. Please follow the instructions from the alternative authenticator app to scan the QR code.



To activate 2FA, you need to enter a 6-digit token in the Activate 2FA screen. This 6-digit token is available on the newly added healthEconnect LogOnce tab in the Authy app or the alternative authenticator app. You need to enter the 6-digit token in the textbox and clicking the Activate button. If the token is valid LogOnce will grant access to healthEconnect Portal. Otherwise, you need to reenter a valid token. If you refresh or close the browser tab before activation is complete, you need to start over again from the Registration screen.

Security Key (FIDO2)

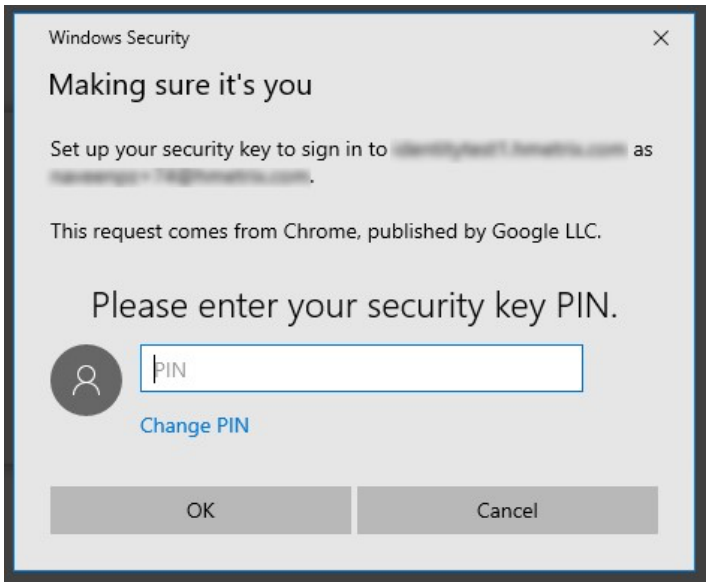
This method of two-factor authentication is the most secure. It requires a hardware or software key that conforms to the FIFO2 standard. Examples are YubiKey, Google Titan, and Feitian ePass FIDO2 security keys. The instructions below assume that you are in possession of such a key and have configured a pin on the key. Please note that a security key cannot be copied or duplicated. Backups of the key are not possible. The key is unique and cannot be substituted with another key.

Step 1. You will be presented with the prompt to register Two-Factor Authentication as shown in the figure below. If you are not ready to activate 2FA, you may skip activation for the next 5 days. After 5 days the activation of 2FA is mandatory, and the skip button will disappear.

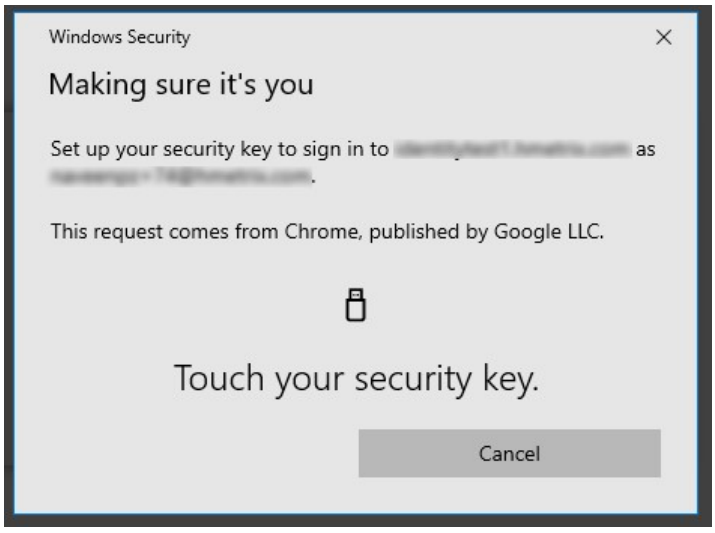
Step 2. Select 2FA method as 'Security Key (FIDO2)' from the dropdown list.

Step 3. Insert the security key into the USB port and click the register button to register the key with the healthEconnect Portal.

