

**Digital Newspaper Website
Use-Case Specification: Change Password**

Version 1.0

404 Not Found

Revision History

Date	Version	Description	Author
18/07/2025	1.0	Specific about Change Password use case	Lê Thị Minh Thư

Table of Contents

1. Use-Case Name: Change Password	4
1.1 Brief Description	4
2. Flow of Events	4
2.1 Basic Flow	4
2.2 Alternative Flows	4
2.2.1 Invalid Current Password	4
2.2.2 The New Password does not meet format/ security requirements.	4
2.2.3 The Confirmation Password and New Password are not the same.	5
2.2.4 User Cancels the Operation	5
2.2.5 The New and Old Passwords are the Same.	5
2.2.6 MFA Verification Failed	5
2.2.6.1 MFA Verification Failed Subflows	5
2.2.7 MFA Code Expired	5
2.2.7.1 MFA Code Expired Subflows	5
3. Special Requirements	5
3.1 Security Requirement	5
3.2 System Performance	5
4. Preconditions	6
4.1 UserAuthentication	6
4.2 Setting Access	6
5. Postconditions	6
5.1 Password Successfully Updated	6
5.2 Confirmation Displayed	6
5.3 Optional Device Logout	6
6. Extension Points	6
6.1 Validate Password Format	6
6.2 Perform Multi-Factor Authentication MFA	6
6.3 Prompt Device Logout	6
7. Low Fidelity Prototype For Use Case	6
7.1 Prompt Used for AI Tool	6
7.2 Generated Interface	7

Use-Case Specification: Change Password

1. Use-Case Name: Change Password

1.1 Brief Description

This use case describes the functionality that allows users to change their current password to a new one in the system.

2. Flow of Events

2.1 Basic Flow

1. The user navigates to the Change Password section through access to the **Setting & Privacy** via their **Profile Information**.
2. The system checks whether **Multi-Factor Authentication (MFA)** is required:
 - a. If yes, the user is prompted to enter a verification code (via SMS, email, or authenticator).
 - b. The user enters the code.
 - c. The system verifies the code before proceeding.
 - d. If the code is valid and not expired, the flow proceeds.
3. The system displays a form requiring:
 - a. Current password
 - b. New password
 - c. Confirm new password
4. The user fills in all fields and submits the form.
5. The system verifies:
 - a. The current password is correct.
 - b. The new password meets format/ security requirements:
 - i. At least 8 characters.
 - ii. Contains at least one number.
 - iii. Includes at least one special notation.
 - iv. Includes both uppercase and lowercase letters.
 - c. The new password matches the confirmation.
 - d. The new password is NOT the same as the old password.
6. If all checks pass, the system updates the password.
7. The system displays a success message: "Your password has been changed."
8. After a successful password change, the system prompts the user: "Do you want to log out from other devices?"
 - a. If the user selects "Yes", the system logs the user out from all other active sessions except the current one.
 - b. If the user selects "No", the current session continues as usual.

2.2 Alternative Flows

2.2.1 Invalid Current Password

- At step 4.a, if the current password entered is incorrect:
- The system displays an error: "Incorrect password".
- The system will go to the step 3 of the **Basic flows** to allow retry.

2.2.2 The New Password does not meet format/ security requirements.

- At step 4.b, if the new password fails format/security rules:

- Depending on the inputting mistakes, the system displays an error:
 - + The password must contain at least one special notation (#, @, \$, ..)
 - + The password must contain at least one number (0,1, ..9)
 - + The password must contain at least one uppercase letter (A, B, C,..)
 - + The password must contain at least one lowercase letter (a, b, c,..)
 - + The password must have at least 8 characters.
- The flow returns to **Step 3**.

2.2.3 *The Confirmation Password and New Password are not the same.*

- At step 4.c, if the new password and confirmation do not match:
- The system displays an error: "Password confirmation does not match."
- The flow returns to **Step 3**.

2.2.4 *User Cancels the Operation*

- At any point before submission, if the user cancels the operation:
- The system closes the form and returns to the **Settings & Privacy** page, and no changes are made.

2.2.5 *The New and Old Passwords are the Same.*

- If the new password is identical to the current one:
- The system displays an error: "New password must be different from the current password."
- The flow returns to **Step 3**.

