Multi Factor Authentication NextGen Office

Multi-Factor Authentication (MFA) is a security process that requires users to provide two or more verification factors to access their accounts. In our Text Message-based or Email based MFA, one of the factors is a unique code sent to your mobile device via Text Message or to your email which will be asked to key in while the MFA registered user logs in to their NextGen® Office account.

Instructions

- All users will be required to setup and login using MFA.
- Use the **Trust this Device** option to bypass the MFA requirement for a single device for 90 days.
- Verification code is valid for 5 minutes. Select **Back to Login** to start again.
- 3 attempts to enter a valid verification code. Select **Back to Login** to start again.
- When locked out or without access to your registered MFA Email and MFA Mobile number, please contact your practice admin to reset MFA and restart the registration process.
- Note: The back button should not be used when interacting with MFA screens

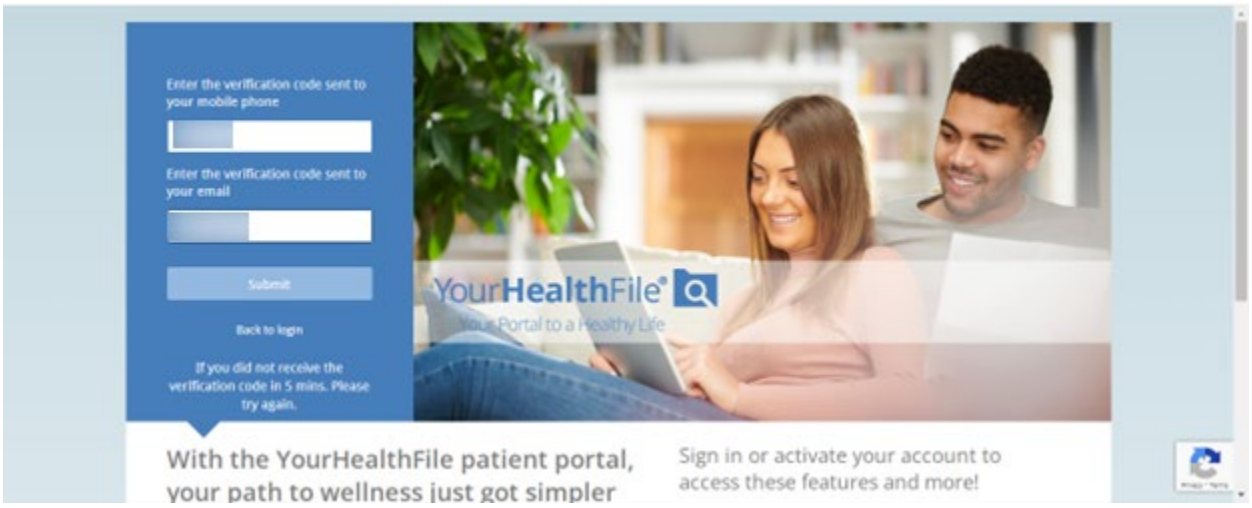
Contents

1. MFA Registration - Patient Portal

Step 1: Navigate to the NextGen Office login Screen and enter your normal User ID and Password to log on.
Step 2: Enter the MFA Mobile phone number & Email, choose the preferred Primary method and select **Submit.**

Note: Multi Factor Authentication via mobile phone is supported only in USA. Please use the email option as an alternative.
* Primary method chosen here is for the login next time onwards but while registering you may need to enter both verification codes

