



# Login to the Clinical Portal Using Multi-Factor Authentication:

Detailed Instructions on How to  
Download and Use Google Authenticator

# Login 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 login to the Clinical Portal

# Error Screen for Denied Access to Clinical Portal



## Denied Access to Clinical Portal

- Organizations that do not have a 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

- [Faded text]
- [Faded text]

Select An Organization

## Accessing the Clinical Portal

- Designated users that are affiliated with more than one organization that has an HIE contract must select an 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 Provider Directory C-CDA Validation Testing

HIE Member Affiliations

Selected Organization: [dropdown]

**Test Sue's Pain Clinic**  
Organization ID: s33e0y00  
OHP HIE OID: 1.3.6.1.4.1.38630.2.1.1.325  
User Name: [redacted]  
User ID: [redacted]  
Clinical Portal Role: Very Restricted access

- 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 an 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)
  - What the user is (such as a fingerprint, iris scan etc.)\*
- Not all applications require MFA. Users will be prompted for MFA only when they try to access an application that requires MFA.
- Currently the Clinical Portal requires users to use Google Authenticator as the 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 six to eight-digit passcode which must be provided in addition to the username and password to login.
  - The App is free and does not use cell phone minutes or data
  - Users do not need to create Google account

**\*NOTE: Currently OneHealthPort does not use this type of identity verification to authenticate users.**

# First Time Using Google Authenticator

Your software token was issued successfully. Please check your email for further instructions.

Ok



**MULTIFACTOR AUTHENTICATION**

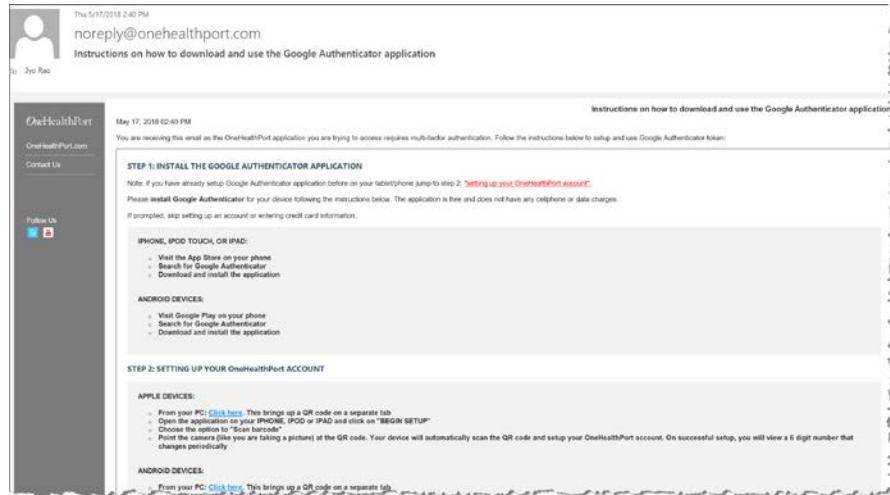
The application you are trying to access requires multi-factor authentication. To verify your identity, enter the code generated by the Google Authenticator application on your smartphone or tablet.

[Verify](#)

[Click here to email instructions on how to download the Google Authenticator application](#)

If the user is using Google Authenticator for the first time, click the hyperlink. The system will email detailed instructions to the email affiliated with the user's OneHealthPort SSO account to download the App to a smartphone or tablet device and link the authenticator to the user's OneHealthPort SSO account.

# Emailed Instructions for Installing and Using Google Authenticator



The content in this email gives directions for:

- Downloading the application
- Linking it to the user's OneHealthPort SSO account
- Using the authenticator passcode



# 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 10)
- [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, the user will be prompted to:

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

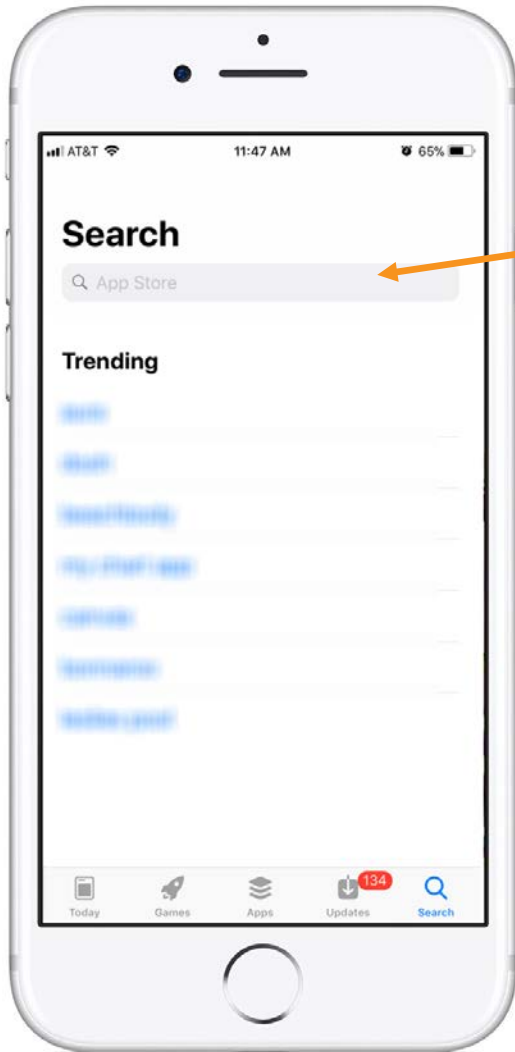
For more information on how to skip adding payment information see <https://support.apple.com/en-us/HT204034#iOS>

