

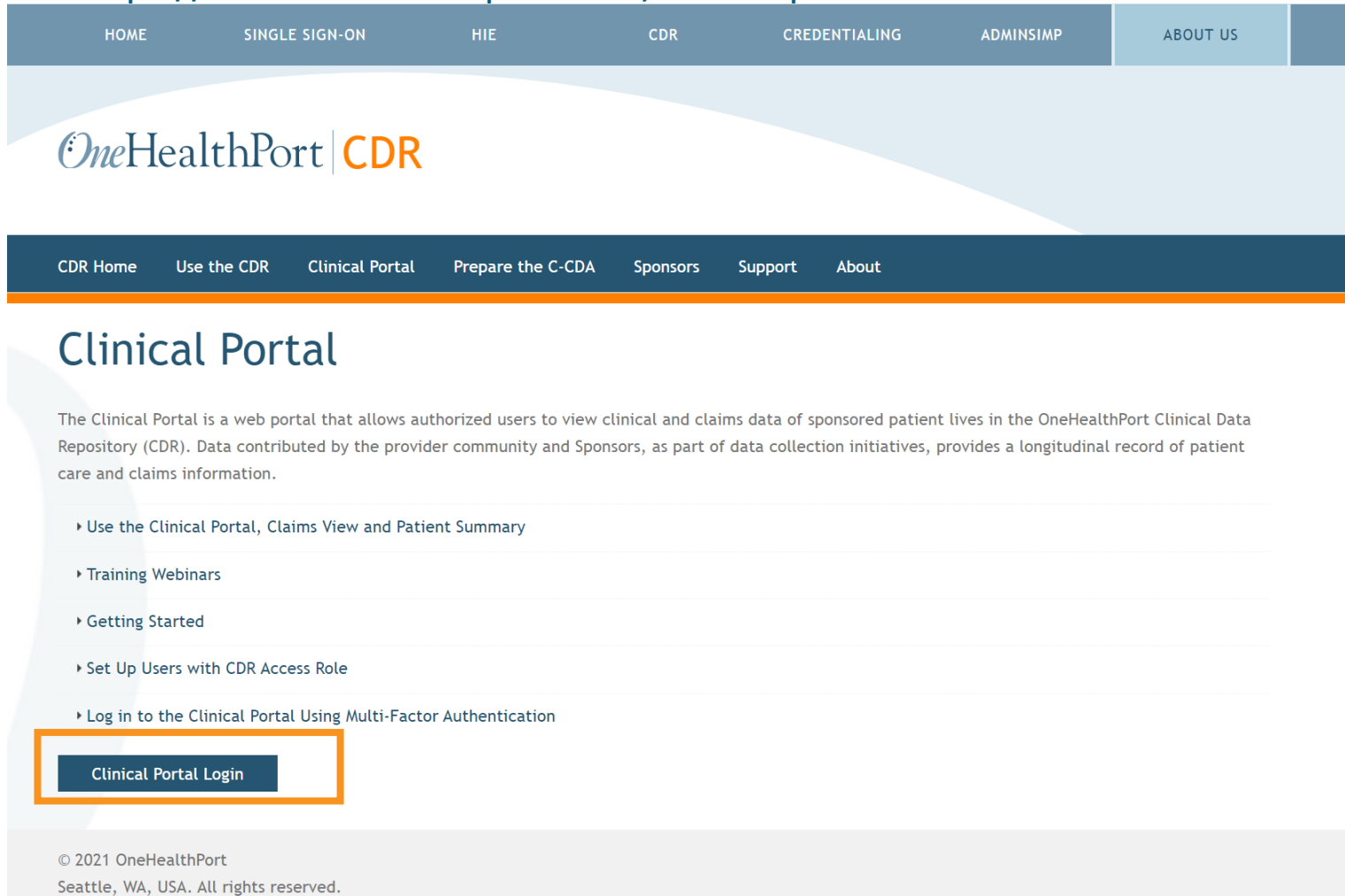


Log in to the Clinical Portal Using Multi-Factor Authentication:

Detailed Instructions on How to
Download and Use Google Authenticator

Link to Clinical Portal

Go to: <https://www.onehealthport.com/clinical-portal>



HOME SINGLE SIGN-ON HIE CDR CREDENTIALING ADMINIMP ABOUT US

OneHealthPort | CDR

CDR Home Use the CDR Clinical Portal Prepare the C-CDA Sponsors Support About

Clinical Portal

The Clinical Portal is a web portal that allows authorized users to view clinical and claims data of sponsored patient lives in the OneHealthPort Clinical Data Repository (CDR). Data contributed by the provider community and Sponsors, as part of data collection initiatives, provides a longitudinal record of patient care and claims information.

- ▶ Use the Clinical Portal, Claims View and Patient Summary
- ▶ Training Webinars
- ▶ Getting Started
- ▶ Set Up Users with CDR Access Role
- ▶ Log in to the Clinical Portal Using Multi-Factor Authentication

Clinical Portal Login

© 2021 OneHealthPort
Seattle, WA, USA. All rights reserved.

Log in to the Clinical Portal



Subscriber ID:

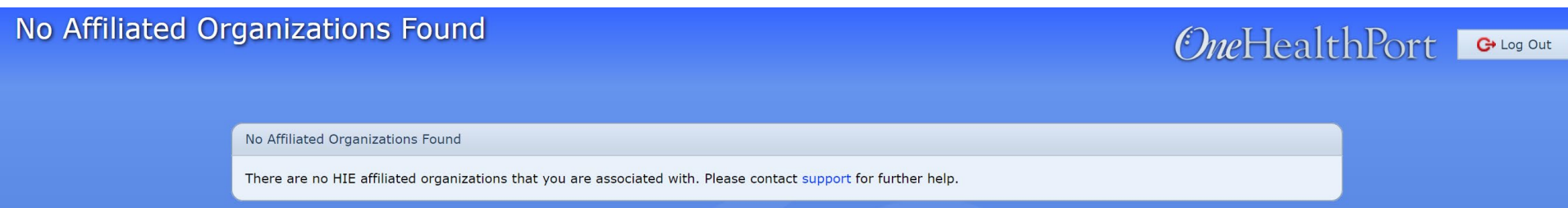
Password:

This login page requires that you have registered as a OneHealthPort Subscriber.

[I'm not a OneHealthPort Subscriber but would like information on subscribing](#)
[Forgot My Password](#)
[Forgot My Subscriber ID](#)

Go to: <http://www.onehealthport.com/clinical-portal> for instructions on how to log in to the Clinical Portal

Error Screen for Denied Access to Clinical Portal



Denied Access to Clinical Portal

- Organizations that do not have an HIE contract will receive this error message.
- Click “support” to be directed to the HIE Support Request Form for HIE contracting information.

Access to the Clinical Portal

- Permitted if organization has an HIE contract.
- Organization’s SSO Administrator has assigned designated user a CDR access role.

Select an Organization

Select Organization

Select the organization you want to use for this session.

