Multi-Factor Authentication

170.315(d)(13)

Yes, the product supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When sending a controlled prescription through the RXNT web version, a two-factor authentication screen will appear prompting credentialed physicians to enter their RXNT login password and approve a verification via push notification through the ID.me Authenticator app. When prescribing a controlled substance with the RXNT mobile apps, a two-factor authentication screen will appear prompting credentialed physicians to enter their RXNT login password and verify their identity using 1Kosmos LiveID.

In addition, users are required to log in to RXNT via a login screen powered by FusionAuth to access their account. After entering their username and password, users are prompted to complete MFA by authenticator app. Users can use an authenticator app of their preference to complete MFA. The code provided by the authenticator app must then be entered into the RXNT login screen to access the system.

The RXNT SSO follows standard OAuth protocols and allows application login and MFA to be managed by Microsoft, Google, and Okta. EPCS support is enabled for Microsoft and Okta. ID.me authenticator app is required for browser based EPCS and 1Kosmos Live ID is required for mobile EPCS.

MFA is also required when patients access the patient portal; they must verify their identity with a one-time code sent via text message or email during the login process.