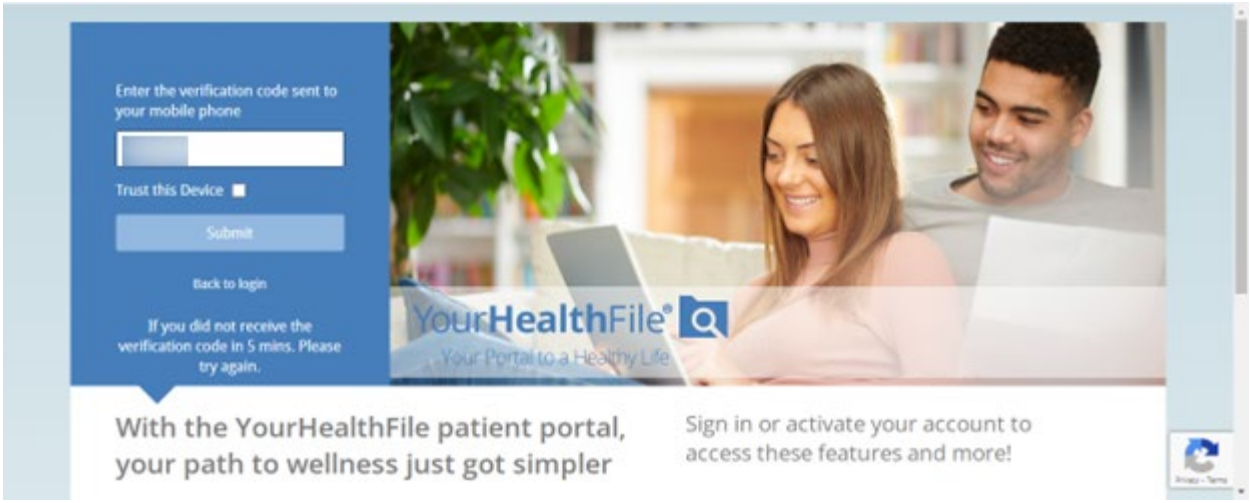
Step 3: Enter the Verification codes received on Mobile Phone and Email and select **Submit**.



Step 4: After selecting **Submit**, user will be logged into the NextGen Office Patient Portal.

2. Logging in using MFA with Primary preference - Mobile Phone

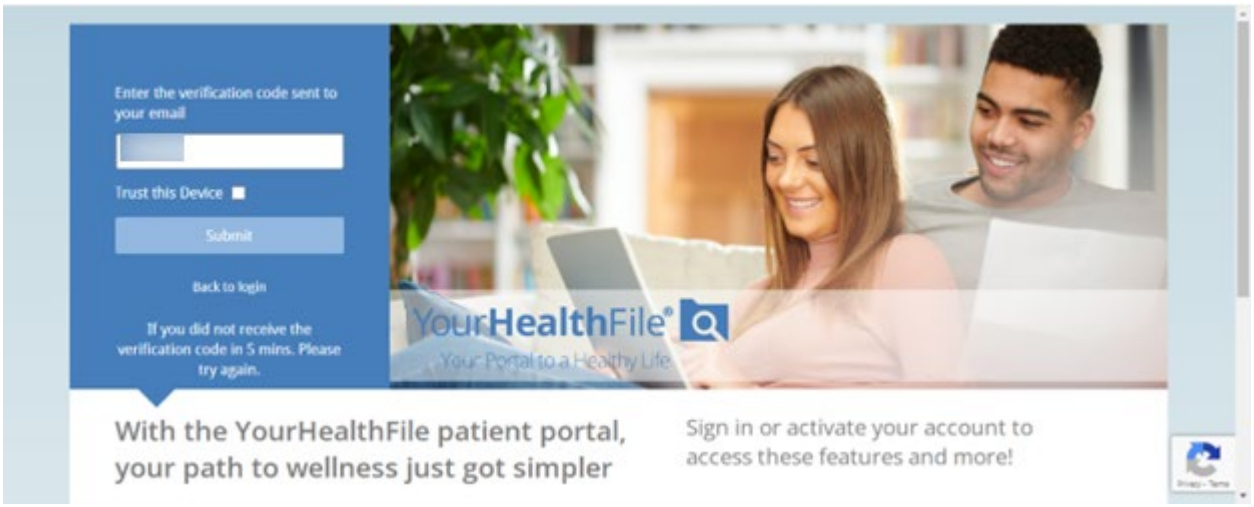
Step 1: Invoke the Login Screen & enter the credentials of MFA registered User then select **Submit.**
Step 2: Enter the verification code received on mobile phone and select **Submit.**



Step 3: After selecting **Submit**, user will be logged into the NextGen Office.

3. Logging in using MFA with Primary preference - Email

Step1: Invoke the Login Screen & enter the credentials of MFA registered user, then select **Log On**.
Step 2: Enter the verification code received on the email and select **Submit**.