OneHealthPort

Log Out

Select an HIE Member Affiliation

- ☐ Select an HIE Member Affiliation
- ☐ Select an HIE Member Affiliation

Select An Organization

Accessing the Clinical Portal

- Designated users that are affiliated with more than one organization that has an HIE contract must select the specific organization to access the Clinical Portal.

HIE Applications Homepage

My Health Information Exchange Account
Summary of HIE Information for Your Organizations

OneHealthPort Log Out

My HIE Information Clinical Portal Reports

HIE Member Affiliations

Selected Organization: Take Out Thai Regression

Take Out Thai Regression Testing
Organization ID: 7uycos08
OHP HIE OID: 1.3.6.1.4.1.38630.2.1.1.326
User Name:
User ID:
Clinical Portal Role: Very Restricted access

Help Documentation
[OneHealthPort Claims View User Guide](#)
[OneHealthPort Clinical Portal User Guide](#)
[Tips For Finding Patients in the Clinical Portal](#)
[OneHealthPort Patient Summary User Guide](#)

- Designated users must have an assigned CDR access role of Normal, Restricted or Very Restricted.
- If user does not have one of these roles, access to the Clinical Portal will not be permitted.
 - If needed, contact the organization's SSO Administrator to obtain a CDR access role.
- Click on Clinical Portal to continue the login process.

Clinical Portal Access Requires Multi-Factor Authentication

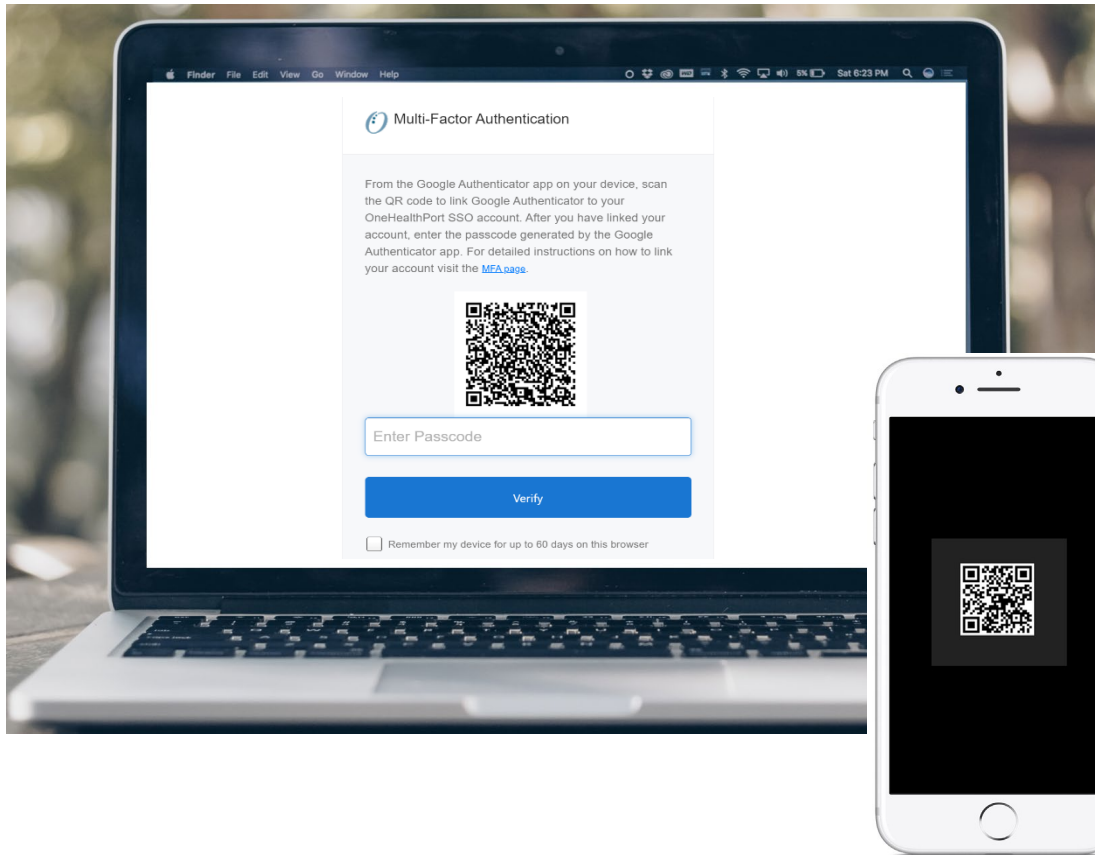
What is Multi-Factor Authentication?

- Multi-Factor Authentication (MFA) adds another layer of security to verify a user's identity by combining two factors that identify an individual.
 - What the user knows (such as a username and password)
 - What the user has (such as a phone or tablet device that generates a token)
- Currently the Clinical Portal requires the use of Google Authenticator for MFA.

What is Google Authenticator?

- Google Authenticator is a free app that is downloaded to a user's mobile or tablet device that generates a 6-digit passcode which must be provided in addition to the username and password to log in.
 - The app is free and does not use cell phone minutes or data
 - Users do not need to create a Google account

First Time Using Google Authenticator



If you are using Google Authenticator for the first time, you will need to download the app before you can begin.

STEP 1: Start the MFA authentication process. For first time users the Google Authentication QR code will automatically appear.*


STEP 2: Using the device camera, scan the QR code **on computer screen** to automatically link Google Authenticator to the OneHealthPort SSO account.

*If you need to link a new device and do not see the QR code, please contact our Help Desk at 1.800.973.4797

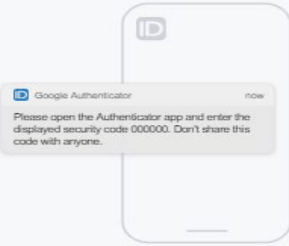
MFA Verification Using the Passcode

Open Google Authenticator on your device, enter the passcode and click **“Verify”**. Do not add spaces when entering your passcode.



 Multi-Factor Authentication

The site or application you are trying to access requires Multi-Factor Authentication. To verify your identity, enter the passcode generated by the Google Authenticator app on your device then press "Verify".



Enter Passcode

Verify

☐ Remember my device for up to 60 days on this browser

Note: The Clinical Portal application does not allow the option to “Remember my device for up to 60 days on this browser.” You will be prompted to complete MFA every time you log in to the application.

Successful Login to the Application

The screenshot displays the OneHealthPort Clinical Portal interface. At the top left is the logo. To its right is a search bar with a plus icon, the text "Find Patients", and a magnifying glass icon. On the far right of the header, there is a user profile icon labeled "jason123" and a "Logout" button. Below the header, the interface is divided into two main sections. The left section, titled "Notifications" with a count of 0, contains a dropdown menu set to "10 days" and a table with columns "Name", "Subject", and "Received". The table body shows the message "There is no data available". The right section, titled "Recent Patients" with a count of 10, displays a list of patient records, each with a star icon and a trash can icon for actions.

Successful verification of the passcode will permit access to the application.