Step 4. You will be presented with a security screen like the one below. You need to enter the pin and click OK to continue. Please note that the screen depends on the operating system you are using.



Step 5. You will be prompted to touch the security key's button or biometric scanner. Once you do so, the key will be registered against your LogOnce account and you will be redirected to the healthEconnect Portal.



If you refresh or close the browser tab before registration is complete, you need to start over again.

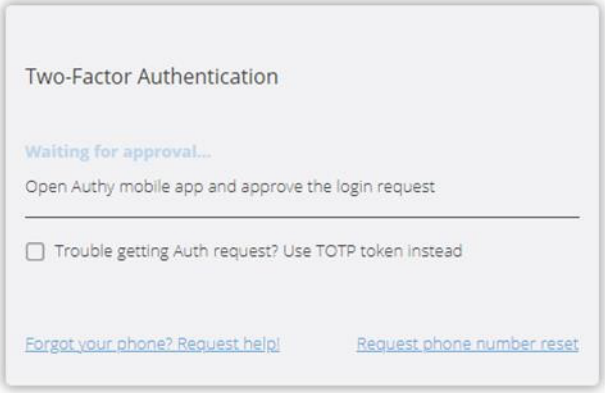
Two-Factor Authentication Login

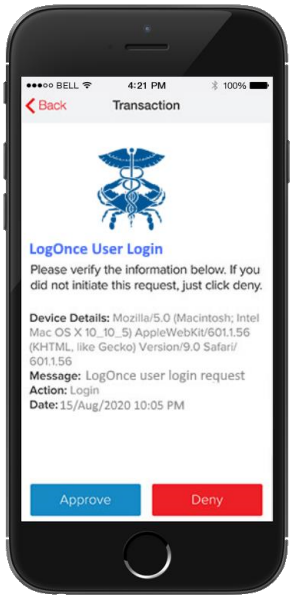
Once 2FA has been activated, when you access the healthEconnect Portal by logging into https://hub.healthEconnectak.org with your User ID and password, you will have the option of verifying 2FA via a push notification that appears on your cell phone via the Authy app, entering the 6-digit token from your chosen Authenticator app, or using a hardware security key. For all future account login attempts you need to follow the steps described below.

Login via Authy

Push Authentication

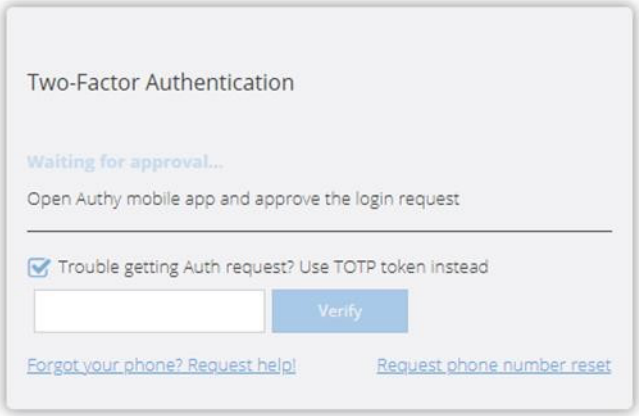
Step 1. If you have registered with the Authy app, you may retrieve pending Push transactions by opening the Authy app. You should verify the information presented on the Authy Authenticator screen before clicking Approve. Should you not recognize the Push request, you should click Deny. If you click Approve, the healthEconnect Portal will grant access to the Landing Page. If you click Deny in the Authenticator app, then the healthEconnect Portal will deny the log in and you will be redirected to the Login page.





TOTP Authentication

Authy's Push notification system requires cellular connectivity. **T**ime-based **O**ne-**T**ime **P**assword (TOTP) allows you to authenticate in healthEconnect Portal without cellular connectivity on your phone. You can generate a TOTP in the Authy application and enter the TOTP token into the healthEconnect Portal instead of the Push approval. The steps below describe the process of user login with TOTP 2FA number.



Step 1. After login to healthEconnect Portal, on the 2FA screen if you have not received the push notification from Authy due to some reason, you can use the TOTP token Authy app to verify your identity.