# Search for an App in the App Store



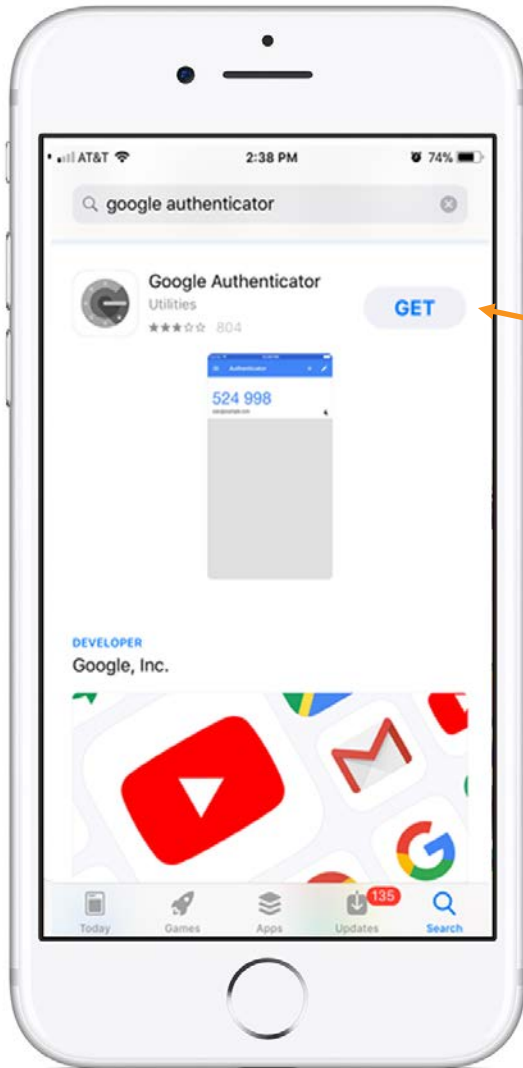
**Tap the Search key.** It's the key that looks like a magnifying glass at the phone's bottom right corner.

# Search for Google Authenticator



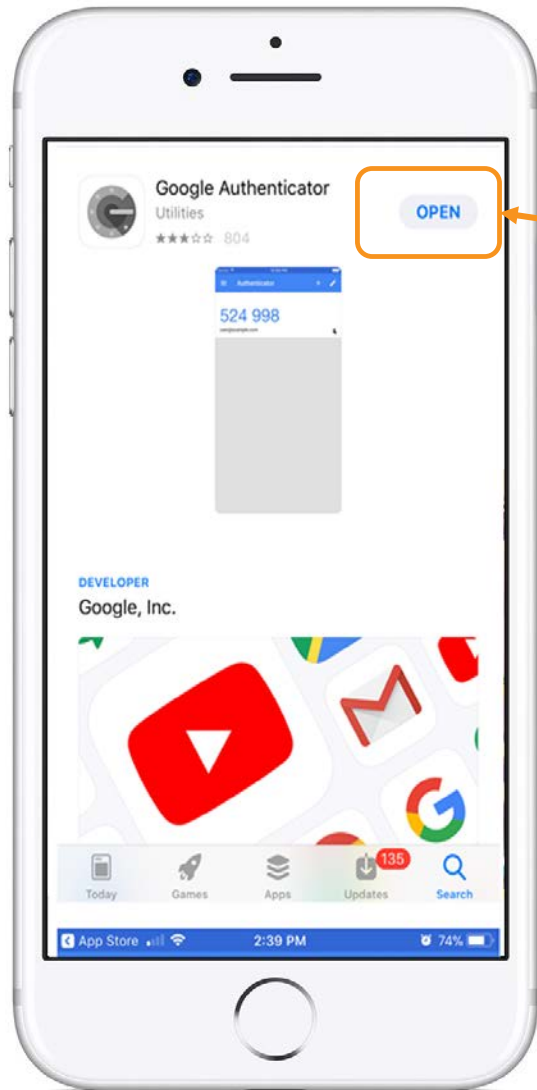
In the Search function, the device brings up the search box. Type **“Google Authenticator”**.

