Supported Use Cases Multi-factor Authentication

myAvatar; myEvolv; myUnity; myUnity Senior Living; myHealthPointe; GEHRIMED

myAvatar™ electronic health record (EHR), myEvolv™ EHR, myUnity™ EHR, myUnity Senior Living™ EHR, myHealthPointe™ EHR, and GEHRIMED EHR applications support multi-factor authentication (MFA) using industry standards in alignment with the Office of the National Coordinator for Health IT's (ONC) multi-factor authentication criterion at 45 CFR 170.315(d)(13) for logging into the application and accessing protected patient information.

Netsmart Identity and Access Management (IAM) solution supports both Centralized and Federated MFA models for identity and access management.

Centralized Netsmart Identity and Access Management
In the Centralized Model, the client provides the end-user identities. Netsmart provides the Identity Provider (IdP) which delivers MFA and single sign-on (SSO) for the client's end user using OpenID Connect internally between Netsmart IAM and the Netsmart solutions.

Centralized Netsmart IAM provides the following supported MFA methods:

- Software one-time passcode (OTP) (e.g., Okta Verify, Google Authenticator)
- Legacy MFA methods currently supported:
  - SMS – Leverages text messaging to send the user a one-time passcode
  - Voice – A call is placed to the user's phone
  - Email – Authentication code is emailed to the user

Federated Netsmart Identity and Access Management
In the Federated model, Netsmart integrates with the client organization provided SAML 2.0 compliant IdP (e.g., Okta, Duo, Azure AD, etc.). The client's IdP is responsible for providing MFA and single sign-on for the client's end-user. Upon authenticating the user within the client provided IdP, an exchange of tokens is performed using SAML 2.0 protocol over TLS encrypted redirects between Netsmart IAM and the client IdP, and using OpenID Connect internally between Netsmart IAM and Netsmart solutions.

In the Federated NIAM model, the client organization provided IdP is responsible for providing the MFA methods as part of its authentication of the end-user identity.

TheraOffice

TheraOffice™ electronic health record (EHR) supports multi-factor authentication (MFA) using industry standards in alignment with the Office of the National Coordinator for Health IT's (ONC) multi-factor authentication criterion at 45 CFR 170.315(d)(13) for logging into the application and accessing protected patient information.

TheraOffice's identity access and management supports a Centralized MFA models for identity and access management.

In the Centralized MFA model, the client provides the end-user identities. TheraOffice provides the Identity Provider (IdP) through a 3rd party IdP Auth0, which delivers MFA for the client's end user using OpenID Connect. TheraOffice's IdP provides the following supported MFA methods:

- Software one-time passcode (OTP) (e.g., Okta Verify, Google Authenticator)

OrderConnect

OrderConnect supports multi-factor authentication (MFA) using industry standards in alignment with the Office of the National Coordinator for Health IT's (ONC) Multi-factor authentication criterion at 45 CFR 170.315(d)(13) for the ePrescribing Controlled Substances (EPCS) workflow.

Netsmart partners with Verizon and leverages their Verizon Identity (VID) cloud-based-identity-as-a-service solution that includes identity-proofing, credential issuance and strong authentication.