TronsHealth
5900 Balcones Drive STE 11857
Austin Texas 78731
Fax: (512) 485-2866

TronsHealth

§170.315(d)(13) Multi-factor authentication

PREPARED FOR

ONC-ACB
ONC Certification

PREPARED DATE
Aug 16, 2024

Contents

1. Overview

Multi-factor authentication (MFA) is a security feature that requires users to verify their identity in multiple ways before they can access a system. This adds an extra layer of protection for electronic health information. For example, even if a user's password is stolen, MFA can prevent unauthorized access by requiring another form of verification, like a code sent to their phone. The ONC requires MFA under §170.315(d)(13) as part of its certification criteria to ensure that electronic health records (EHR) systems are secure, and that sensitive health information is protected.

2. Key Requirements

- The criterion does not require health IT to include multi-factor authentication or mandate its implementation for any specific use case. Instead, health IT developers must attest "yes" or "no" to whether their Health IT Module supports multi-factor authentication. There are no requirements for healthcare providers to use these capabilities, even if they are available in their products.

- If developers attest "yes," they must submit a report detailing the supported use cases to the ONC Authorized Certification Body (ONC-ACB). This report can be in hard copy or an acceptable electronic format. Additionally, developers must provide a hyperlink to any required or optional documentation for public access on the ONC Certified Health IT Product List (CHPL).

2.1 Attesting "Yes"

- If a health IT developer attests "yes" to supporting multi-factor authentication, they must describe the supported use cases. For example, they could state that the Health IT Module supports MFA for remote access by clinical users, specifying the relevant user roles.
- Detailed technical information is not required; a brief, high-level summary of the supported uses is sufficient. If a new MFA use case is added, it must adhere to the "yes" attestation requirements and be included in the quarterly CHPL reporting as outlined in § 170.523(m).

2.2 Attesting "No"

- Health IT developers are allowed, but not required, to provide a reason for attesting "no" to supporting multi-factor authentication.
- For example, a developer might explain that the Health IT Module doesn't support MFA because it is used for system-to-system public health reporting, where MFA is not applicable.

3. Importance

Multi-factor authentication (MFA) is critical in safeguarding sensitive health information. As healthcare data is a prime target for cyberattacks, MFA provides an additional layer of defense beyond simple password protection. By requiring multiple forms of verification, MFA significantly reduces the risk of unauthorized access, thereby protecting patient privacy and maintaining the integrity of the EHR system.

4. Implementation

TronsHealth EHR has implemented MFA in compliance with §170.315(d)(13) to ensure the security of electronic health information. It provides robust security while maintaining ease of use, helping healthcare organizations protect sensitive patient information effectively.

- Open the web browser and go to the EHR TronsHealth website.
- The user successfully signs in, the dashboard will appear. See Fig 5