# Download Google Authenticator



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

# Open the App

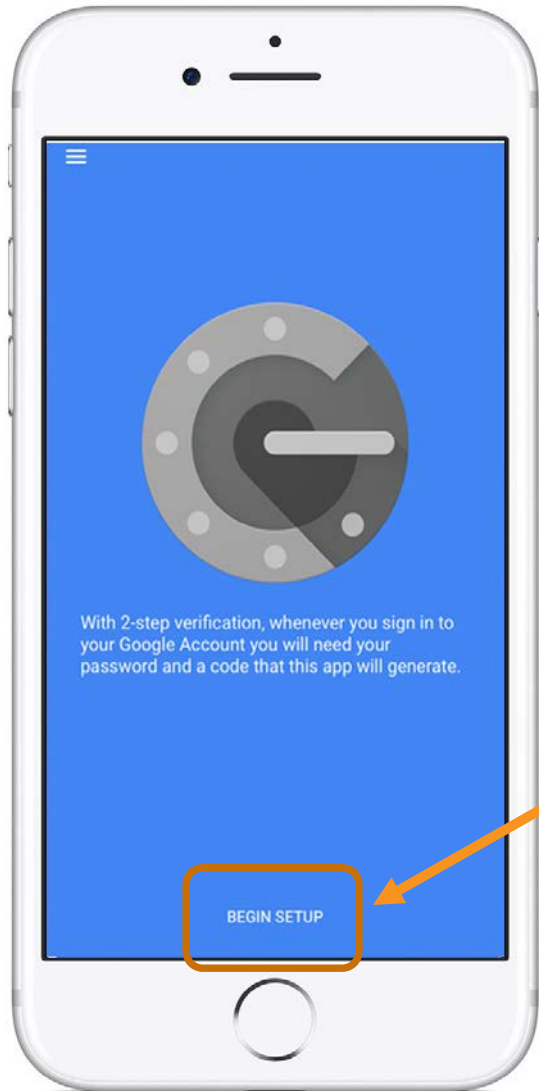


Tap on **“OPEN”** once the App has completed the download.

# Linking the App to the User's OneHealthPort SSO Account

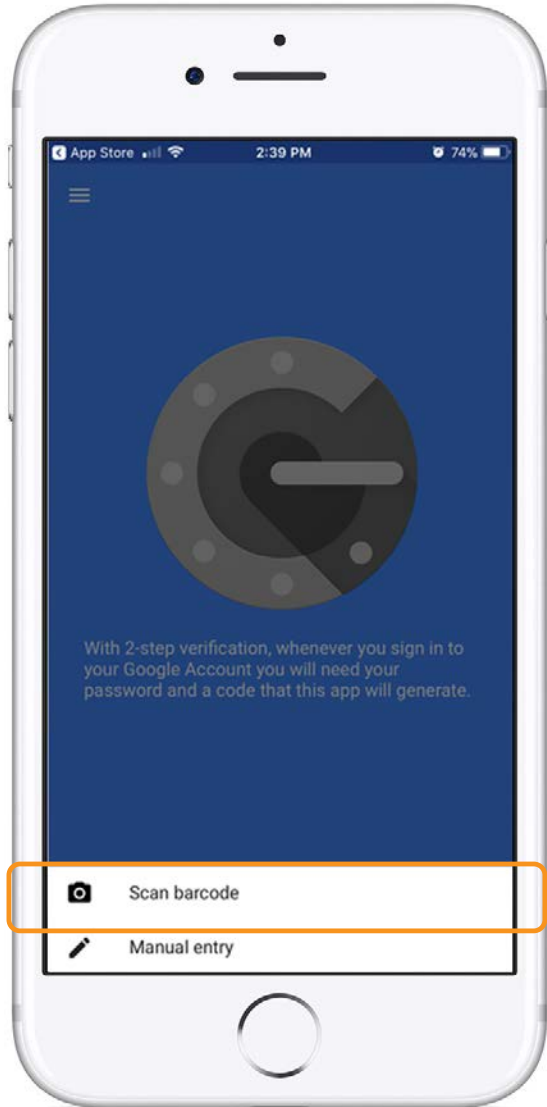


# Setup



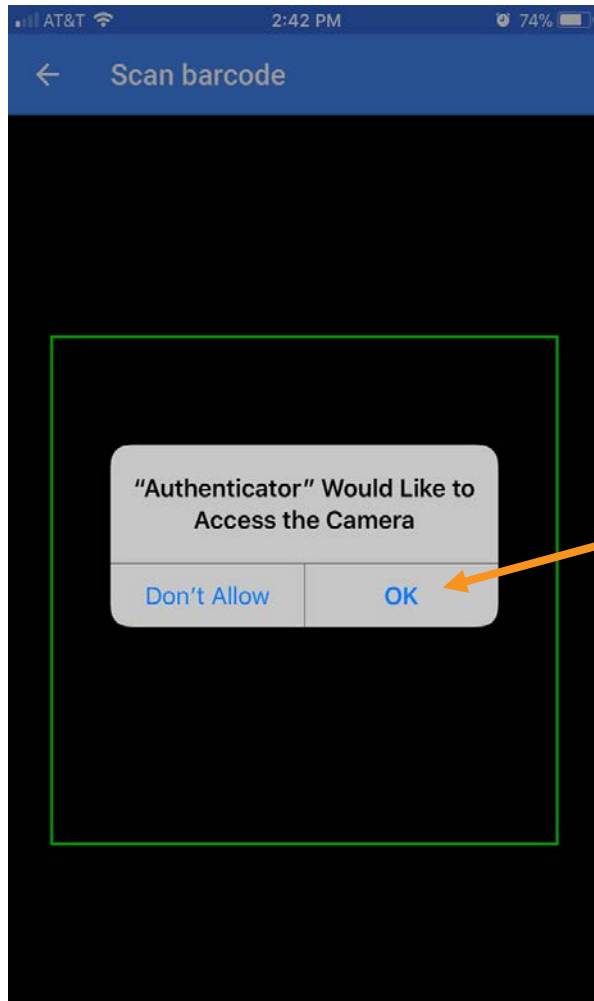
Tap on **“Begin Setup”**.

# Scan Barcode



Tap on “Scan barcode”.