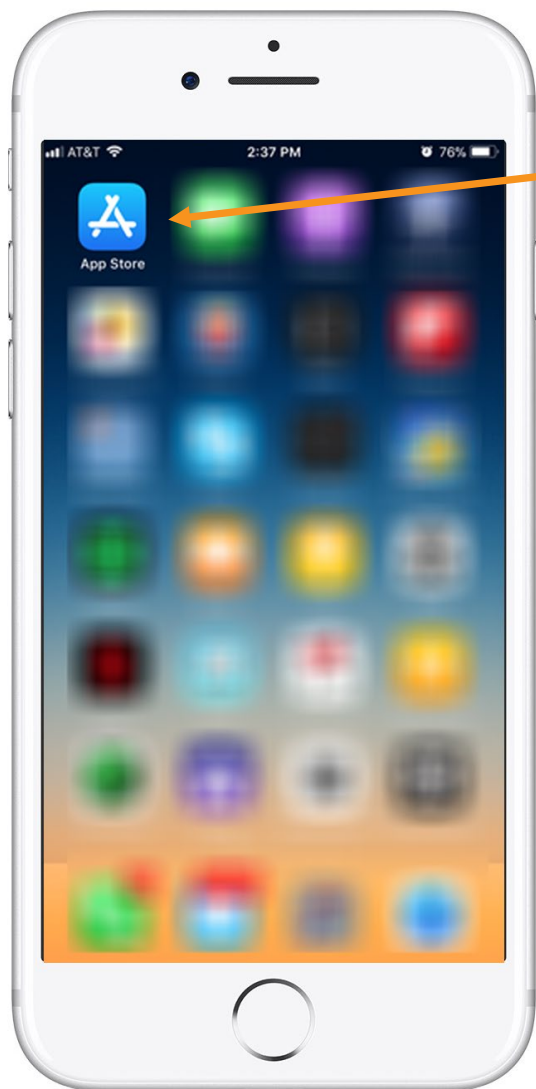
Detailed Instructions to Download Google Authenticator

Step-by-step instructions for downloading the Google Authenticator app and linking it to the user's OneHealthPort SSO account.

- [Instructions for Apple Devices](#) (Slide 12)
- [Instructions for Android Devices](#) (Slide 25)

Instructions for Apple Devices

Access the App Store



Tap on the App Store icon. If it's the first time opening the App Store, you will be prompted to:

- Log in with Apple ID and password
- Enter payment details (this step can be **SKIPPED***)

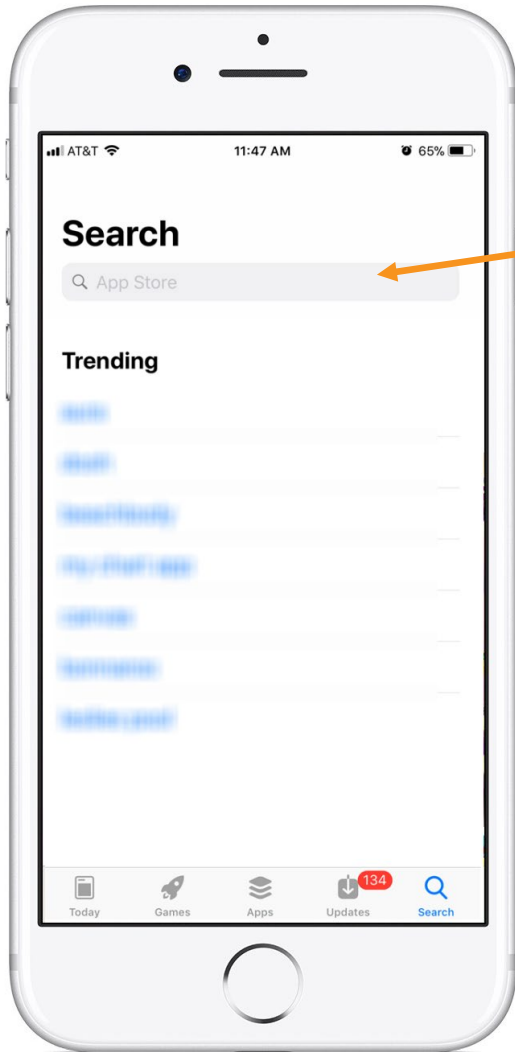
*For more information on how to skip adding payment information see <https://support.apple.com/en-us/HT204034#iOS>

Search for an App in the App Store



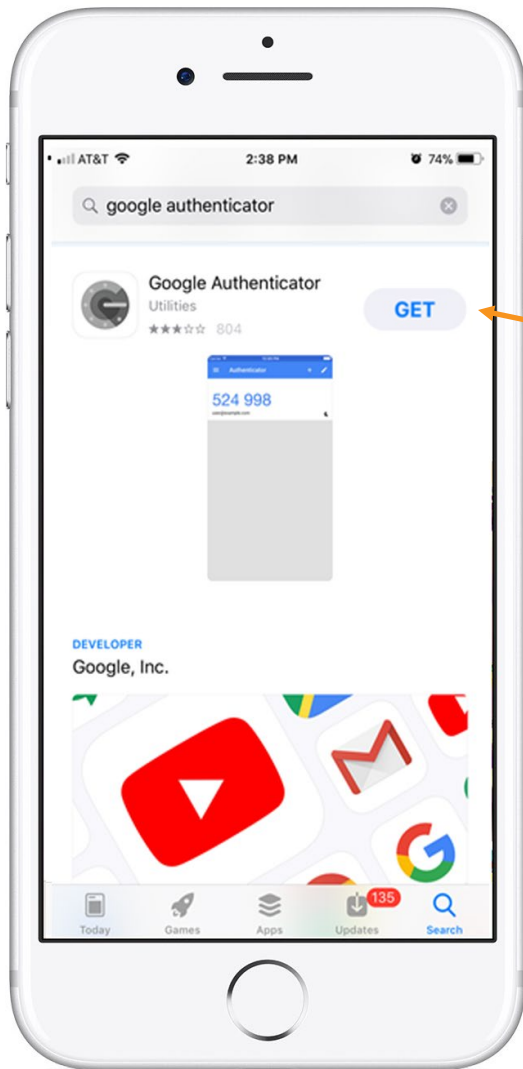
Tap the Search key. It's the key that looks like a magnifying glass at the phone's bottom right corner.

