MILogin 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 MILogin are:

- **Text message** – get a text passcode on your mobile phone, type passcode into MILogin
- **Duo App Token** – download and register a free app on your mobile phone and use app to create passcode, type passcode into MILogin
- **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 MILogin

Update your MILogin Profile with correct information to complete MFA

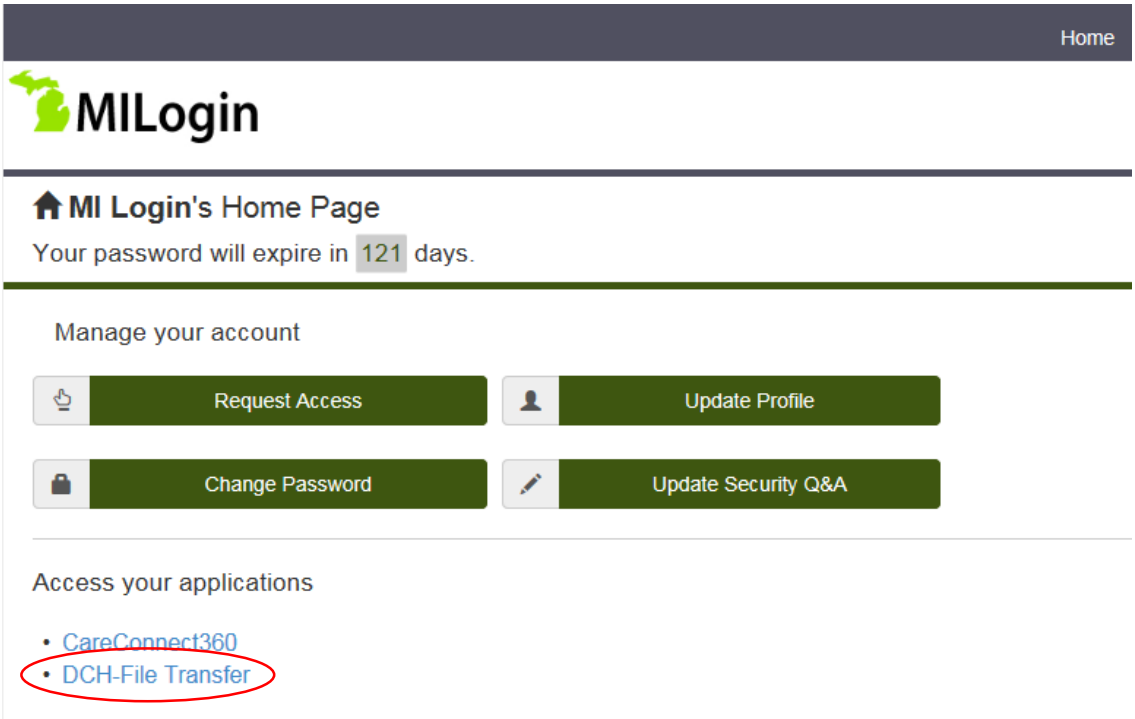
Email address – Where you will receive **email passcode**