# Authenticator Access to the Camera



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

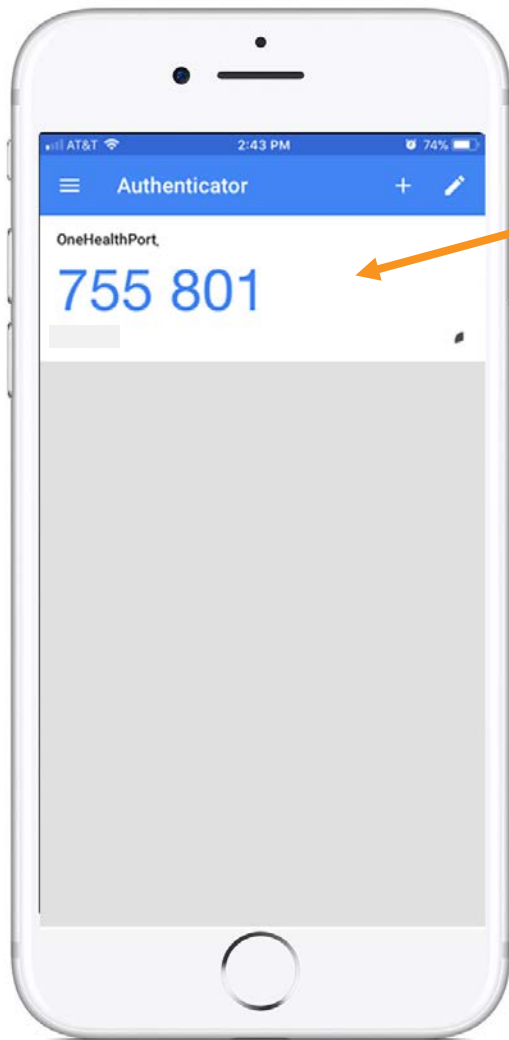
# Linking to OneHealthPort SSO Account



STEP 1: From the email (on computer), click on the link to open a QR code.

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

# Successful Link to OneHealthPort Account



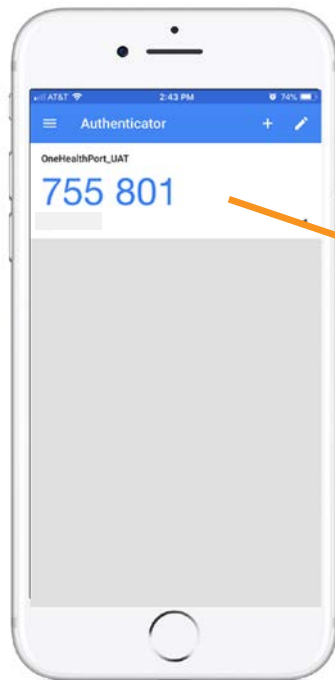
Linking is successful to the user's OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and "OneHealthPort" is above the passcode.

# Using the Passcode

# MFA Verification Using The Passcode

When access to applications require MFA, a prompt screen will appear for use in entering the passcode. Enter the passcode from the device and click on “**Verify**”.

OneHealthPort



**MULTIFACTOR AUTHENTICATION**

The application you are trying to access requires multi-factor authentication. To verify your identity, enter the code generated by the Google Authenticator application on your smartphone or tablet.

Enter Verification Code

**Verify**

[Click here to email instructions on how to download the Google Authenticator application](#)

# Successful Login to the Application

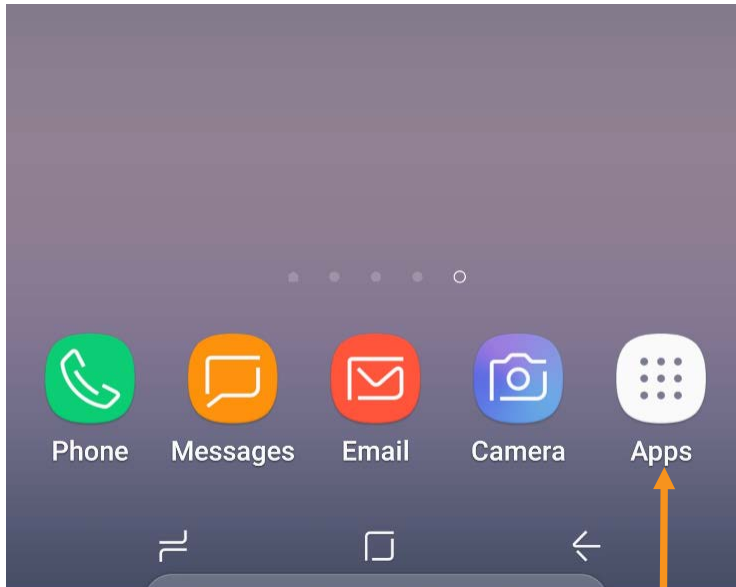
The screenshot displays the OneHealthPort Clinical Portal interface. At the top left is the logo "OneHealthPort Clinical Portal". To its right is a search bar with a plus sign, the text "Find Patients", and a magnifying glass icon. In the top right corner, there is a user profile icon labeled "jason@h..." and a "Logout" button. Below the header, the interface is divided into two main sections. On the left is the "Notifications" section, which has a blue header with a "0" badge. It includes a dropdown menu set to "10 days" and a table with columns for "Name", "Subject", and "Received". The table content is empty, with the text "There is no data available" displayed. On the right is the "Recent Patients" section, which has a blue header with a "10" badge. It contains a list of patient entries, each with a star icon and a trash can icon for actions.