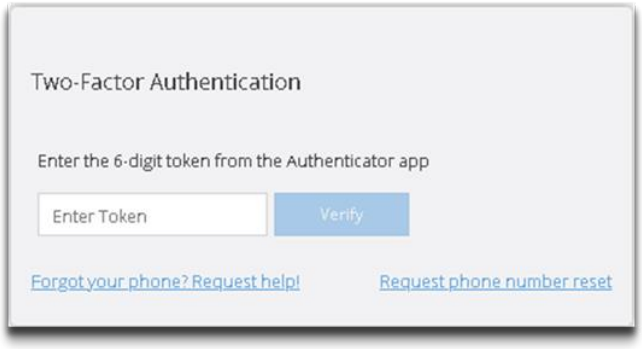
Step 2. You can click to check the option box next to 'Trouble receiving an Auth request? Use TOTP Token Instead".

Step 3. Then you can generate the TOTP token by opening the Authy application on your phone and selecting the healthEconnect Portal tab. The screen will display a token that changes every 30 seconds as shown below.

Step 4. Enter the TOTP token and click Verify to enter the healthEconnect Portal.

Login via other Authenticator Apps

If you activated 2FA using an alternative authenticator app such as Google or Microsoft Authenticator, you need to follow the steps described below. A **T**imebased **O**ne-**T**ime **P**assword (TOTP) allows you to authenticate in healthEconnect Portal without cellular connectivity on your phone in the same way it works for the Authy app.



Step 1. After login to healthEconnect Portal, you will be redirected to a screen like the one below.

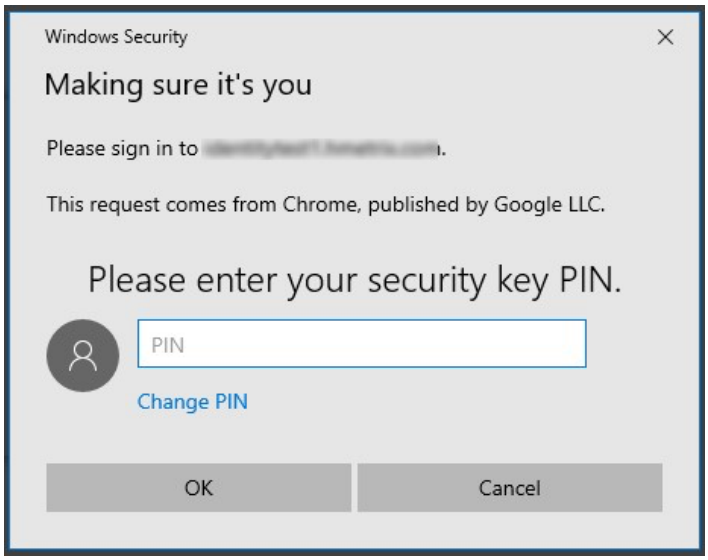
Step 2. Generate the 6-digit TOTP token using the registered Authenticator application on your phone.

Step 3. Enter the token and click Verify complete 2FA.

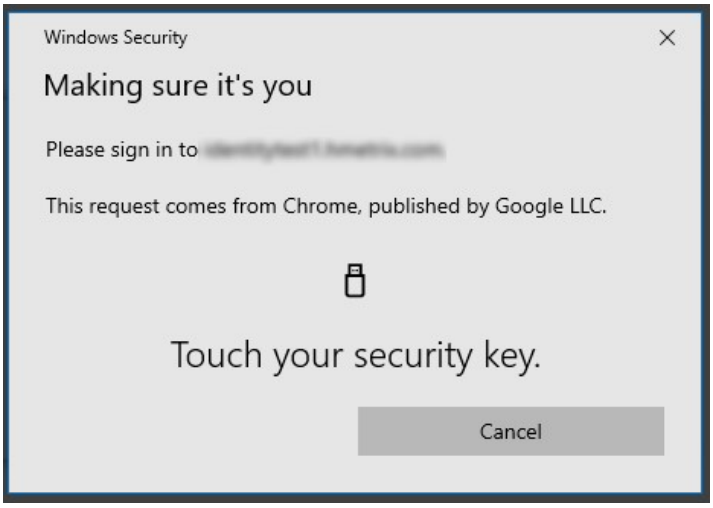
Login via Security Key (FIDO2)

If you activated 2FA using a security key, you need to follow the steps described below. You need to use the same key that you registered with the healthEconnect Portal. No other key will work.

