What is Multi-Factor Authentication (MFA)

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to application(s). MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyberattack.

Benefits of Multi-Factor Authentication (MFA)

The main benefit of MFA is as we have PHI and PII data, it will enhance Beacon Health Options security by requiring users to identify themselves by more than a username and password in an effort to protect data and information. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like cell phone, Desktop, other approved devices and methods means increased confidence that Beacon Health Options will stay safe from cyber criminals.

User First Time Login after MFA Implementation:

There are three options to enroll in CSA Connector MFA.

1. **Enrolling into MFA using Authy App for Desktop/Laptop**
	1. **To determine operating system in Windows environment, follow steps below**
		1. Go to start
		2. Right Click on “My PC”
		3. Click Properties
		4. Find and note down “System type” (ex “64-bit”; 32-bit) 
		5. Find and note down “Edition” (ex “Windows 10 Enterprise”)



* 1. **Download Authy App from url:** <https://authy.com/download>
		1. Select the appropriate operating system (ex “Windows 10 Enterprise”) from the options in dropdown from screenshots below





**Other Operating System Options:**

**Linux**



 **MacOS**



* 1. **Follow the screen until Icon downloads** 
	2. **Launch Authy Desktop Icon for the first time**
		1. A two (2) screen recovery information is requested in case Desktop/Laptop is lost or replaced.
			1. Enter a recovery phone number as directed below, then Click Submit



1. Enter a recovery email as directed below, then Click Submit 
2. A message “Verify your account. Select one of the following methods to verify your account”
	* + - 1. Receive WhatsApp
				2. Receive SMS message
				3. Receive Call
3. User must choose an option to proceed
4. This completes Desktop Download, now let’s move to linking Authy Desktop to CSA Connector.
5. **Access CSA Connect**
	* 1. Click Login 
		2. Enter existing Credentials (userid & password), then Click Login 
		3. User is directed to MFA setup page. Let us focus on Authy Desktop/Laptop for now.
			1. Click “Next Step” from the screenshot below



1. Note the information to link Authy Desktop/Laptop from the next screenshot
	* + - 1. Account Name: (CSA Connector-STG)
				2. Secret Key:



1. Linking Desktop to CSA Connector
	* + - 1. Launch Authy Desktop Icon 
				2. Click +(Plus Sign) from screenshot below

****

* + - * 1. Enter the Secret Key from the CSA Connector page. It is much easier to copy and paste.



1. Enter Account Name from CSA Connector page. It is much easier to copy and paste.
2. Keep selection for Token length as 6-Digits
3. Select a desired color
4. Click Save



1. A message indicating “CSA Connector App was added to Authy and a new Code will be generated every 30 seconds, and this Code can be entered into the CSA Connector App as the validation Code” will be displayed.



1. Click Next button from the CSA Connector page, and a confirmation pop-up displays, then Click “Okay” which confirms Authentication is done from the user side and user will be directed to One-Time password (OTP) page to enter Codes to login to CSA Connector.
2. Click Okay

****

1. **Enrolling into MFA using IPhone**
	1. **This is for IPhone users only**
		1. Locate and launch the App Store 
		2. Download Google Authenticator App 
		3. Access CSA Connector
			1. Click Login



* + - 1. New MFA Page – Enter Login Credentials (userid, password)
			2. Then Click Login



* + - 1. User is directed to MFA Setup Page and given 3 options, but we are focusing on IPhone only at this time.



* + - 1. On user IPhone Launch downloaded Google Authenticator 
			2. On user IPhone Google Authenticator Click +(Plus Sign) 
			3. While in Google Authenticator Click Scan a QR Code, point to App Store on CSA Connector page 
			4. User IPhone Google Authenticator displays 
			5. Click Next Step on CSA Connector
			6. Click Next on CSA Connector page to conclude IPhone setup



1. **Enrolling into MFA using Android Phone**
	1. **This is for Android users only**
		1. Locate and Launch the Play Store 
		2. Download Google Authenticator App 
		3. Access CSA Connector
			1. Click Login



* + - 1. New MFA Page – Enter Login Credentials (userid, password)
			2. Click Login



* + - 1. User is directed to MFA setup page and given three (3) options, but we are focusing on Android phone only at this time.



1. On user Android phone launch Google Authenticator 
2. On user Android Google Authenticator Click the +(Plus Sign) 
3. While in Android Google Authenticator Click on “Scan a QR Code, point scanner to CSA Connector page 
4. User Android phone Google Authenticator displays 
5. Click Next on CSA Connector
6. Click Next on CSA Connector page to conclude Android setup

**Validate One-Time-Password (OTP) Code**

1. Once user sets up App and syncs CSA Connector account to a mobile device and/or Authy desktop App, user has to enter 6-digit code from Google Authenticator for IPhone, Android or Authy Desktop App to gain access.



1. If user enters invalid code five (5) times, App will take user back to user login screen. On the 4th trial entering invalid code, a warning message will be displayed to the user indicating the next invalid attempt will log off and take user back to the login page.



1. If user stays on Multifactor Authentication screens for more than ten (10) minutes without activity, a message will be shown saying the session has timed out and user will be navigated to login screen.
2. Once user is enrolled in MFA, for subsequent logins, user will be prompted to enter six (6-digit) code that generates in Google Authenticator App on Mobile device or Authy App on desktop, depending on where user is enrolled.



1. Once valid username & password are provided, user will be navigated to the OTP screen, where user is required to enter six (6-digit) code from mobile device or Authy on the desktop.



1. User will have five (5) attempts to provide valid six (6-digit) code, upon failure to provide valid code, user will be redirected to the login page. If user is not able to login for some reason, user can reach out to the Admin counterpart to reset the password or MFA.