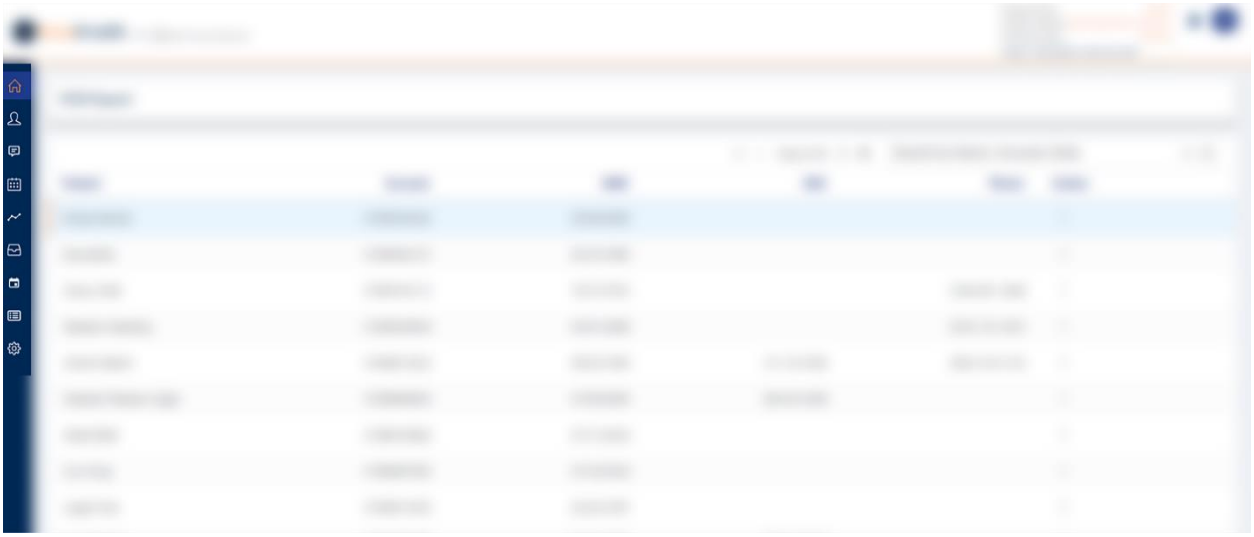

Fig 5

- Hover to the left of the blue bar to navigate the system. See Fig 5.1

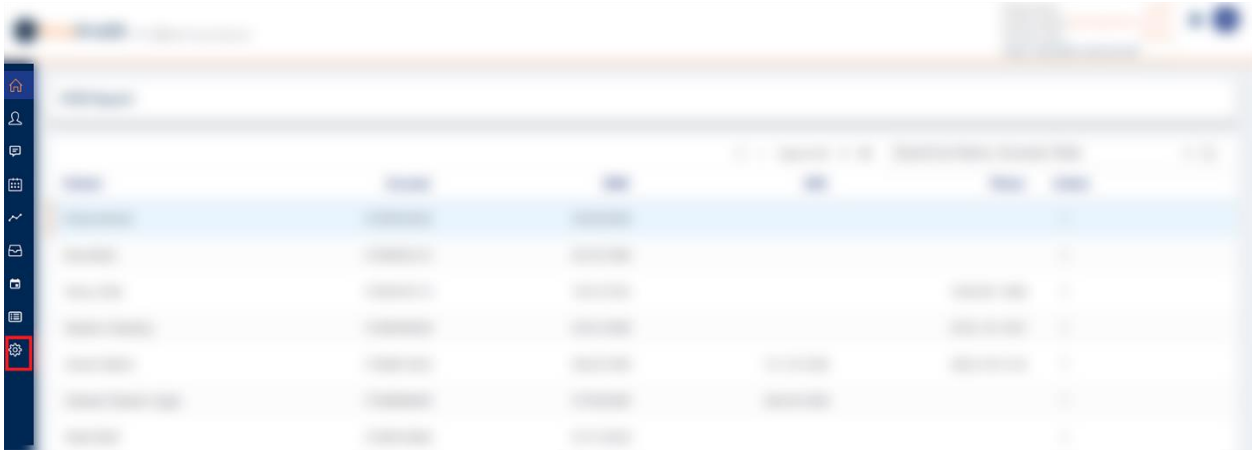

Fig 5.1

- After clicking on the setting icon, the side menu appears. See Fig 5.2

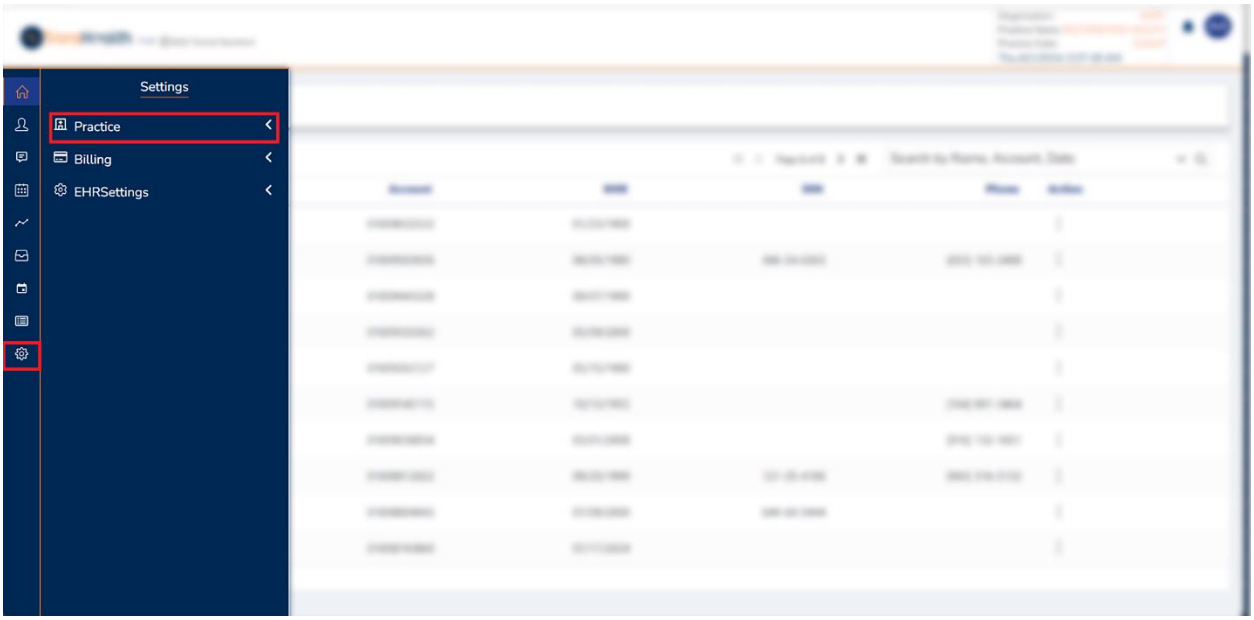

Fig 5.2