2.2.6 *MFA Verification Failed*

- At Step 2.b, if the entered OTP is invalid:

2.2.6.1 *MFA Verification Failed Subflows*

1. Show error: "Invalid verification code."
2. Allow the user to retry (max 3 attempts).
3. After 3 failed attempts, temporarily lock the password change process for 5 minutes.
4. The system returns to step 3 of the basic flows.

2.2.7 *MFA Code Expired*

- At Step 2.b, is the OTP has expired:

2.2.7.1 *MFA Code Expired Subflows*

- Show error: "Verification code has expired."
- Provide a button **Resend Code**
- Return to the OTP entry step after resending.

3. **Special Requirements**

3.1 **Security Requirement**

- Passwords must be stored using secure hashing algorithms (e.g: **SHA-256 with salt**) to ensure data protection and prevent password breaches.
- The system must prevent password reuse and brute-force attacks.

3.2 **System Performance**

- Password update operation should complete within 2 seconds under normal load.
- Error messages must appear within 500 milliseconds of validation failure.
- The system should handle simultaneous password change requests for up to 500 users without performance

degradation.

4. Preconditions

4.1 UserAuthentication

- The user must be logged in to their account.

4.2 Setting Access

- The **Settings & Privacy** section is accessible from the user's profile.

5. Postconditions

5.1 Password Successfully Updated

- The user's password is securely updated and stored.

5.2 Confirmation Displayed

- A success message is shown: **"Your password has been changed."**

5.3 Optional Device Logout

- If the user chooses to log out from other devices, all other sessions are terminated except the current one.

6. Extension Points

6.1 Validate Password Format

- **Location in flow:** Step 5 of the Basic Flow
- **Description:** The system checks whether the new password meets the format requirements and security criteria.

6.2 Perform Multi-Factor Authentication MFA

- **Location in flow:** After Step 1 (user accesses Change Password section)
- **Description:** The system may require additional verification such as OTP before proceeding to display the form, depending on user settings or risk evaluation.

6.3 Prompt Device Logout

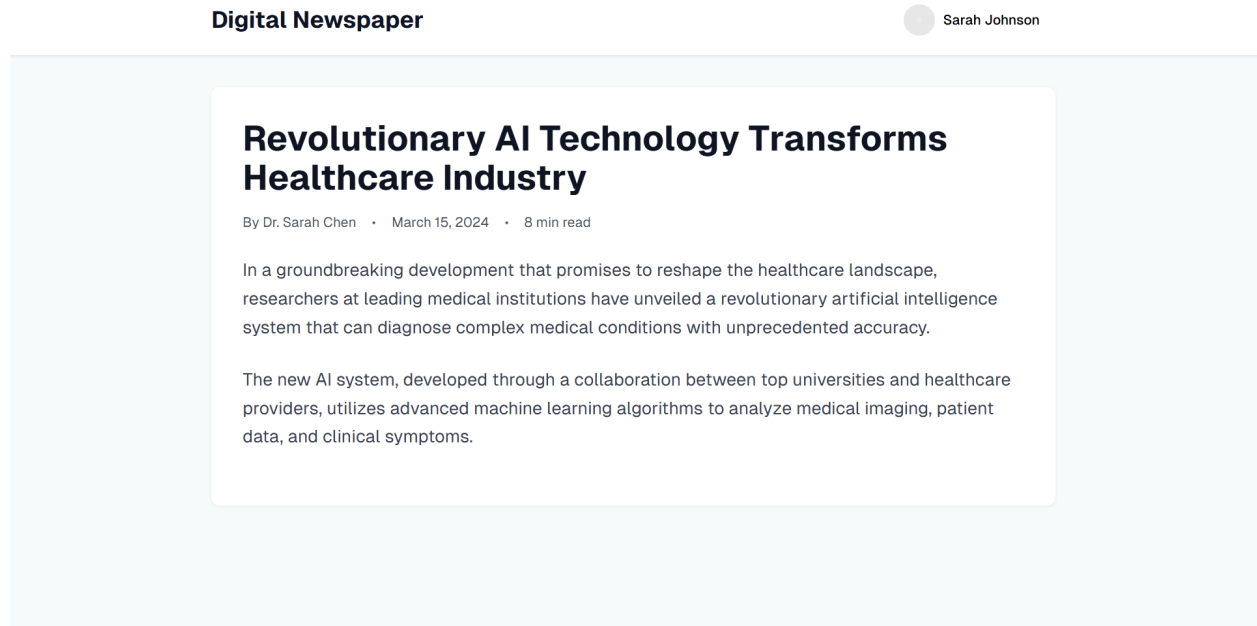
- **Location in flow:** After step 6 of Basic Flow
- **Description:** The system asks whether the user wants to log out of other devices. If yes, the system ends all other active sessions.