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

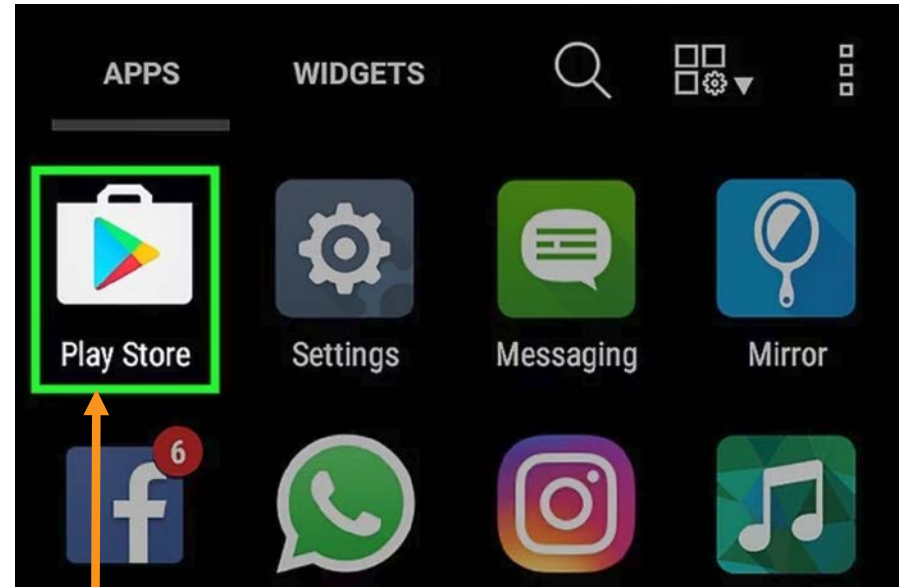


# Instructions for Android Devices

# Access the Play Store



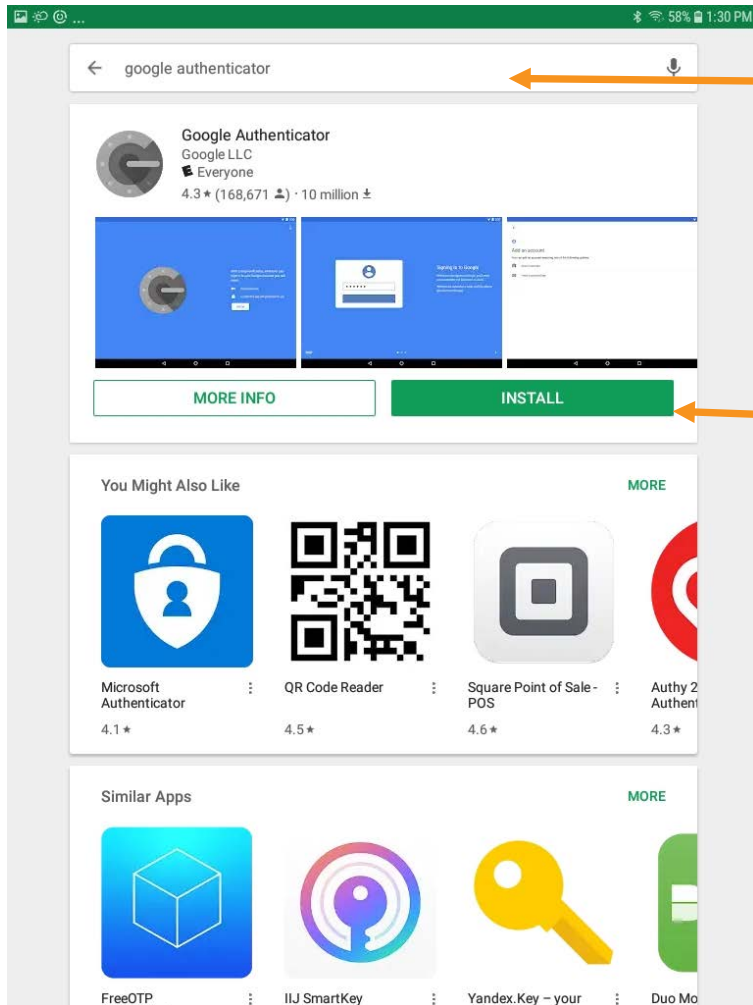
STEP 1: Tap on the “Apps” icon



STEP 2: Tap on the “Play Store” icon

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

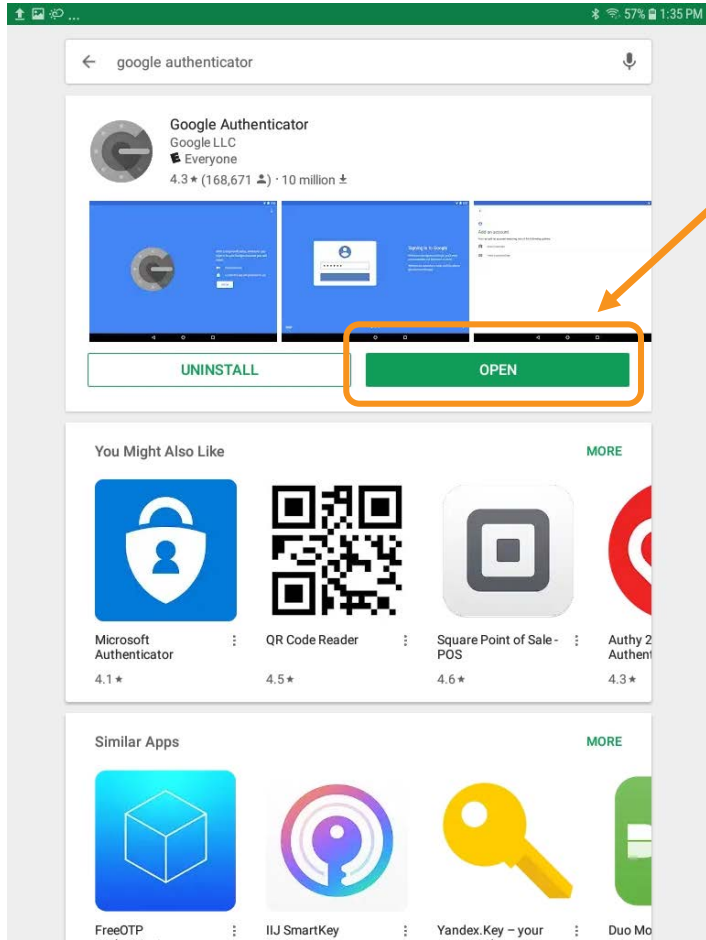