- The user must click on Practice to explore more options; a drop-down menu appears when clicking the practice button.
- Now, the user clicks on the user management. See Fig 5.3

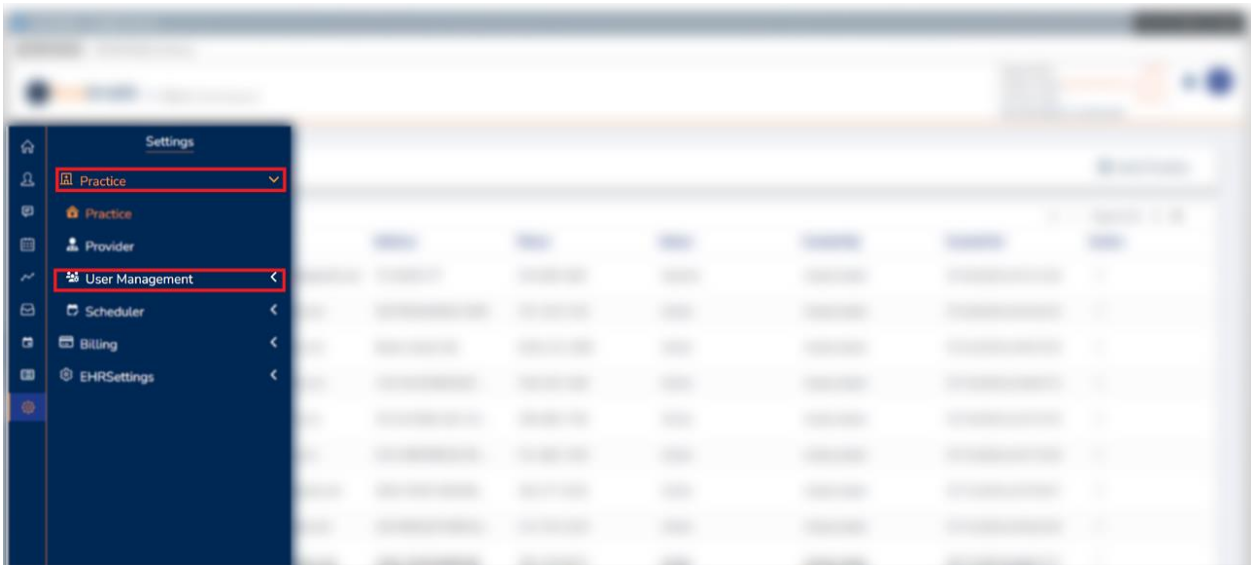

Fig 5.3

- After clicking on user management, the user clicks on the practice user to add a test user. See Fig 5.4

