

MI Login Multi-factor Authentication [MFA]

For Providers and Advocates (third party)

Multi-Factor Authentication [MFA] is required for applications with *Protected Health Information (PHI)* or sensitive data.

The three *standard* MFA tools for MI Login are:

- **Text message** – get a text passcode on your mobile phone, type passcode into MI Login
- **Duo App Token** – download and register a free app on your mobile phone and use app to create passcode, type passcode into MI Login
- **Phone call back** – get a phone call at the number you specify, answer and press any key to log in (no ext.)

Some applications have a *Non-Standard MFA*

Email passcode– get a passcode emailed to the address you specify, type passcode into MI Login

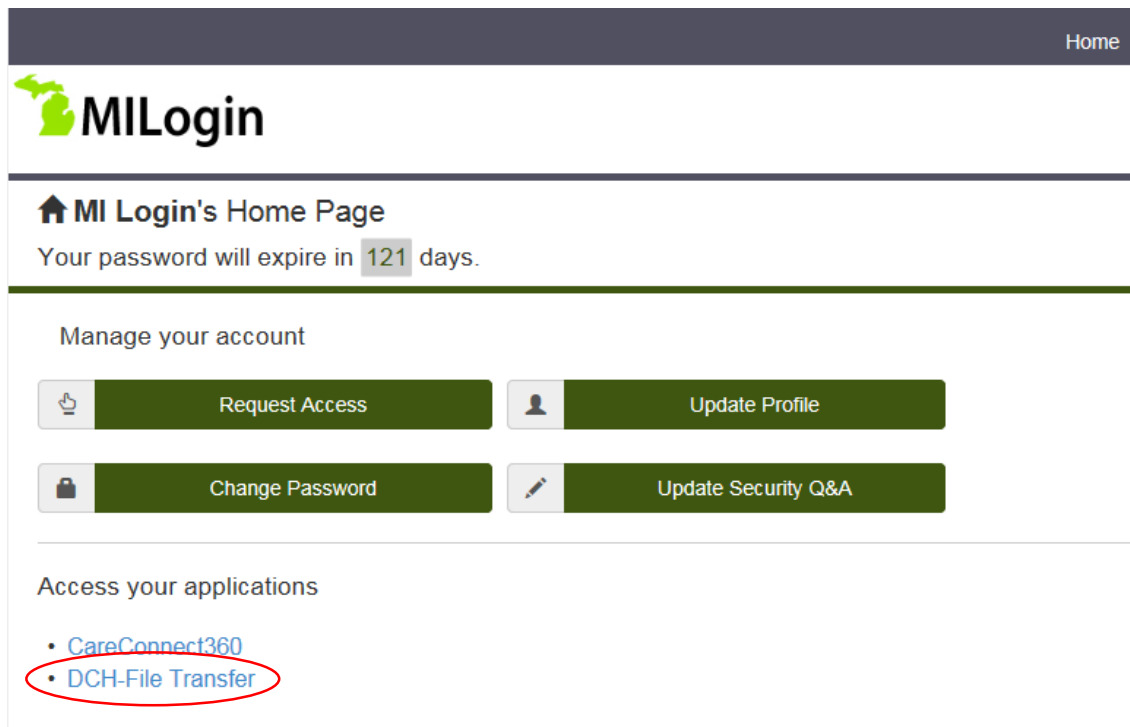
Update your MI Login Profile with correct information to complete MFA

Email address – Where you will receive **email passcode**

Work Phone Number – Where you will receive **phone call back**

Mobile Number – Where you will receive **text message**

1. Open a web browser and go to <https://milogintp.michigan.gov>; Login to MI Login with your SSO Username and Password
2. Access your application by clicking the application link



The screenshot shows the MI Login user interface. At the top right is a 'Home' link. The main header features the MI Login logo. Below the header, it says 'MI Login's Home Page' and 'Your password will expire in 121 days.' Under the heading 'Manage your account', there are four buttons: 'Request Access', 'Update Profile', 'Change Password', and 'Update Security Q&A'. Under the heading 'Access your applications', there are two links: 'CareConnect360' and 'DCH-File Transfer', with the latter circled in red.

3. If your application requires MFA you will choose your MFA option

The screenshot shows the MILogin Multifactor Authentication (MFA) selection screen. At the top right, there are links for 'Home' and 'MI.gov'. The MILogin logo is on the left. The main heading is 'MILogin Multifactor Authentication (MFA)'. Below this, a message says 'Hello MI, Select one of the following options to proceed with additional authentication required to access the application.' There are four options, each with a green button and a description: 'Text Message' (passcode via text to xxx-xxx-7614), 'Duo App Token' (passcode via Duo Mobile app to xxx-xxx-7614), 'Phone Call Back' (call on work phone xxx-xxx-7614), and 'Email' (passcode in email m*****@gmail.com). A blue callout box on the right says 'Not all applications have email option. If you do not see email, it is not available for your application' with a line pointing to the 'Email' option.

4. Type passcode into MILogin and Click Submit to access your application

The screenshot shows the MILogin Multifactor Authentication (MFA) passcode entry screen. At the top right, there are links for 'Home' and 'MI.gov'. The MILogin logo is on the left. The main heading is 'MILogin Multifactor Authentication (MFA)'. Below this, a red asterisk indicates a required field. There is a text input field for the passcode. Below the input field are two buttons: 'Submit' (green) and 'Back' (white). A blue callout box on the right says 'Type passcode Click Submit' with a line pointing to the input field. At the bottom, there is a note: 'For a different option / to regenerate a passcode, click on Back button'.

Reminder: Your MFA passcode is active for 24 hours. You may log in multiple times within the 24 hour period, using same device and web browser, without additional MFA

- Your MFA passcode will apply to all of the applications in your profile, even if you use different methods of MFA for different applications
- If you change browsers, devices or location though, you may have to complete MFA again
- If you are sharing a workstation, each person will need to complete MFA for their MILogin application(s)