Multi-Factor Authentication Use Cases

Required documentation for ONC Health IT Certification § 170.315(d)(13)

Document	Multi-Factor Authentication Use Cases
Version	1.0
Date	June 10, 2026
Classification	Public (CHPL listing)
Prepared By	MindWise Health Engineering
Applicable Criterion	170.315(d)(13) Multi-Factor Authentication

1. Purpose

Per ONC § 170.315(d)(13), this document describes the multi-factor authentication (MFA) capabilities provided by MindWise Health and the specific use cases for which MFA is available or required. MindWise Health is capable of authenticating the user's identity through multiple elements using industry-recognized standards as required by the criterion.

2. Supported MFA Methods

Method	Standard	Use
TOTP (Time-Based One-Time Password)	RFC 6238 (TOTP) / RFC 4226 (HOTP)	Primary MFA factor. Compatible with Google Authenticator, Microsoft Authenticator, Authy, 1Password, Bitwarden.
WebAuthn / FIDO2 Security Keys	W3C Web Authentication API; FIDO2 CTAP	Hardware security key (YubiKey, Titan, etc.) or platform authenticator (Touch ID, Windows Hello).
Recovery Codes	One-time use codes generated at enrollment	Backup method when primary factor is unavailable. Ten codes issued per user; each consumed on use.

3. Authentication Flows

3.1 Clinical Provider Login

Users with the **PHYSICIAN** or **CAREPROVIDER** role accessing protected health information through the MindWise Health platform are subject to the following MFA flow:

- First-time login: user is required to enroll a TOTP authenticator (or WebAuthn security key).
- Subsequent logins from a recognized device: password + remembered session.
- Subsequent logins from a new or unrecognized device: password + second factor (TOTP or WebAuthn) required.
- Recovery codes may be used to satisfy the second factor when the primary authenticator is unavailable.

3.2 Organization Administrator Login

Users with the **ORGADMIN** or **SUPERORGADMIN** role have elevated privileges and are subject to a stricter MFA flow:

- Every login (regardless of device recognition) requires password + second factor.
- Session timeout: 30 minutes of inactivity forces full re-authentication including MFA.
- Recovery codes available for emergency access; usage is audit-logged.

3.3 Patient Portal Login

Patient users accessing the MindWise patient portal have optional MFA, available via **Account Settings** → **Security**:

- TOTP enrollment self-service through the patient portal UI.
- Once enabled by the patient, all subsequent logins require the second factor.
- Patients may disable their own MFA at any time after authenticating with the current factor.

4. Implementation

MFA is enforced via Keycloak v24 as the identity provider for the MindWise Health platform. Specific Keycloak components used:

- **OTP Policy** — configures TOTP algorithm (SHA-256), period (30s), digit count (6), and look-around window.
- **WebAuthn Policy** — configures relying party ID, signature algorithms (ES256, RS256), user verification requirements.
- **Browser authentication flow** — chains username/password validation, MFA challenge, and conditional risk-based step-up.
- **Required Actions** — enforces MFA enrollment for accounts that lack a configured second factor.

5. Industry-Recognized Standards

Standard	Applicability
NIST SP 800-63B — Digital Identity Guidelines, Authenticator Assurance Level 2 (AAL2)	Clinical user authentication: TOTP + password satisfies AAL2.
RFC 6238 — TOTP (Time-Based One-Time Password)	Algorithm used for one-time passwords generated by authenticator apps.
RFC 4226 — HOTP (HMAC-Based One-Time Password)	Foundational algorithm underlying TOTP.
W3C Web Authentication (WebAuthn) Level 2	Browser-based authentication using FIDO2 security keys and platform authenticators.

FIDO2 CTAP2 — Client to Authenticator Protocol	Communication protocol between MindWise client and hardware security keys.

6. Contact

For inquiries regarding this document or the MindWise Health MFA implementation, please contact:

MindWise Health

1800 Mallory Lane, Ste D, Franklin, TN 37067

Email: info@MindWiseHealth.com

Phone: (615) 678-9600

Web: https://www.mindwisehealth.com