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

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

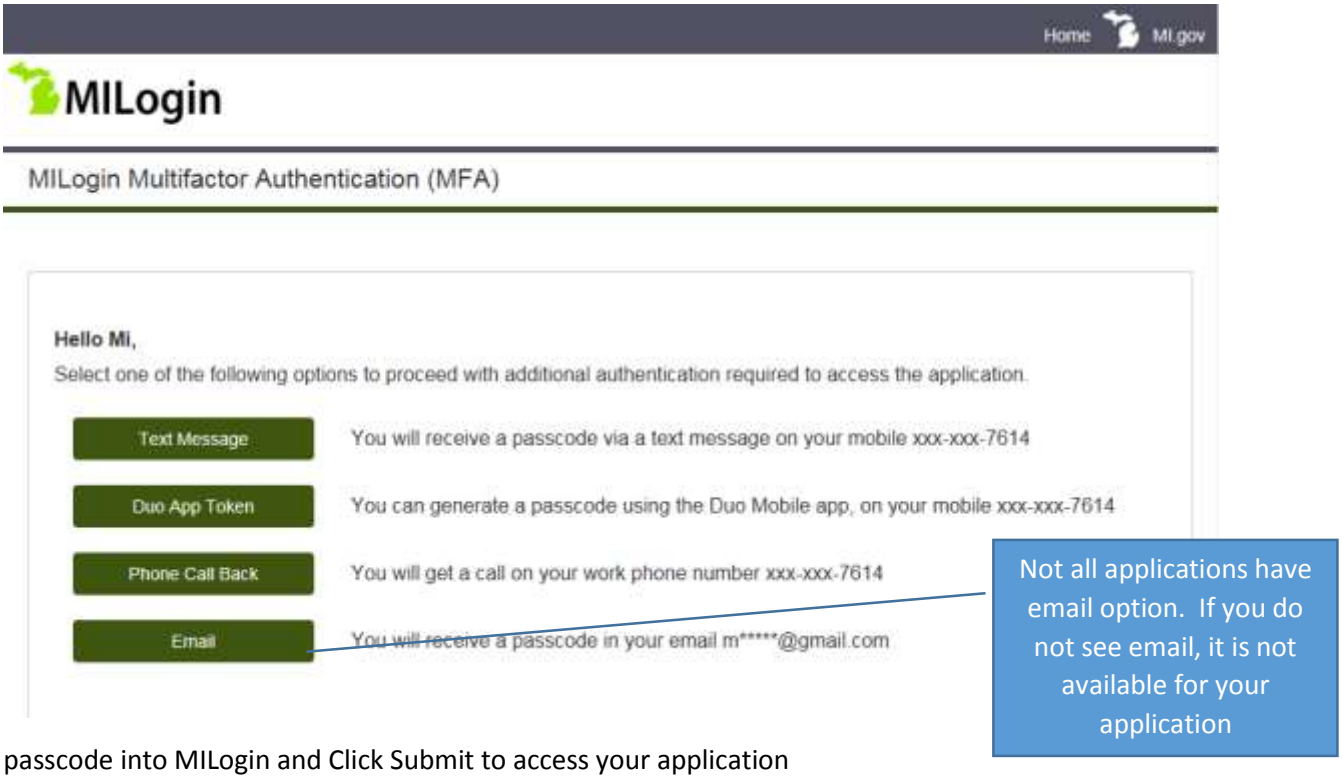
1. Open a web browser and go to https://milogintp.michigan.gov; Login to MILogin with your SSO Username and Password

2. Access your application by clicking the application link

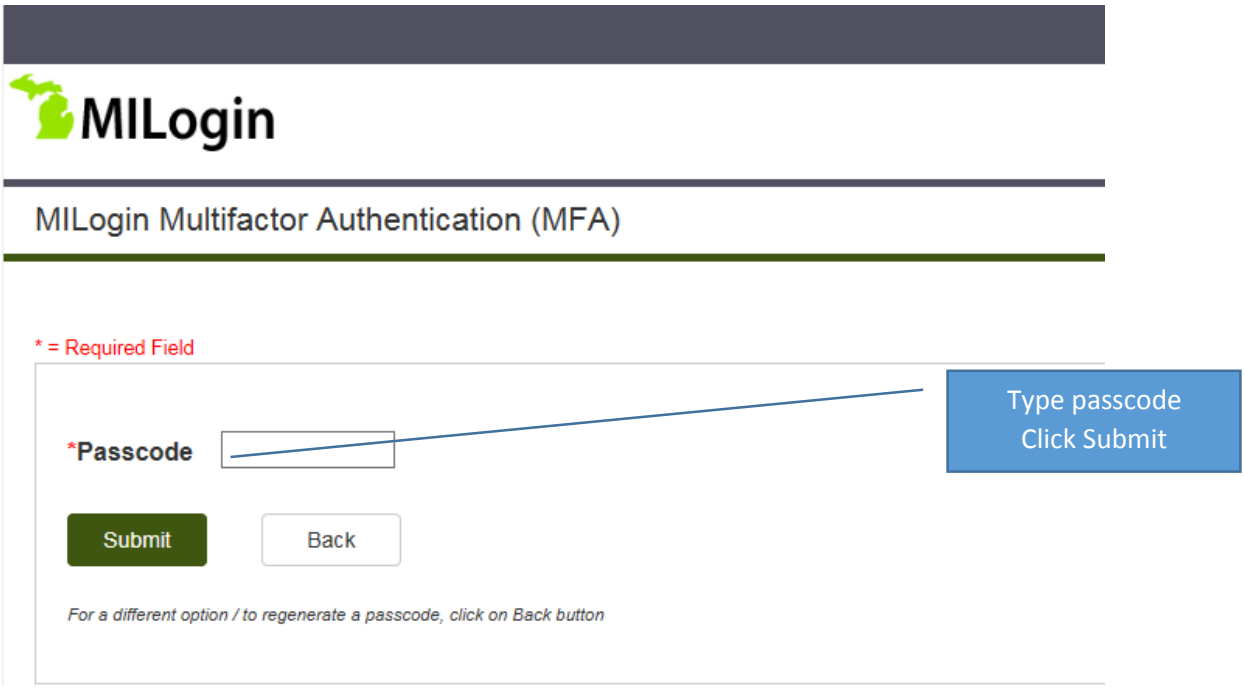


Revision Date: May 25, 2016

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



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



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)