# Search for Google Authenticator



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



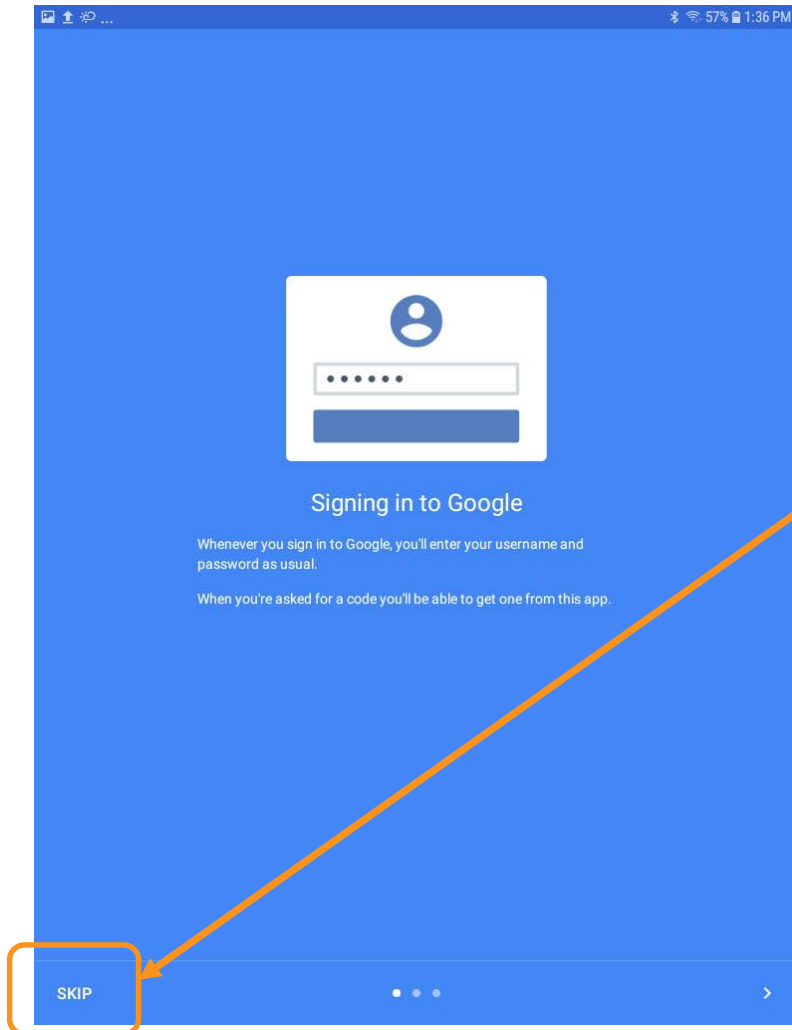
Tap on **“OPEN”** once the App has completed the download. App may also be accessed from the icon on the home screen.



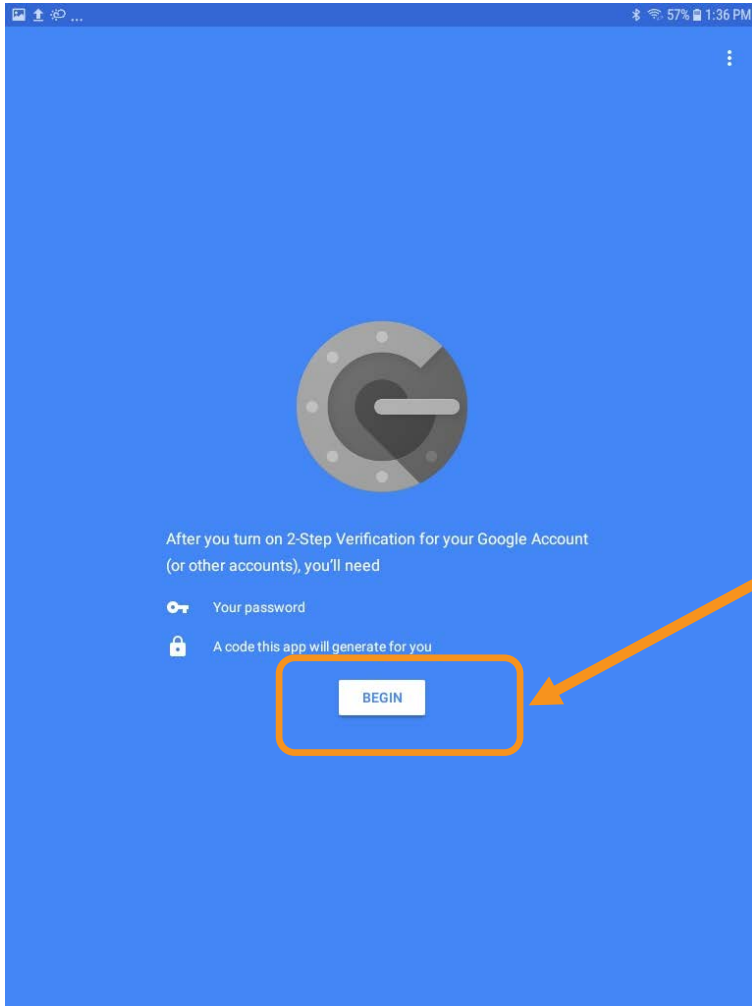
# Linking the App to the User's OneHealthPort SSO Account

# Setup

Open the Google Authenticator App. **Skip** the Signing in to Google.