7. Low Fidelity Prototype For Use Case

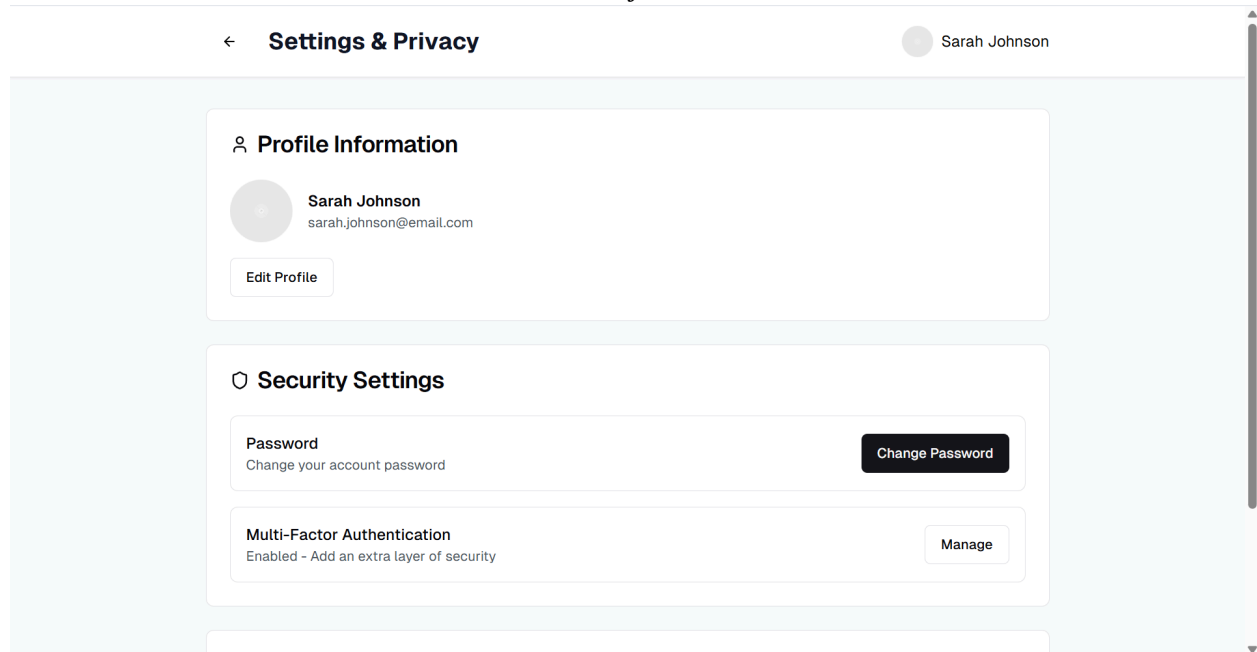
7.1 Prompt Used for AI Tool

- Create a responsive web UI for a digital newspaper article page with a "Change Password." feature.
- Requirements: Meets all that have been specified in the use-case specification.
[2. Flow of Event 6.Extension Points] (*Paste the use case specification from section 2 to 6 here*)
- The UI should be mobile-friendly and support modern browsers. Prioritize usability and simplicity.
- The system must show OTP code verification, show expired time, message error and allow it to try again.


7.2 Generated Interface




The main screen of the main website



Here are the Profile Information after the user click to their profile symbol. At the Security Setting has a Change Password button.

 **Multi-Factor Authentication**

 **Verification code sent via SMS to your phone**
Enter the 6-digit code to continue


Code expires in: **4:58**


Attempts remaining: 3

Verify

Cancel

Here is the main screen after clicking the Change Password button. The OTP code hasn't input yet, so the Verify button is invalid

 **Multi-Factor Authentication**

 **Verification code sent via SMS to your phone**
Enter the 6-digit code to continue


Code expires in: **4:26**


Attempts remaining: 3

Verify

Cancel


The OTP code is input, but the length is not equal to 6, so the Verify button is invalid

 **Multi-Factor Authentication**

 **Verification code sent via SMS to your phone**
Enter the 6-digit code to continue


Code expires in: **4:09**


Attempts remaining: 3

 **Verifying...**

Cancel



The OTP code is input, the Verify button is Valid. Here is the processing screen after clicking the Verify button.

