170.315(d)(13)(i) Multi-factor authentication

Requirement:

1. The health IT developer attests, "Yes, the Health IT Module supports authentication, through multiple elements, of the user's identity with the use of industry-recognized standards," and;
2. The health IT developer submits description of the supported use cases.

Response:

- Yes – the Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards. When attesting "yes," the health IT developer must describe the use cases supported.

- Use Cases:

  IntelleChartPRO Login
  IntelleChartPRO can be configured to use the following multi-factor authentication methods in order to facilitate a more secure login workflow into the EHR:

  - Time-based One-time Password (TOTP) authentication via email address associated to user profile
  - Time-based One-time Password (TOTP) authentication via mobile authenticator app, Android, IOS or PC Browser

  If Feature is Enabled:

  - Application Authentication + MFA Authentication will be required during every login workflow into the EMR in order to gain access to the EMR
    - Including when using EMR Single Sign-On (UAM) from the Practice + Practice Management software

- Relied Upon Software:

  - Twilio-SendGrid: Used to facilitate the sending of emails containing Time-based One-Time Passwords (TOTP) to the user authenticating into the EMR via Multi-Factor Authentication.
  - Azure AppService: The technical host for the various Multi-Factor Authenticator systems and services used to facilitate this feature within the EMR.