Pando App User Flow: User Onboarding

Goal:

To securely register, verify identity, and gain access to the platform to begin using clinical communication features.

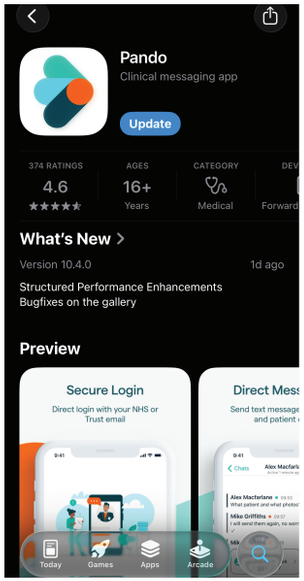
Preconditions:

User has access to a mobile device compatible with the application

User has a valid NHS or organisational email address

User has been invited or is eligible to register

Step 1: Application Download



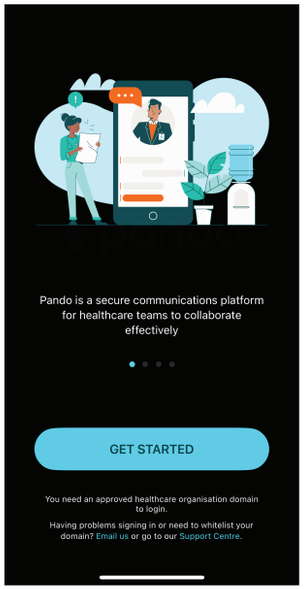
Step Overview: User downloads and opens the app

Touchpoints: Welcome screen displayed with “Get Started” option

Potential Risks: User uncertainty about purpose of app

Mitigation: Clear onboarding messaging and branding

Step 2: Get Started



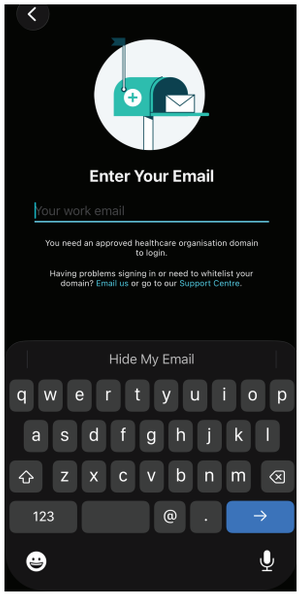
Step Overview: Get started screen

Touchpoints: User selects “Get Started”

Potential Risks: User exits onboarding before registration is completed

Mitigation: Clear onboarding flow with visible progression through setup steps

Step 3: Enter your email



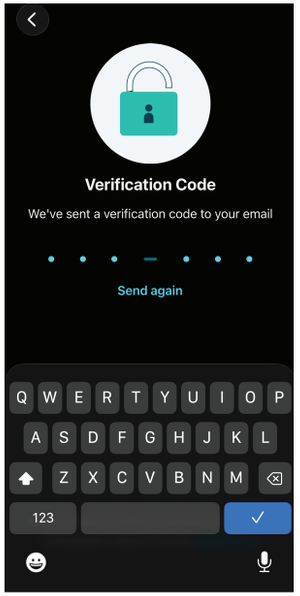
Step Overview: User enters email address

Touchpoints: System checks eligibility

Potential Risks: Delays or confusion during authentication

Mitigation: Clear instructions

Step 4: Verification Code



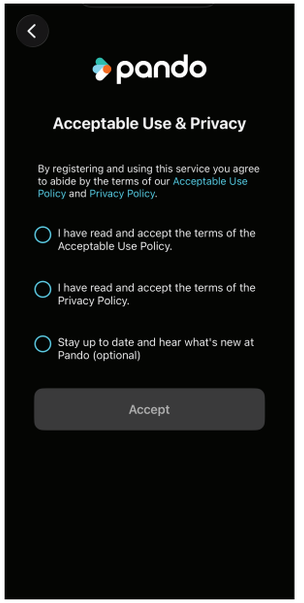
Step Overview: User asked to enter code sent securely to email they signed up with

