Multi-factor Authentication Use Cases

daVinci EHR (v1.0)

Use Case 1: Admin Enables/Disables 2FA for a User

Actors: Admin user
Preconditions: Admin is logged in and has access to user management.
Main Flow:

1. Admin navigates to the user creation or edit page.
2. Admin sees a toggle labelled "Enable 2FA".
3. Admin checks or unchecks the "Enable 2FA" option.
4. System saves the 2FA setting for that user.

Postconditions:

- Only admin users can enable/disable the 2FA option.
- The 2FA setting is stored and reflected in the user's profile.

Use Case 2: 2FA is Enabled for a User

Actors: End user
Preconditions: The user has 2FA enabled in their profile.
Main Flow:

1. User attempts to log in to the EHR system.
2. System prompts the user for two-factor authentication through **Auth0**.
3. User completes the 2FA challenge.
4. System grants access to the EHR.

Alternative Flow:

- If the 2FA challenge fails or times out, access is denied.

Use Case 3: 2FA is Disabled for a User

Actors: End user
Preconditions: The user has 2FA disabled in their profile.
Main Flow:

1. User logs in with valid username and password.
2. System does not prompt for 2FA.
3. User is granted access immediately after credential verification.

Use Case 4: Default 2FA Setting

Actors: Admin user
Preconditions: A new user is being created.
Main Flow:

1. Admin opens the "Create User" form.
2. Admin does not modify the "Enable 2FA" option.
3. System defaults the "Enable 2FA" setting to **enabled**.
4. Upon user creation, the default 2FA setting is saved.

Use Case 5: Integration with Auth0

Actors: System, Auth0
Preconditions: Auth0 is integrated for 2FA services.
Main Flow:

1. Admin enables or disables 2FA for a user.
2. System updates the user's 2FA setting in Auth0.
3. Auth0 handles the 2FA challenge at login based on this setting.

Use Case 6: 2FA is Enabled and User clicks on the Lock button from the Menu

Actors: End User
Preconditions: 2FA is enabled for the User
Main Flow:

1. User is login and on Dashboard.
2. User clicks on the Profile icon from top right corner
3. User clicks on the Lock Button
4. User enter Valid Password
5. System does not prompt for 2FA.
6. User is granted access immediately after credential verification.