Search for Google Authenticator



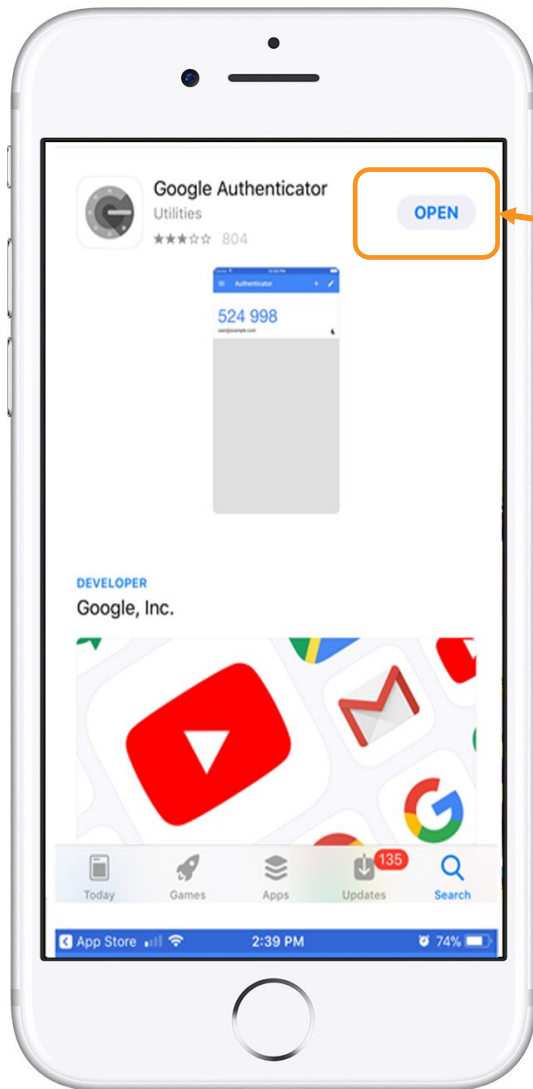
In the Search function, the device brings up the search box. Type “**Google Authenticator**”

Download Google Authenticator



Once you find the App, tap on **“GET”** to start downloading the app.

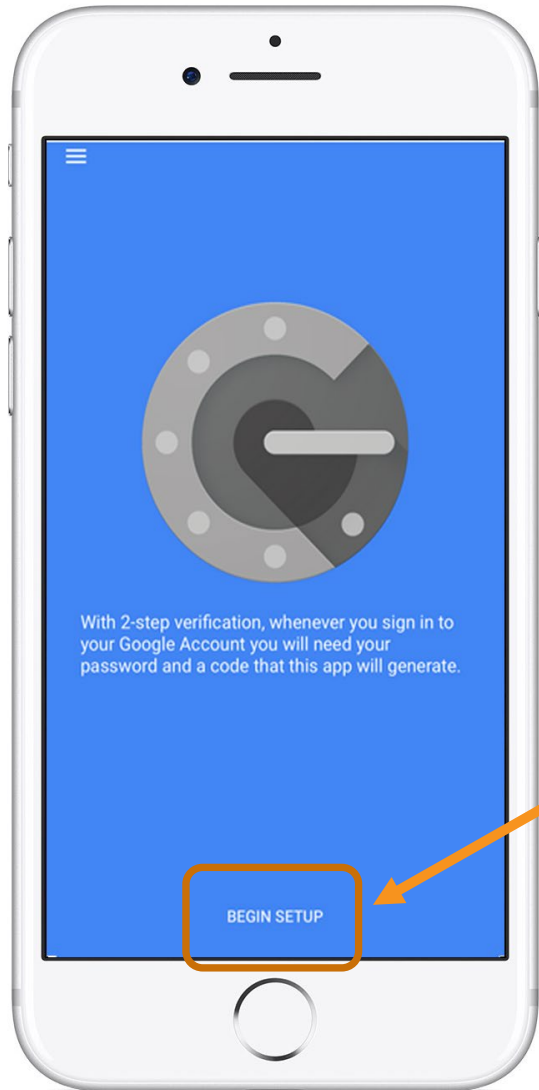
Open the App



Tap on **"OPEN"** once the app has completed the download.

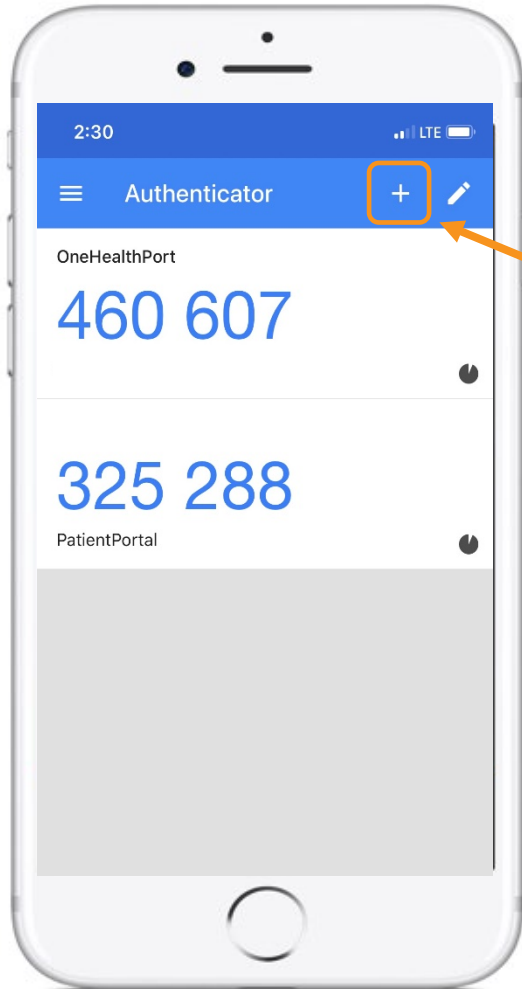
Linking the Google Authenticator App to Your OneHealthPort SSO Account

Setup



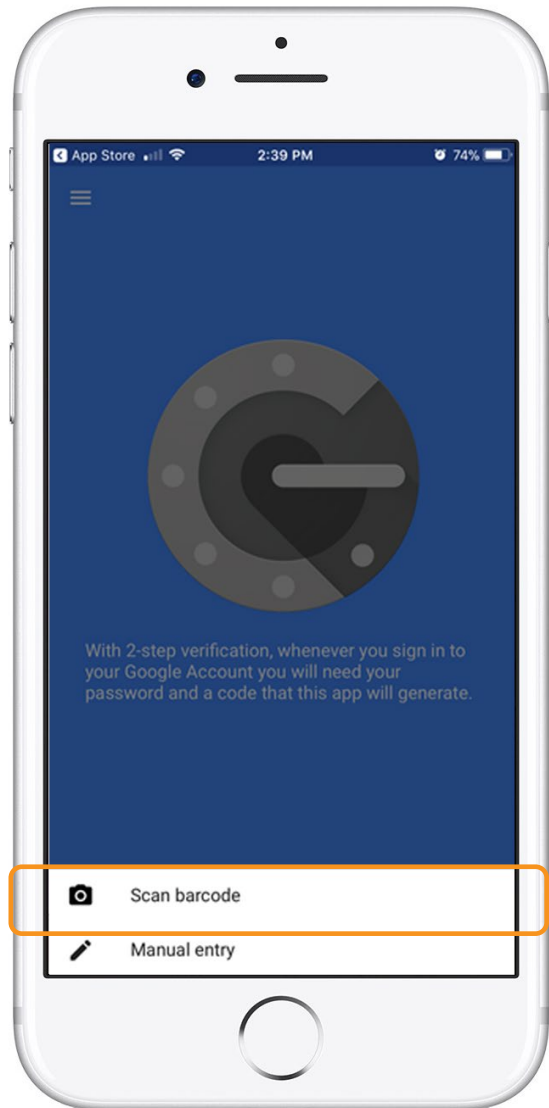
Tap on **“Begin Setup”**.