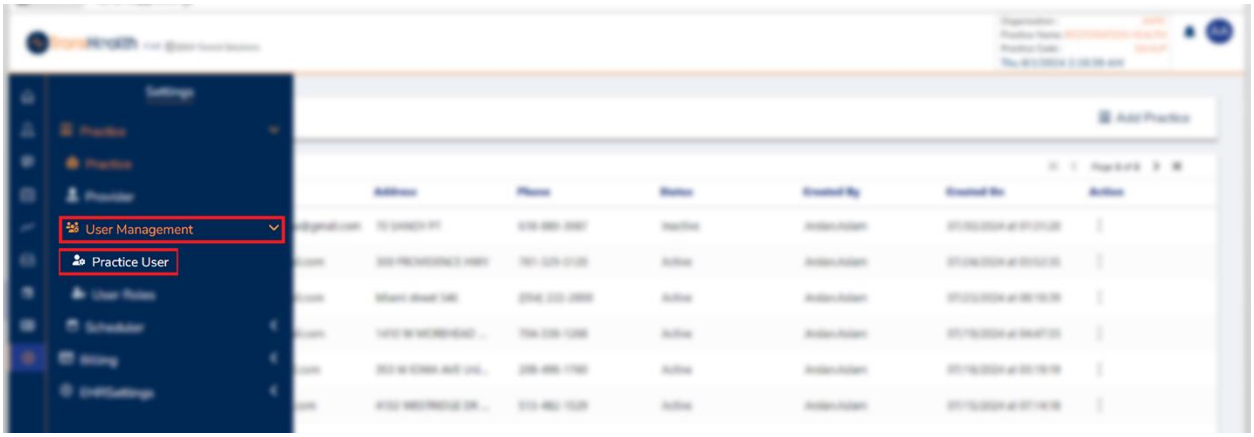

Fig 5.4

- The new practice user screen will appear. The logged in user adds a new user. See Fig 5.5

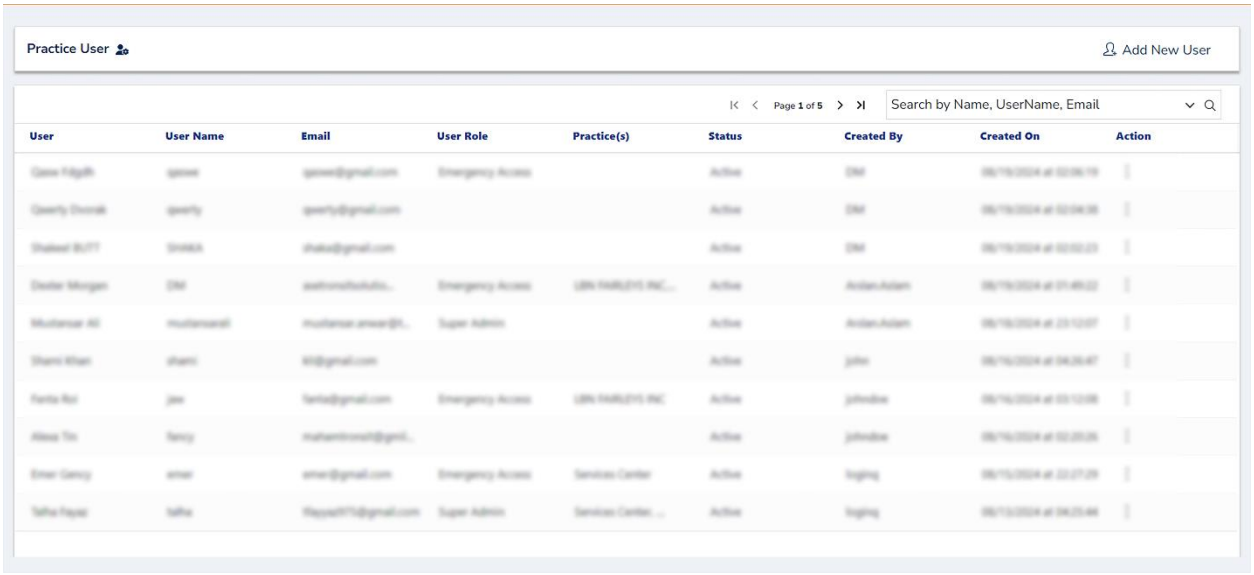

Fig 5.5

- The logged in user fills in all the required fields to create a test user.
- After fulfilling all the required fields, the logged in user which has permissions to add or update any user enables Email MFA and saves the information. See Fig 5.6
- Mutli-factor authentication will only come into effect for users with at least a valid email address or phone number in their profiles.