Step 1. After entering your username and password in the healthEconnect Portal, you will be redirected to a security screen like the one below. Please insert the key in your computers USB port. You need to enter the pin and click OK to continue.

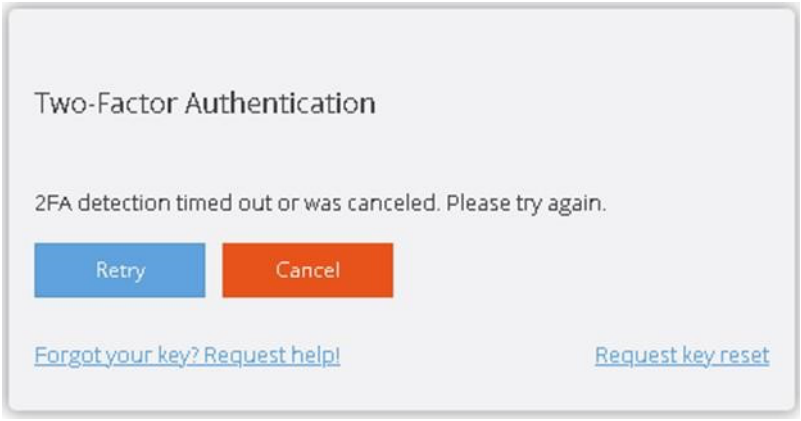


Step 2. You will be prompted to touch the security key's button or biometric scanner. Once you do so and the key is validated, you will be redirected to the healthEconnect Portal.



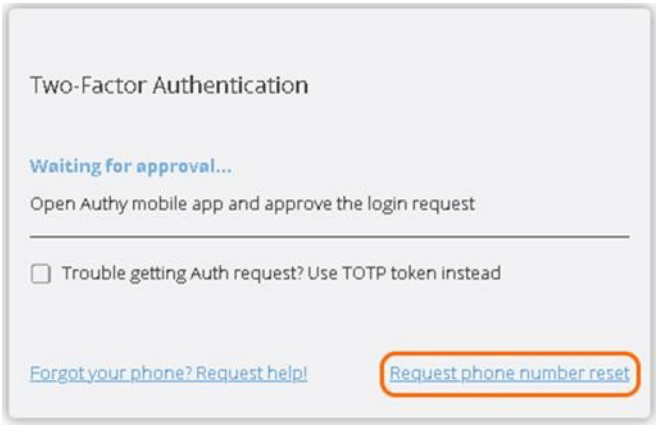
Step 3. If you have temporarily forgotten your security key or lost it and you would like to replace it, click Cancel to request a suspension of 2FA or a reset key request.

Step 4. You will be redirected to the screen below. At the bottom of the screen, you will see the two options for requesting help when you have forgotten you key and a reset key request. The Retry button will redirect you to Step 1 and clicking the Cancel button will redirect you to the login screen.



Reset Phone Number or Security Key

If you need to reset your phone number or security key, you may click on the 'Request phone number reset' or 'Request key reset' link in the healthEconnect Portal 2FA screen. An email will be sent to help@healthEconnectak.org, requesting a Support team member to approve or deny the request. A support team member will verify your identity to approve the request is legitimate. If approved, you must repeat the activation process described in TwoFactor Authentication Set Up section above.



Suspend 2FA

If you forget or misplace your phone or security key temporarily but require important reporting information from the healthEconnect Portal, you may click on the 'Forgot your phone? Request help!' or 'Forgot your key? Request help!' link in the healthEconnect Portal 2FA screen. An email will be sent to help@healthEconnectak.org, requesting a support team member to approve or deny the request. A support team member will verify your identity to ascertain that the request is legitimate. Once the request is approved, the user will be allowed to login to the healthEconnect Portal without 2FA for a temporary period. healthEconnect will monitor these requests closely and has strict protocols in place prevent malicious behavior. Please note this feature is only available during normal office hours.