Adding An Account



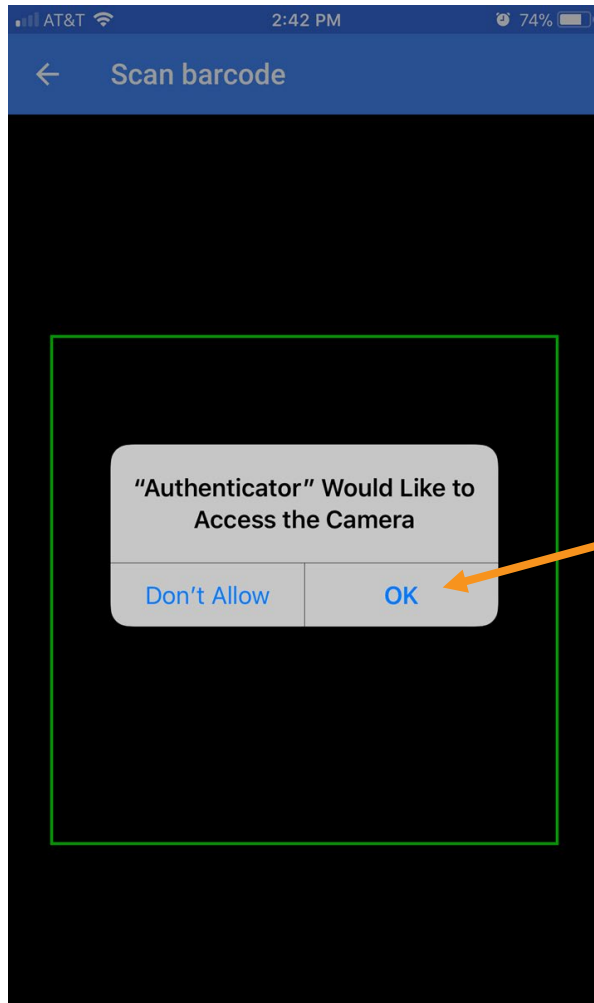
If you've already downloaded Google Authenticator to your phone and are using it with a different account, you can add your OneHealthPort account by clicking the plus sign at the top.

Scan Barcode



Tap on “Scan barcode”.

Authenticator Access to the Camera



Google Authenticator requires access to the device camera to complete the linking process with your OneHealthPort SSO account. Tap on "OK".

Linking to OneHealthPort SSO Account

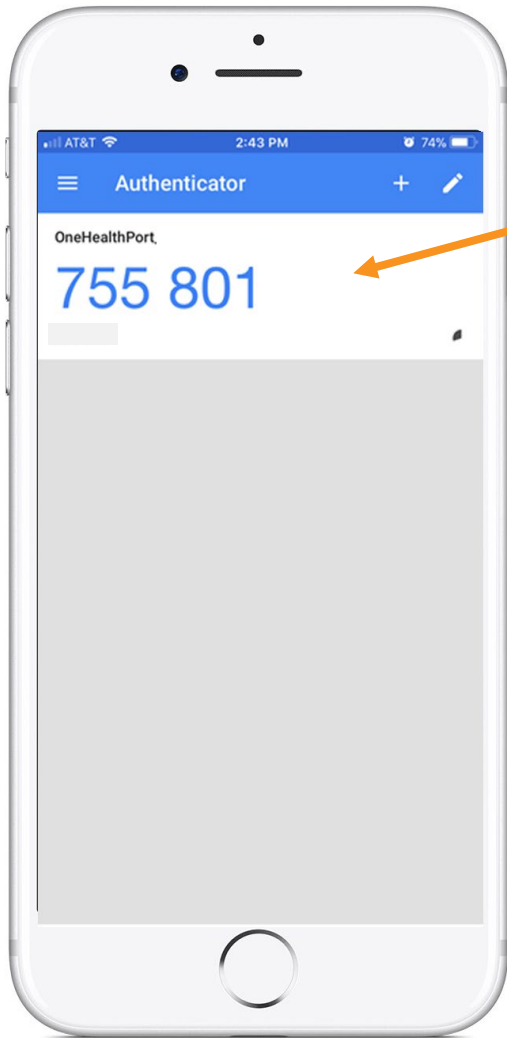


STEP 1: Start the MFA authentication process. For first time users the Google Authentication QR code will automatically appear.*

STEP 2: Using the device camera, scan the QR code **on computer screen** to automatically link Google Authenticator to the OneHealthPort SSO account.

*If you need to link a new device and do not see the QR code, please contact our Help Desk at 1.800.973.4797

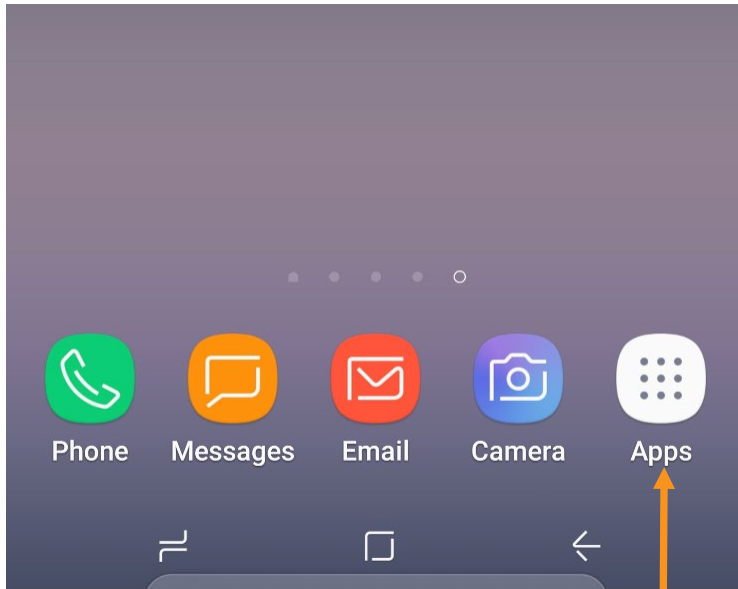
Successful Link to OneHealthPort Account



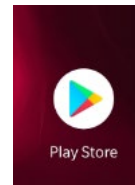
Linking is successful to your OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and “OneHealthPort” is above the passcode.