Touchpoints: User will navigate to email the come back to app to enter code

Potential Risks: Organised emails fraudulently used

Mitigation: Verification code sent to email must be entered

Step 5: Accept Policies



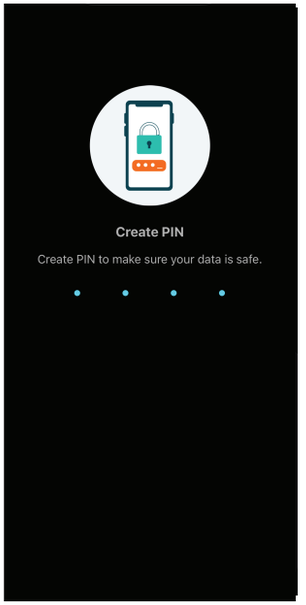
Step Overview: User reviews and accepts required policies

Touchpoints: Acceptable Use Policy, Privacy Policy, optional communications consent

Potential Risks: User may not fully review policies before accepting

Mitigation: Policies are presented clearly during onboarding and require explicit acknowledgement before proceeding

Step 6: Create PIN



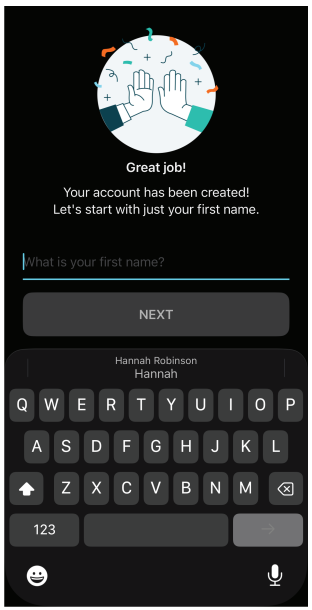
Step Overview: User creates and confirms PIN

Touchpoints: PIN creation screen

Potential Risks: Weak PIN combinations may reduce security if easily guessed

Mitigation: PIN authentication is combined with verification code authentication, reducing reliance on the PIN as the sole authentication factor

Step 7:
Enter First Name



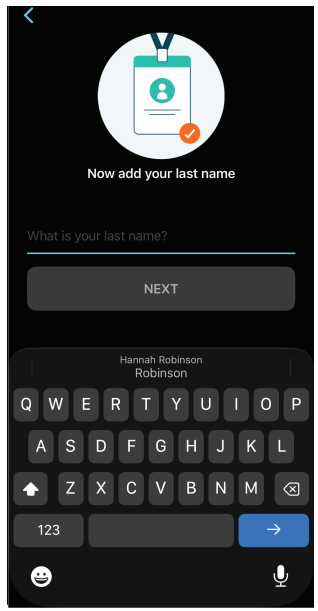
Step Overview: User enters first name for profile setup

Touchpoints: Text input field

Potential Risks: Incorrect user information entered

Mitigation: User can review entered details during onboarding

Step 8:
Enter Last Name



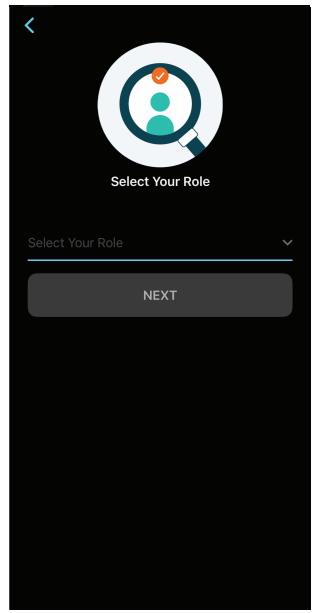
Step Overview: User enters surname for profile setup

Touchpoints: Text input field

Potential Risks: Incorrect user information entered

Mitigation: User can review entered details during onboarding

Step 9:
Select Role



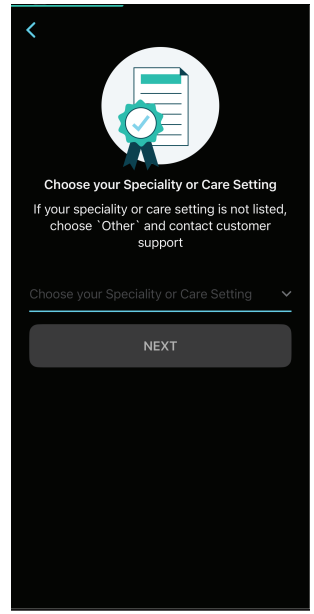
Step Overview: User selects role from available options