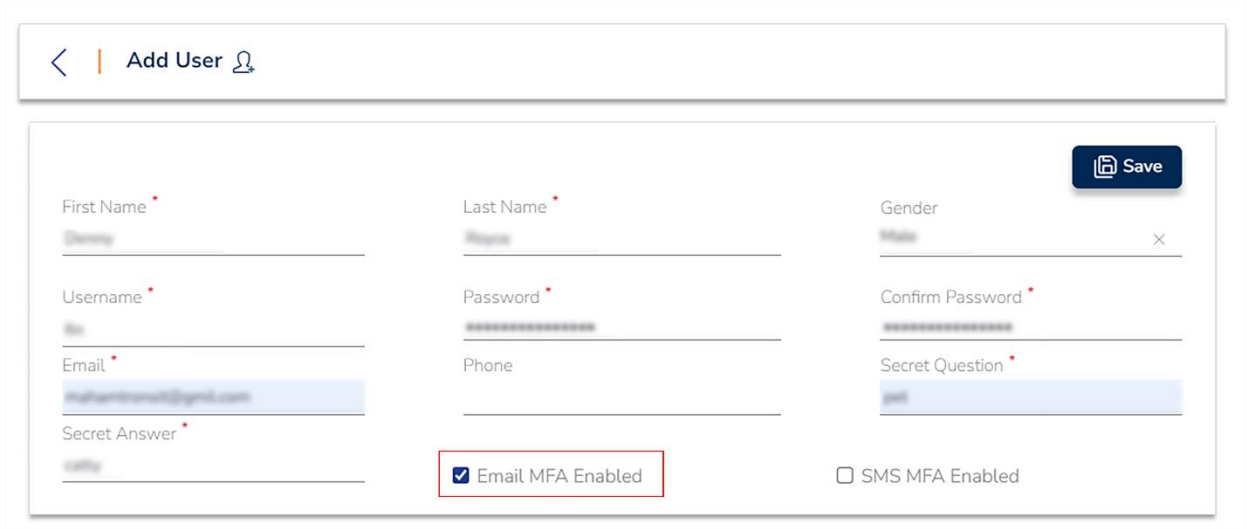

Fig 5.6

- The user receives the OTP from TronsHealth on his/her active email address.
- The OTP verification screen appears when the test user logs in with the assigned credentials. See Fig 5.8
- Upon successful verification of the OTP, the user will be redirected to the application's home page

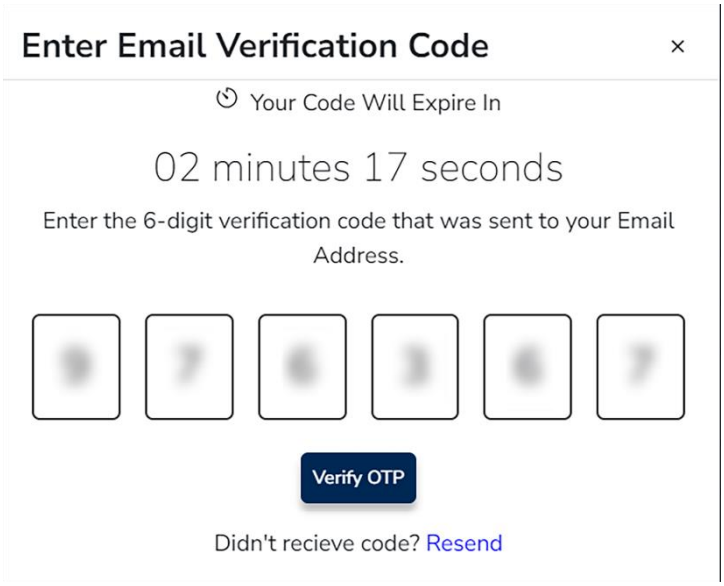

Fig 5.8

- The user must enter the received OTP in the application before expiration, i.e. in 3 minutes.

NOTE: The admin can enable or disable MFA for the user and choose to activate SMS, email, or both for authentication.