Instructions for Android Devices

Access the Play Store



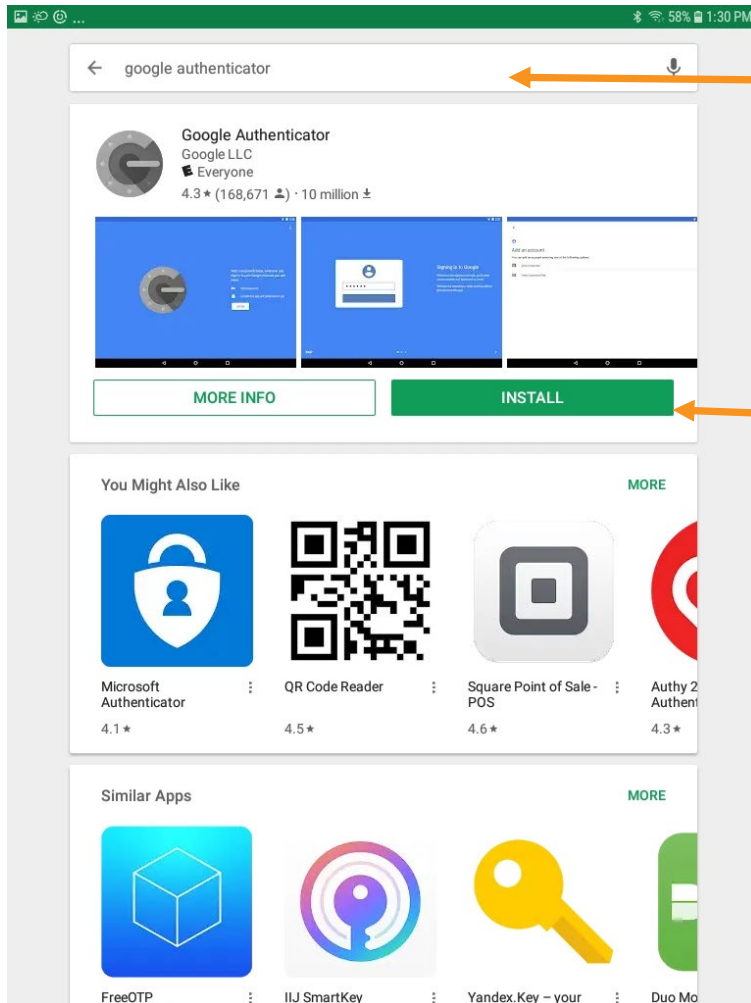
STEP 1: Tap on the “Apps” icon



STEP 2: Tap on the “Play Store” icon

If it's the first time opening the Play Store, you will be prompted to enter Google account information and payment details. This step can be **SKIPPED**.

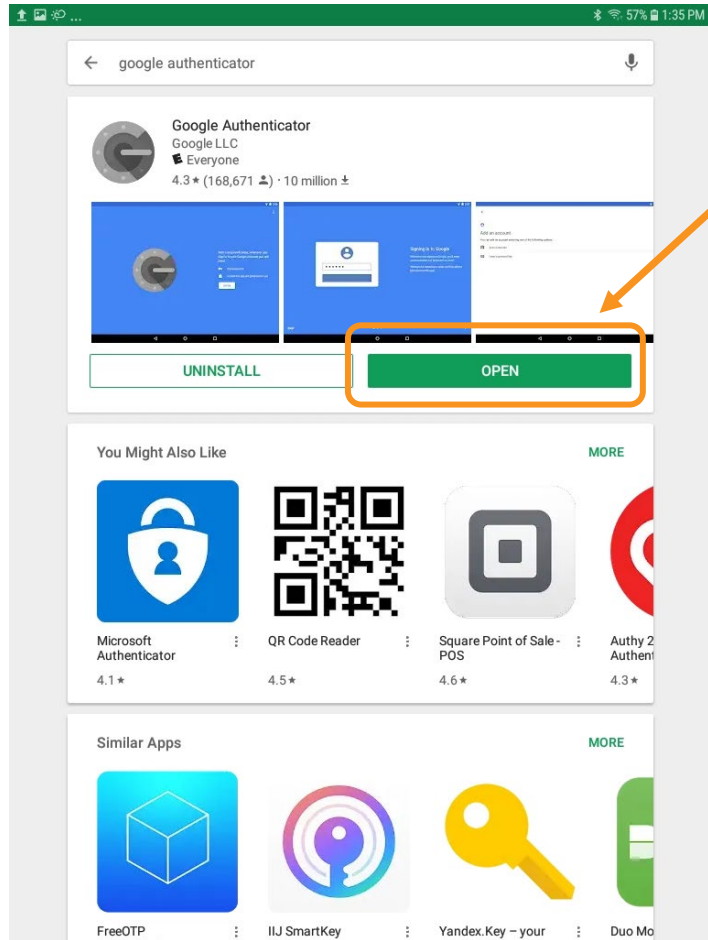
Search for Google Authenticator



Type "Google Authenticator" in the Search box.

Once the Google Authenticator app is found, tap on "**INSTALL**" to start downloading the app.

Open the App

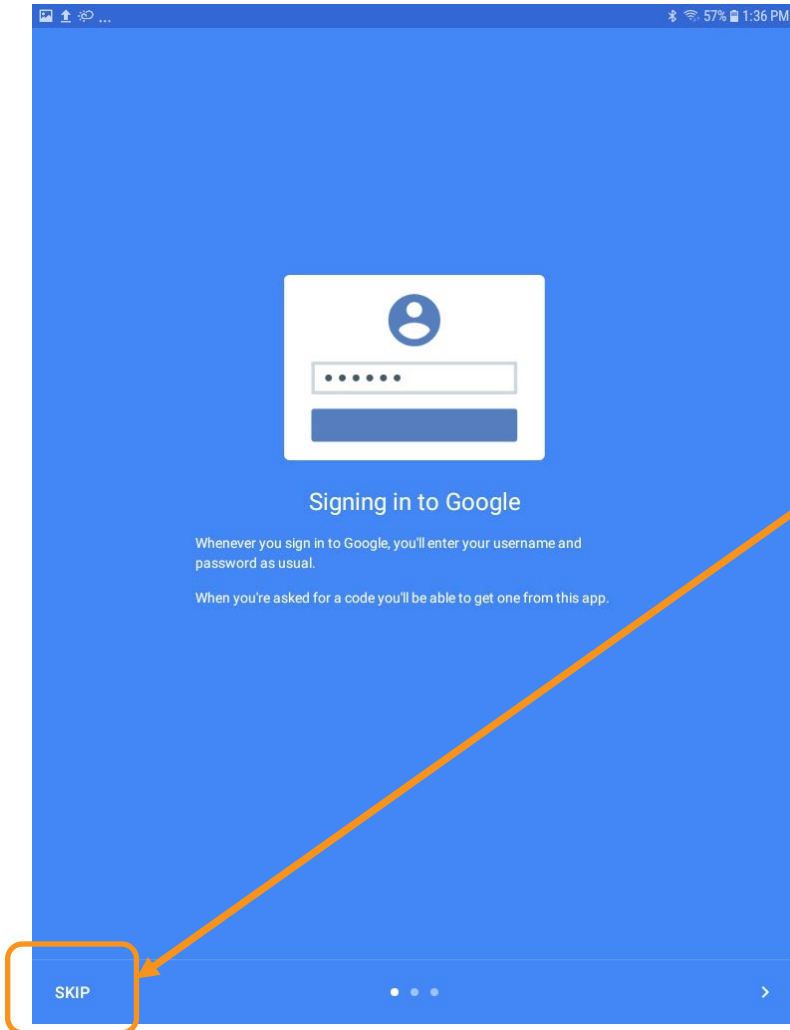


Tap on “**OPEN**” once the app has completed the download. App may also be accessed from the icon on the home screen.



