SETTING UP MULTI-FACTOR AUTHENTICATION (MFA)

MI Provider Portal & InteleConnect

Secure Access for Referring Providers

TRA Medical Imaging and Diagnostic Imaging Northwest offer two secure, web-based portals to support referring providers with convenient access to patient imaging and referrals. The MI Provider Portal streamlines the referral process, allowing providers to submit electronic imaging referrals quickly and securely, while InteleConnect provides web-based access to patient imaging and reports from anywhere, at any time.

New Security Feature – Multi-Factor Authentication (MFA)

Beginning July 22, 2025, Multi-Factor Authentication **(**MFA**)** will be required to access both the MI Provider Portal and InteleConnect. This added layer of security helps protect patient information and aligns with industry best practices for safeguarding electronic health data.

Setting Up Multi-Factor Authentication

If multi-factor authentication is enabled in your user account, the first time that you attempt to log in after the privilege is enabled, you will be prompted to set up a multi-factor authentication app for use with your the MI Provider Portal or InteleConnect application.

Multi-factor authentication adds a layer of security to your account by requiring a second step of verification when you log in. In addition to your password, you will also need to enter a verification code that is generated by the authentication app.

You can install and set up a multi-factor authentication app on your mobile device (Android or iOS), or on your desktop (Windows/MacOS). If you already have an authentication app installed on a device, you can create a new account in the app for use with your portal application.

To set up multi-factor authentication:

1. Log in to your portal application (MI Provider Portal or InteleConnect).
   The two-factor authentication setup dialog appears:

2. Do one of the following:
    - **If you do not have an authentication app installed on a device**, do the following:
        - Install a two-factor authentication app on your mobile or desktop device. You can install one of the authentication apps provided in the link on the two-factor authentication setup dialog, or another app of your choice. If you want to install an authentication app on your mobile device, you can install the app from your mobile app store.
        - In your authentication app, add a new account.
    - **If you already have an authentication app installed on a device**, access the authentication app, and then add a new account.
3. In the authentication app, scan the QR code that appears in the two-factor authentication setup dialog, or enter the key.

   The authentication app creates a new account for use with your TRA/DINW portal application.

4. In the two-factor authentication setup dialog, enter the verification code that appears in the authentication app.

5. Press **Verify Code**.

   Two-factor authentication setup is complete.