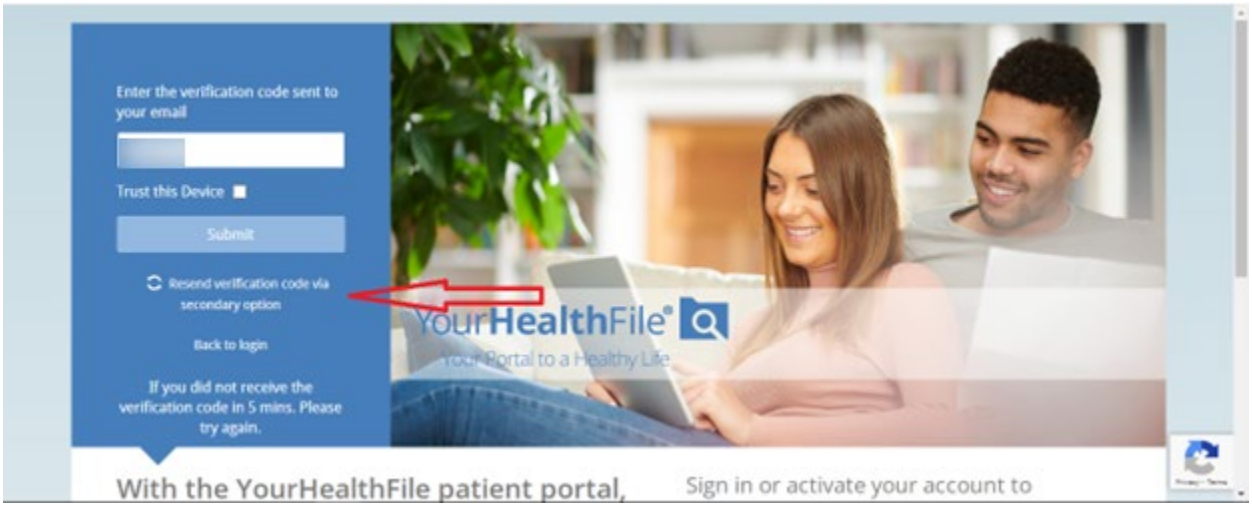


Step 3: After selecting **Submit**, user will be logged into the NextGen Office.

4. Logging in using MFA with Secondary Preference

In the event of MFA user **not being** able to receive the Verification code in their primary method, they will be able to use **Resend Verification Code Via Secondary option** and get the Verification code in secondary method and login.

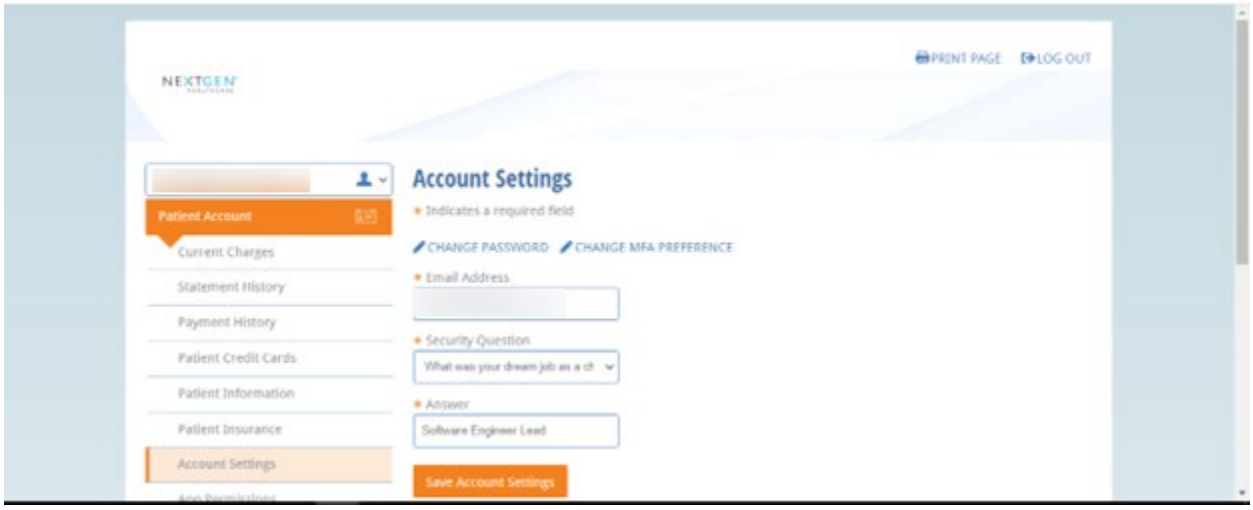
Step 1: Invoke the Login Screen & enter the credentials of MFA registered user, then select **Log On**.
Step 2: Select **Resend Verification Code Via Secondary option**.