 **Multi-Factor Authentication**


 **Verification code sent via SMS to your phone**
Enter the 6-digit code to continue

Code expires in: **3:59**

123456


Attempts remaining: 2


 Invalid verification code.

Verify

Cancel

In case the OTP code is incorrect, or time out, the system will message “Invalid verification code”. The cancel will go back to the main screen of the Profile Information.

 **Multi-Factor Authentication**




Verification code sent via SMS to your phone
Enter the 6-digit code to continue

Code expires in: **3:39**

543210

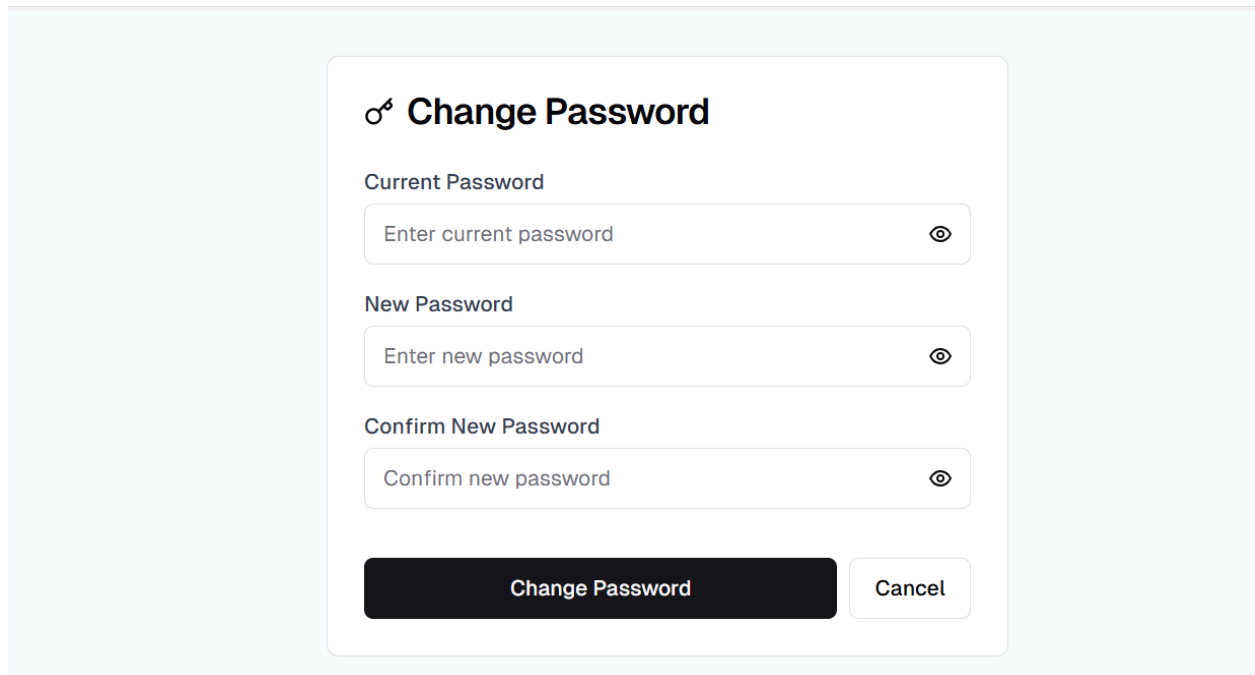
Attempts remaining: 2


 **Verifying...**

Cancel


The previous OTP code is incorrect, so that the Attempts remaining decrease from 3 to 2. After retyping the OTP code and clicking the Verify button. The verification is processing.

← Change Password


A screenshot of a mobile application's 'Change Password' screen. The screen has a light blue background. In the center is a white rounded rectangle containing the title 'Change Password' with a key icon. Below the title are three input fields: 'Current Password', 'New Password', and 'Confirm New Password'. Each field has a placeholder text and a toggle icon on the right. At the bottom of the white rectangle are two buttons: a dark blue 'Change Password' button and a light blue 'Cancel' button.

