Compliance with ONC Certification Criteria §170.315(d)(13) – Multi-Factor Authentication

Product Name: OneConnect
Health IT Developer: MedOne Healthcare Partners
ONC Certification Criterion: 45 CFR §170.315(d)(13) – Multi-Factor Authentication
ONC Certification ID: 15.04.04.3182.Onec.00.00.1.231227

Overview

The Multi-Factor Authentication (MFA) certification criterion identifies whether a certified Health IT Module supports the use of multiple authentication factors to verify a user's identity when accessing the system. MedOne Healthcare Partners attests "Yes" to supporting the 45 CFR §170.315(d)(13) Multi-Factor Authentication certification criterion for the OneConnect Health IT Module. MFA provides an additional layer of security by requiring users to verify their identity using more than one authentication factor before access to the system is granted. Consistent with ASTP/ONC guidance, this documentation provides a high-level description of multi-factor authentication capabilities supported by the OneConnect platform.

Supported Use Cases & User Roles

The OneConnect platform supports multi-factor authentication for user identity verification in scenarios that may include:

- User login to the OneConnect application
- Remote access to the OneConnect application
- Login attempts from new or unrecognized devices

MFA applies to authorized clinical staff and administrative users accessing the OneConnect platform, particularly when accessing the system remotely or in situations where enhanced identity verification is required. These workflows help ensure that access to the system is limited to authorized and verified users.

Authentication Process

MFA requires users to complete an additional verification step after entering their login credentials before access to the OneConnect system is granted. The authentication workflow includes the following steps:

- **User Credential Authentication**
  The user enters their username and password to initiate the login process.
- **Additional Verification Step**
  After valid credentials are entered, the user completes a second verification step using an authenticator application on a registered mobile device. The user receives a sign-in verification request and confirms the login using a one-time verification code.