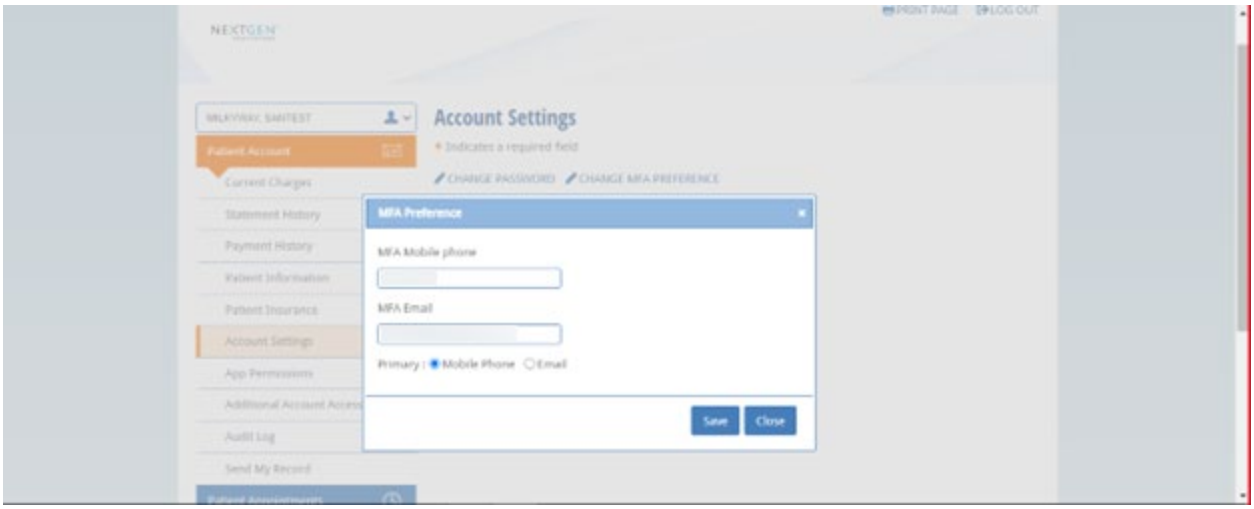


Step 3: Enter the verification code received on mobile phone and select **Submit**.
Step 4: After selecting **Submit**, user will be logged into NextGen Office.

5. Updating MFA Primary preference

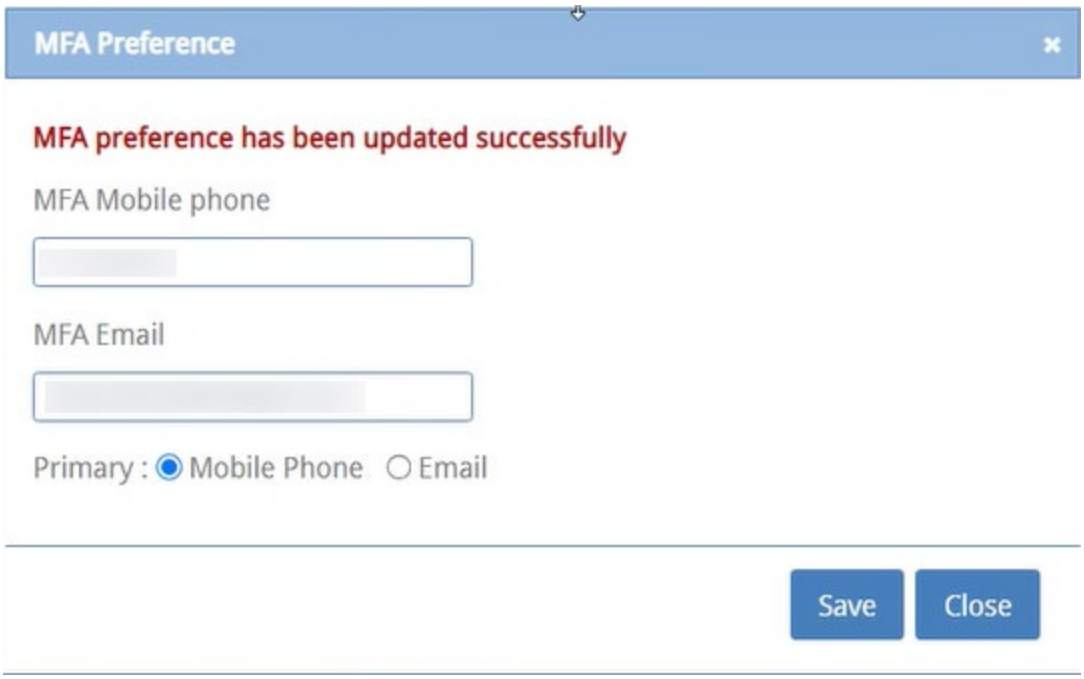
MFA Primary Preference can be updated based on the User Type. After logging to Patient Portal, select the Account Settings icon on the left corner and select **Change MFA Preference**.





