Proven.

Office of the National Coordinator for Health Information Technology §170.315(d)(13) – Multi-Factor Authentication

Product Name: Proven Software, Inc
Software Version: Proven EMR/EHR v2
Prepared For: ONC Health IT Certification Program
Certification Criterion: §170.315(d)(13) Multi-Factor Authentication
ONC-Authorized Certification: Drummond Group-https://www.drummondgroup.com
Certified Health IT Product List (CHPL) ID: 15.04.04.3273.Prov.02.00.0.260813
Document Version: 1.0
Effective Date: 08/13/2026

Proven EHR implements comprehensive multi-factor authentication (MFA) support with multiple authentication methods and security features:

1. Supported Authentication Methods

A. SMS Authentication

- Users receive security codes via text message to their registered phone number
- Most used method for patient portal access
- Requires phone number verification before activation

B. Email Authentication

- As an alternative to SMS, users can receive security codes by email.
- Users can choose between SMS or email when logging in

C. Authenticator App Support

- Support for TOTP (Time-based One-Time Password) authenticator apps
- Generates QR codes for easy setup with apps e.g. Google Authenticator, Microsoft Authenticator.
- Provides backup codes for account recovery

2. Key Security Features

A. Recovery Codes

- System generates 10 recovery codes when 2FA is first enabled
- Users can generate new recovery codes when needed
- Recovery codes provide backup access if primary 2FA method is unavailable
- System warns users when running low on recovery codes (3 or fewer remaining)

B. Device Management

- "Remember this device" option to skip 2FA on trusted devices

© 2026 Proven Software. All Rights Reserved

- Users can forget trusted browsers/devices to force 2FA on next login
- Rate limiting on verification code requests to prevent abuse

C. Account Security

- Automatic account lockout after failed login attempts
- Comprehensive logging of all authentication attempts
- Session management to prevent unauthorized access

3. User Experience

A. Setup Process

- Users can enable 2FA through their account management settings
- For SMS: Must verify phone number first
- For authenticator apps: Scan QR code with authenticator app
- System automatically generates recovery codes during setup

B. Login Process

- User enters username and password
- If 2FA is enabled, system prompts for second factor
- Users can choose SMS or email for code delivery
- Enter the received code to complete login
- Option to remember device for future logins

C. Administrative Features

- Users can disable 2FA if needed
- Reset authenticator keys
- Generate new recovery codes
- View remaining recovery codes

4. Implementation Details

The system uses ASP.NET Core Identity framework with custom extensions for:

- SMS delivery integration
- Email delivery integration
- Rate limiting for security code requests
- Comprehensive audit logging
- Session management for 2FA state

This multi-layered approach ensures that Proven EHR provides robust security while maintaining usability for both healthcare providers and patients accessing the system.

 © 2026 Proven Software. All Rights Reserved