Multi-Factor Authentication (MFA) Use Cases
Azalea EHR 4.0

§ 170.315(d)(13) Multi-Factor Authentication **requires certified Health IT to attest "yes" or "no" to its support of Multi-Factor Authentication. This Health IT Module supports the authentication, through multiple elements, of the user's identity with the use of industry-recognized standards.**

If a health IT developer attests "yes," the developer must provide a description of the supported use cases.

MFA Use Cases for Azalea EHR:
Azalea EHR requires that a user setup multi-factor authentication using one of the following methods:

- TOTP via email address associated with the user profile
- TOTP via SMS text associated with the mobile number on the user profile
- TOTP via phone call associated with the mobile number on the user profile
- TOTP via authenticator app associated with the user profile
- Passkeys using the WebAuthn standard

MFA Frequency is based on a detection algorithm combining various factors such as MAC address, IP address, time of last login, device specs, and more to determine if the user should be challenged for MFA.

Azalea relies on text, phone call or authenticator app TOTP.