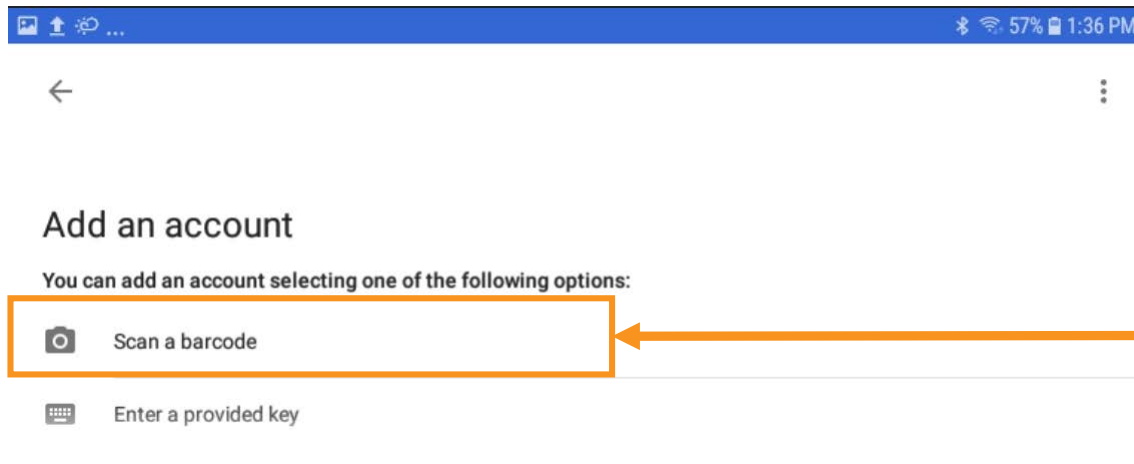


# Begin



Tap to **Begin** setup.