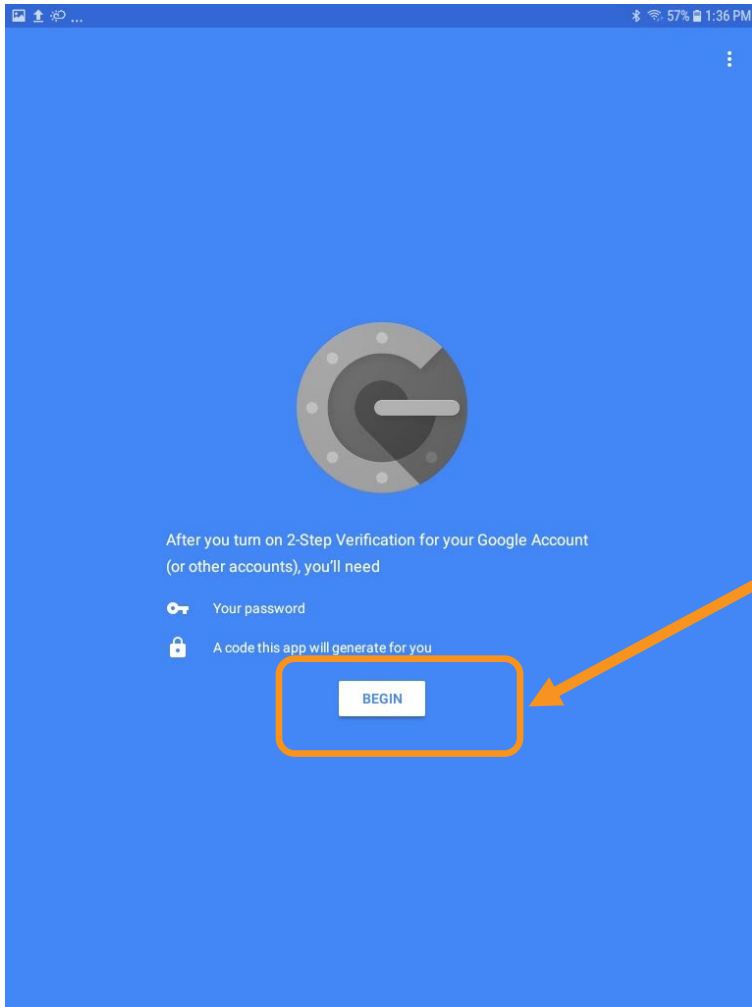
Linking the Google Authenticator App to Your OneHealthPort SSO Account

Setup



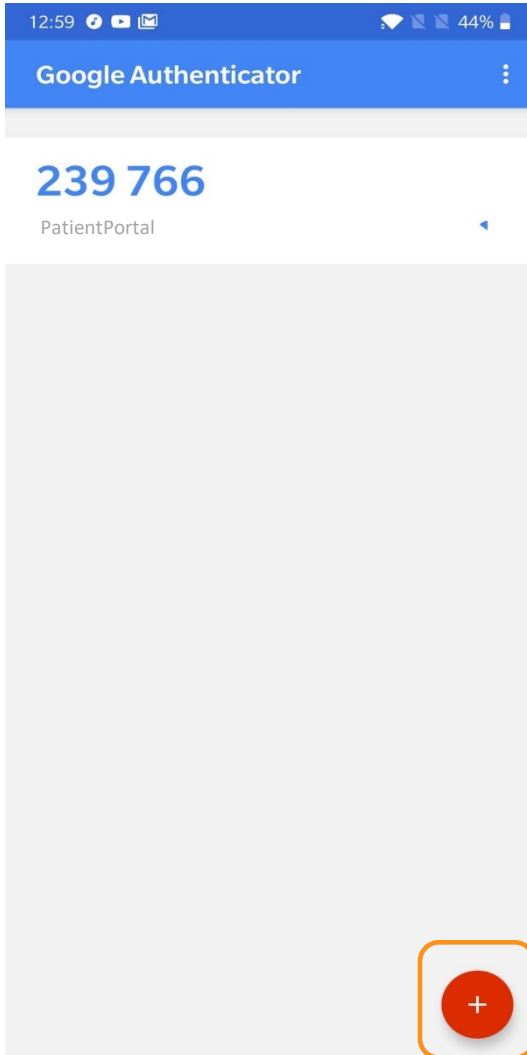
Open the Google Authenticator app. **Skip** Signing into Google.

Begin



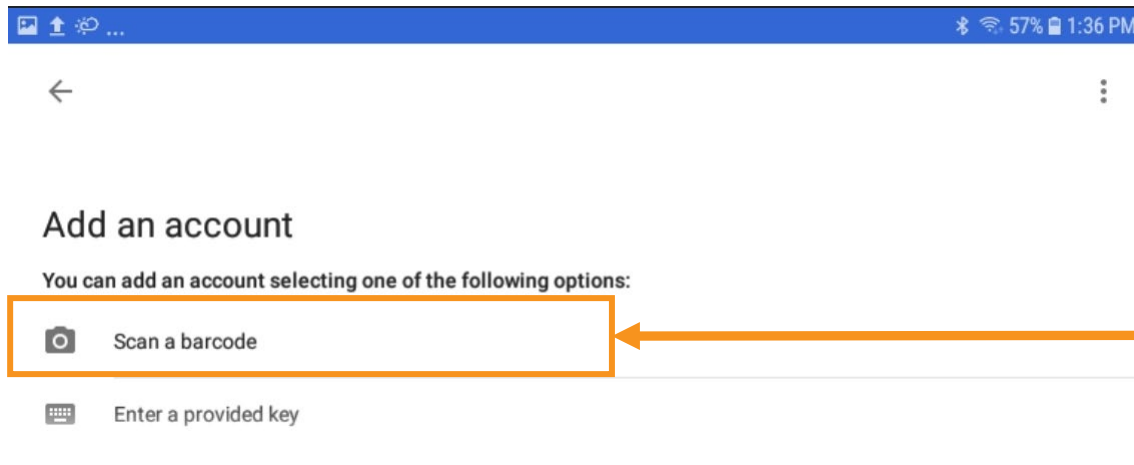
Tap to **Begin** setup.