Updating the Preference and MFA details

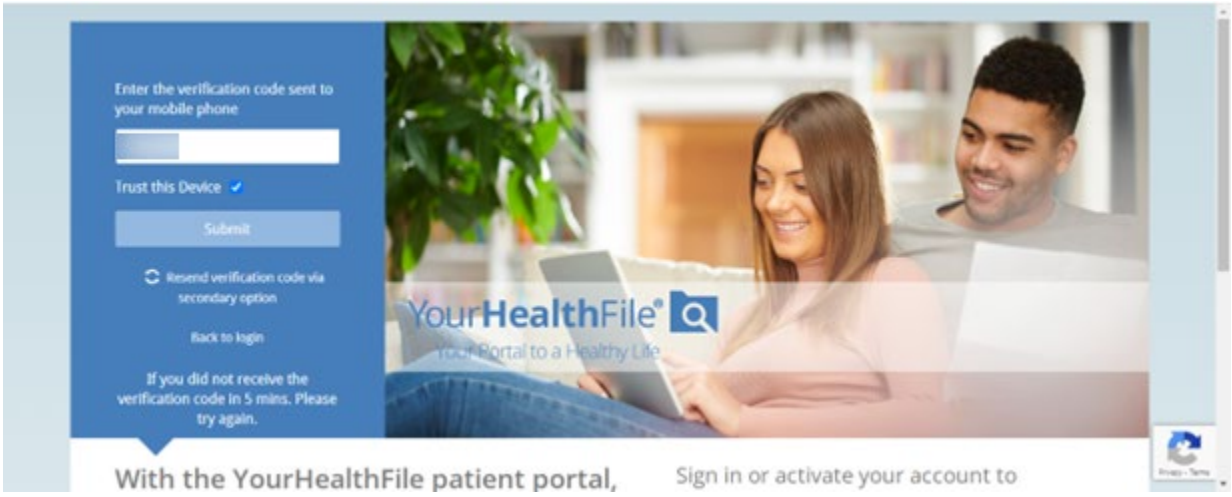
Modify the details and select **Save**.



Note: Updating the MFA Mobile Phone and MFA Email on this screen is **not** recommended and will **not** be verified by sending the verification code. Hence if you choose to edit or modify the Email or Phone Number, please enter the correct Email and Phone number to receive the Verification Codes while logging in from next time onwards.

6. Trust this Device

Step1: Invoke the NextGen Office login Screen and enter the credentials.
Step 2: Enter the verification code received on the email and select **Trust this Device** and select **Submit**.