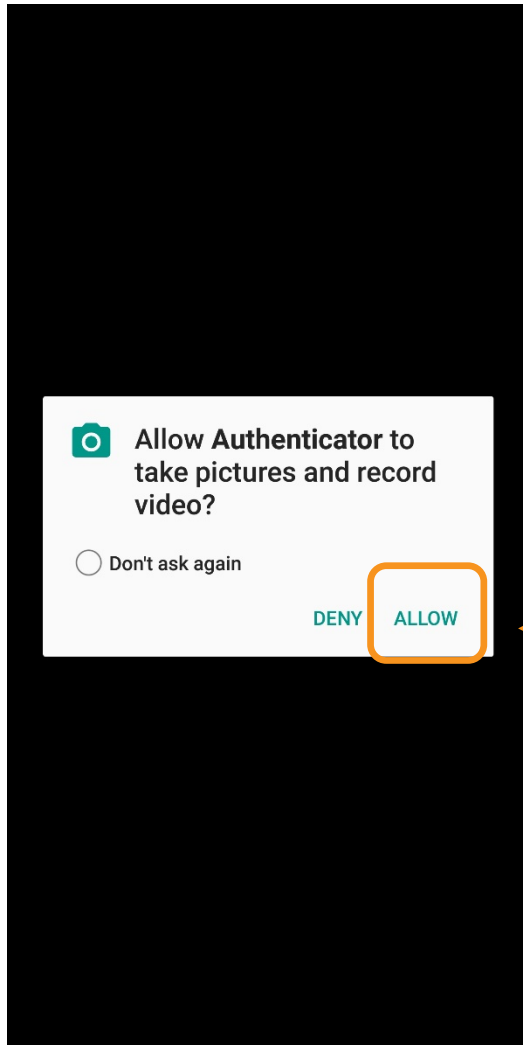
# Scan a Barcode



Tap to **Scan a barcode.**



# Authenticator Access to the Camera



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

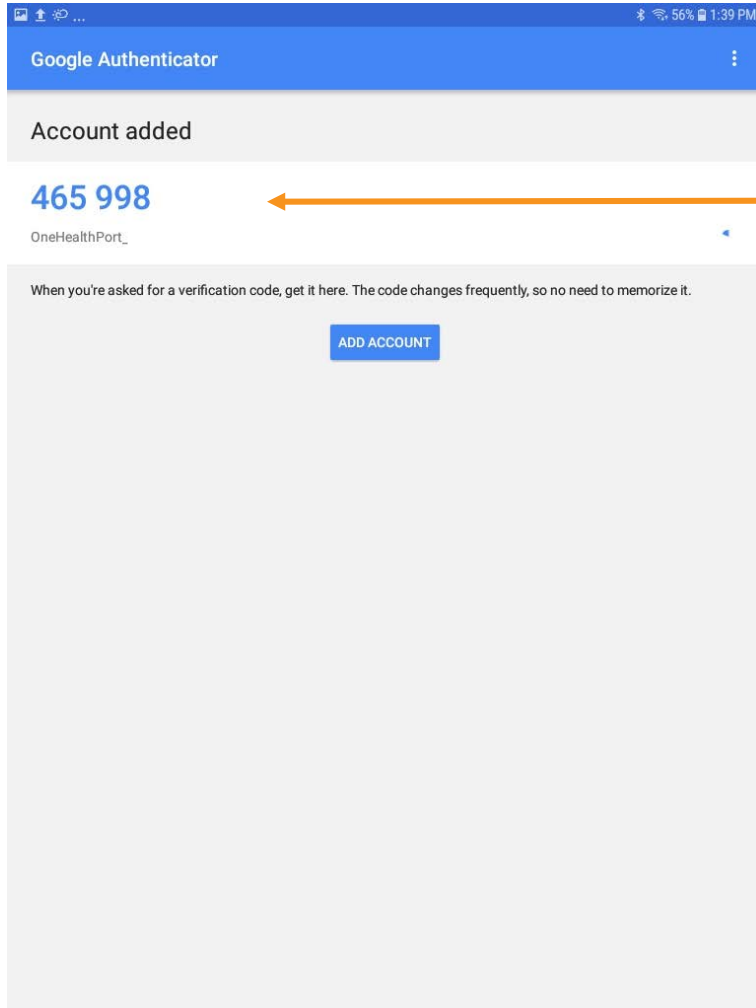
# Linking to OneHealthPort SSO Account



STEP 1: From the email (on computer), click on the link to open a QR code.

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

# Successful Link to OneHealthPort Account

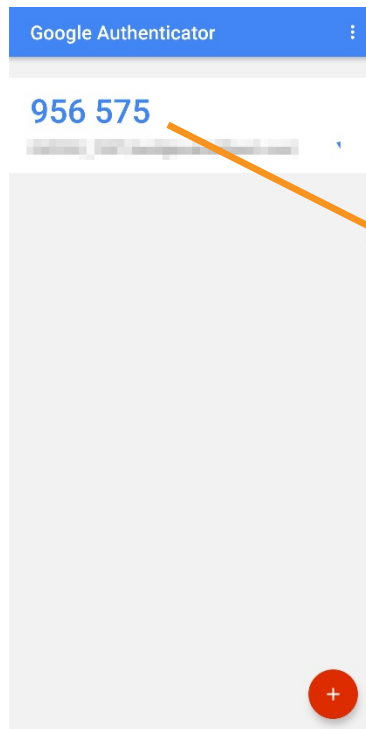


Linking is successful to the user's OneHealthPort SSO account when a periodically changing 6-digit number (passcode) displays and "OneHealthPort" is below the passcode.

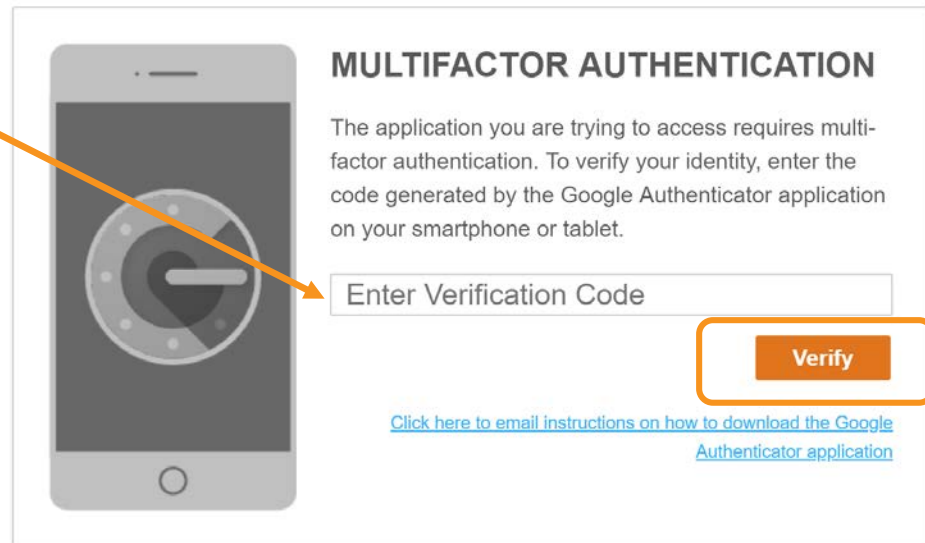
# Using the Passcode

# MFA Verification Using The Passcode

When access to applications require MFA, a prompt screen will appear for use in entering the passcode. Enter the passcode from the device and click on “Verify”.



OneHealthPort



# Successful Login to the Application

The screenshot displays the OneHealthPort Clinical Portal interface. At the top left is the logo "OneHealthPort Clinical Portal". To its right is a search bar with a plus sign, the text "Find Patients", and a magnifying glass icon. In the top right corner, there is a user profile icon labeled "jason@h..." and a "Logout" button. Below the search bar, the interface is divided into two main sections. The left section is titled "Notifications" and has a blue header with a "0" badge. It features a dropdown menu set to "10 days" and a table with columns for "Name", "Subject", and "Received". The table content is empty, with the text "There is no data available" displayed. The right section is titled "Recent Patients" and has a blue header with a "10" badge. It shows a list of patient entries, each with a star icon and a trash can icon to its right.

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