 **Change Password**


Current Password

Enter current password 

New Password

Enter new password 

Confirm New Password


Confirm new password 

Change Password Cancel


After the OTP code is successfully verified, the Change Password screen is displayed.

Change Password

Current Password


chaseyoudream

New Password

helloevery1

- ✓ At least 8 characters
- ✓ Contains at least one number
- ✗ Contains special character
- ✗ Contains uppercase letter
- ✓ Contains lowercase letter
- ✓ Different from current password

Confirm New Password


helloevery1

- ✓ Passwords match

Change Password

Cancel


The new password does not meets the format and security criteria for the password. Depends on which mistakes, the system shows to the user to adjust the right format password. In this case, if the user chooses the Cancel button, it will go to the Profile Information screen.



Change Password


Current Password


.....





New Password


.....





 At least 8 characters

 Contains at least one number

 Contains special character


 Contains uppercase letter


 Contains lowercase letter

 Different from current password

Confirm New Password

.....



 Passwords match

Change Password

Cancel

The same as the picture above. One difference is that the user can click to the Eye Symbol to show or hide the

404 Not Found

password.

Change Password

Current Password

New Password

- ✓ At least 8 characters
- ✓ Contains at least one number
- ✗ Contains special character
- ✗ Contains uppercase letter
- ✓ Contains lowercase letter
- ✓ Different from current password

Confirm New Password

✓ Passwords match

 Incorrect password

Change Password


Cancel

404 Not Found


After the user clicks the Change Password button, the system will check the information. In this case, the password does not meet the format and security criteria for password requirements, so that the system messages "Incorrect password"

Change Password

Current Password




New Password



- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter
- ✗ Different from current password

Confirm New Password



✓ Passwords match


Change Password

Cancel


The systems show the mistakes directly when the user typing the wrong password.

Change Password

Current Password


Minhth@070705 

New Password

Minhth@070705 

- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter
- ✗ Different from current password

Confirm New Password

Minhth@070705 

- ✓ Passwords match

❗ Incorrect password

Change Password

Cancel

The system still check the Confirm New Password with New Password regardless of it is the same or not the same with Old Password.

Change Password

Current Password

Enter current password



New Password



Please fill out this field.

Minhth@070705




- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter

Confirm New Password

Minhth@070705



✓ Passwords match

 Incorrect password

Change Password

Cancel

404 Not Found

The system messages “Please fill out this field” at the box that the user leave it empty.

Change Password

Current Password

Minhth@0707054123



New Password

Minhth@070705412



- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter
- ✓ Different from current password

Confirm New Password

Minhth@0707054123



✗ Passwords match

Change Password

Cancel

Change Password

Current Password

Minhth@0707054123



New Password

Minhth@070705412



- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter
- ✓ Different from current password

Confirm New Password

Minhth@070705412



✓ Passwords match

Change Password

Cancel

404 Not Found

No red color check, that means the password is correct with the format and security criteria for password requirements.

Change Password

Current Password

Minhth@0707054123



New Password

Minhth@070705412




- ✓ At least 8 characters
- ✓ Contains at least one number
- ✓ Contains special character
- ✓ Contains uppercase letter
- ✓ Contains lowercase letter
- ✓ Different from current password

Confirm New Password

Minhth@070705412



- ✓ Passwords match

 Updating...

Cancel

404 Not Found

After clicking the Change Password button, because the Old Password is corrected and the New Password and Confirm New Password meet and concurrency. So that the system Updating the New Password.



Your password has been changed

Your account is now more secure with your new password



[→] Log Out Other Devices?

Your password has been successfully changed. Do you want to log out from other devices for added security?

Recommended: Logging out other devices helps protect your account if someone else had access to your old password.


Yes, Log Out Other Devices

No, Keep Sessions

After Change Password successfully, the system asks the user if they want to log out other devices or not

404 Not Found

← **Settings & Privacy**

 Sarah Johnson

Profile Information



Sarah Johnson
sarah.johnson@email.com

Edit Profile

Security Settings

Password

Change your account password

Change Password

Multi-Factor Authentication

Enabled - Add an extra layer of security

Manage

After choosing “Yes, Log Out Other Devices” or “No, Keep Sessions”, the system back to the Profile Information scree