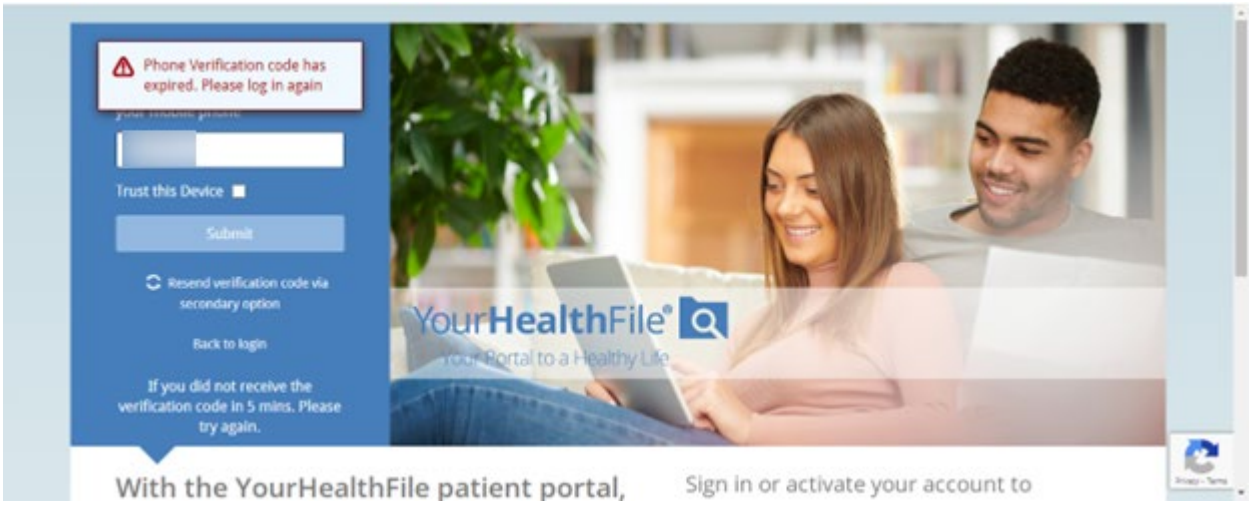


- **Trust this Device** option will help bypass the MFA if the user logs into the same device and in same browser.
- **Trust this Device** will be reset when the below conditions occur:
    - User logs into different device
    - User logs in using different browser
    - User resets the password
    - User clears the browser cache
    - User did not use MFA Verification for quite some time

Note: Only Trust a Device that is not shared, trust a device that is used the most often.

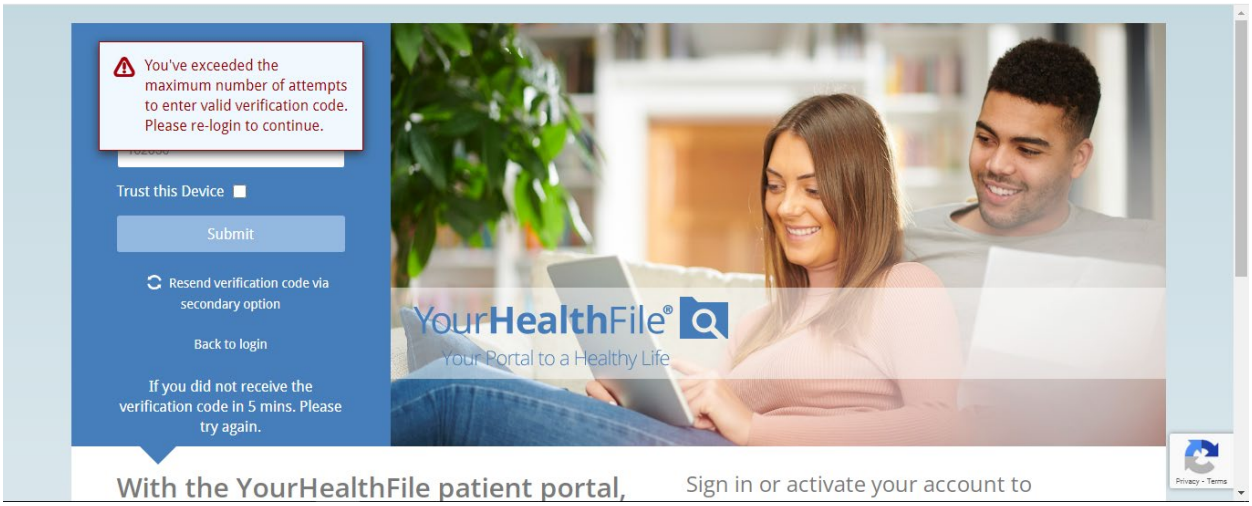
7. Verification Code expiration - When the user enters the Verification code after its expiry (5 minutes)

- When a user tries to enter the code after 5 mins, user must restart the login.



8. Exceeding the Maximum Number of Invalid attempts

- When a user enters the 3 invalid codes, user must restart the login again.



Frequently Asked Questions:

1. **What should I do if I encounter issues while registering for MFA?**
   Reach out to their practice for assistance.

2. **Whom should I contact to reset my MFA?**
   Contact the practice for assistance with resetting your MFA.

3. **How can I change my MFA preferences?**

Log in to the Patient portal, navigate to the account settings tab, and select **Change MFA preferences** to make changes.

4. **What should I do if I don't receive the code promptly via mobile phone or email?**
   There is a 5-minute window for receiving and entering the OTP. If issues persist, you should log in again.

5. **What happens if I don't select the 'Trust this device" option?**
   You will need to enter the OTP every time they log in to the patient portal.

6. **What occurs if I surpass the Maximum Number of Invalid attempts for the verification code?**
   You will need to log in again, triggering a new code.

7. **What if I lack a mobile device for MFA?**
   Select **Resend Verification Code Via Secondary option** to receive the code through an alternative method and proceed with login.