Adding An Account



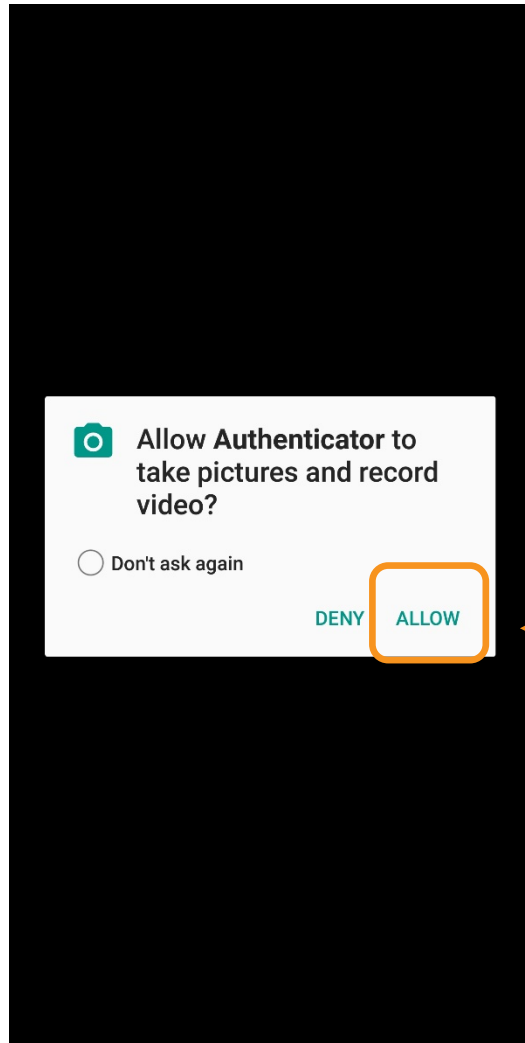
If you've already downloaded Google Authenticator to your phone and are using it with a different account, you can add your OneHealthPort account by clicking the plus sign at the bottom.

Scan a Barcode



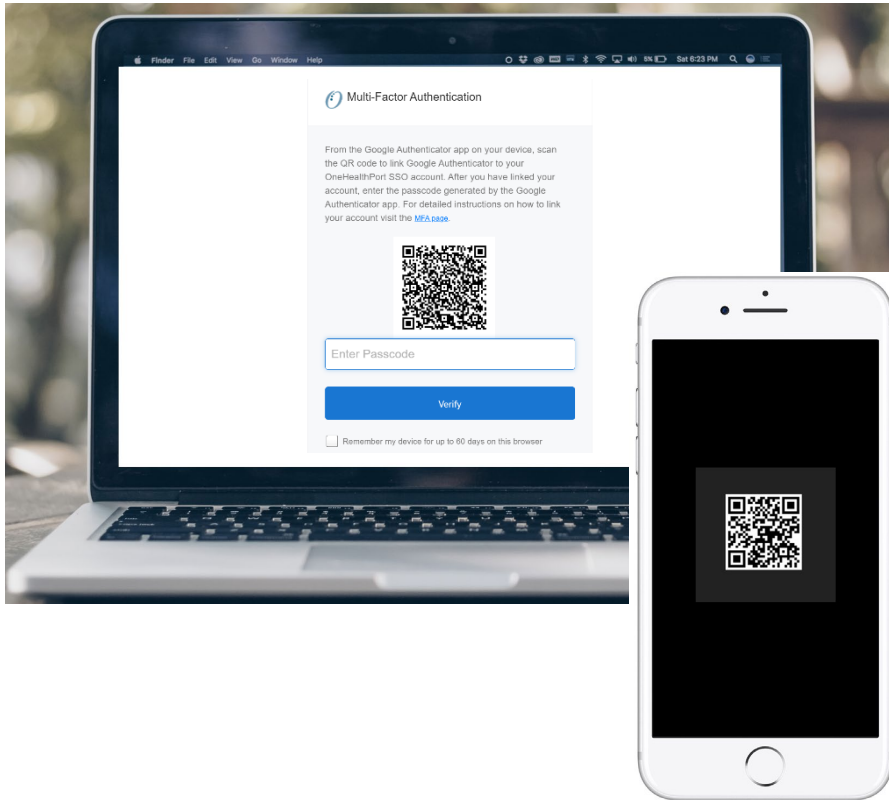
Tap to **Scan a
barcode**

Authenticator Access to the Camera



Google Authenticator requires access to the device camera to complete the linking process with your OneHealthPort SSO account. Tap on **“ALLOW”**

Linking to OneHealthPort SSO Account

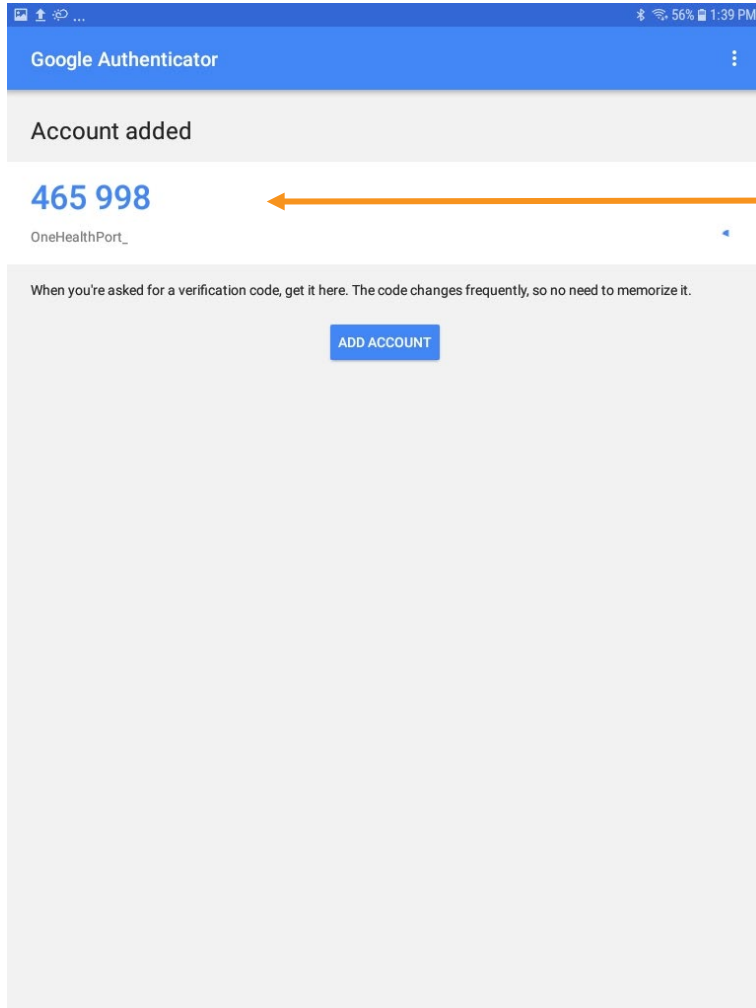


STEP 1: Start the MFA authentication process. For first time users the Google Authentication QR code will automatically appear.*

STEP 2: Using the device camera, scan the QR code **on computer screen** to automatically link Google Authenticator to the OneHealthPort SSO account.

*If you need to link a new device and do not see the QR code, please contact our Help Desk at 1.800.973.4797

Successful Link to OneHealthPort Account



Linking is successful to your OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and "OneHealthPort" is below the passcode.