Touchpoints: Role selection dropdown/list

Potential Risks: User unable to locate an exact role match

Mitigation: Standardised role options support consistency across organisations

Step 10:
Select Speciality or Care Setting



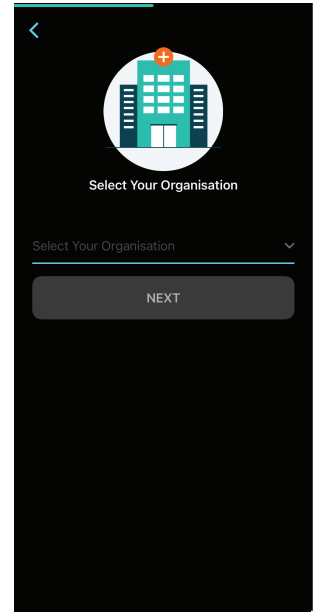
Step Overview: User selects speciality or care setting

Touchpoints: Dropdown selection field

Potential Risks: User speciality may not appear in predefined list

Mitigation: Alternative selection options and support guidance provided within onboarding

Step 11:
Select Organisation



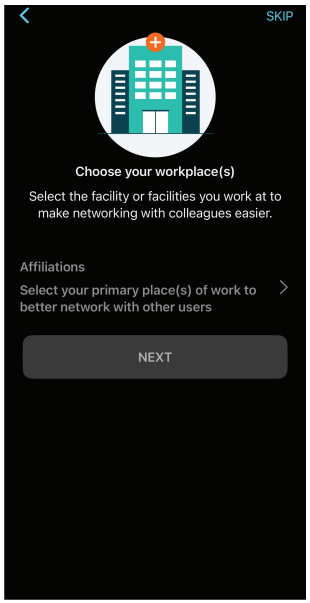
Step Overview: User selects organisation from available list

Touchpoints: Organisation selection field

Potential Risks: Incorrect organisation selected

Mitigation: Organisation selection list presented clearly during onboarding

Step 12: Select Workplace(s)



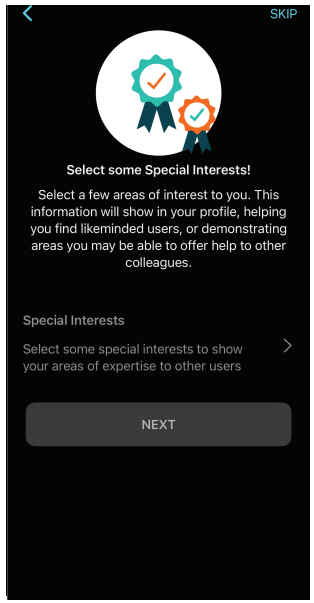
Step Overview: User selects workplace or affiliated locations

Touchpoints: Affiliation selection screen

Potential Risks: User may skip workplace selection

Mitigation: Workplace selection can be updated later within the application

Step 13: Select Special Interests



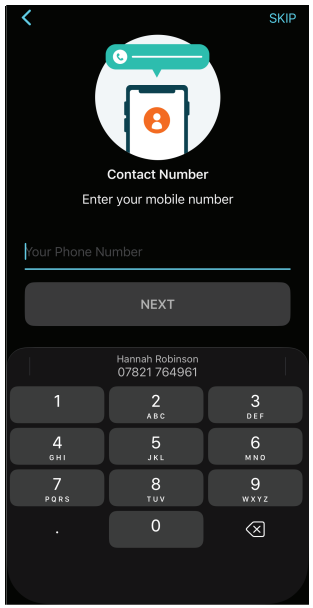
Step Overview: User selects areas of interest or expertise

Touchpoints: Special interests selection screen

Potential Risks: User may not complete optional profile information

Mitigation: Special interests section is optional and can be updated later

Step 14: Enter Mobile Number



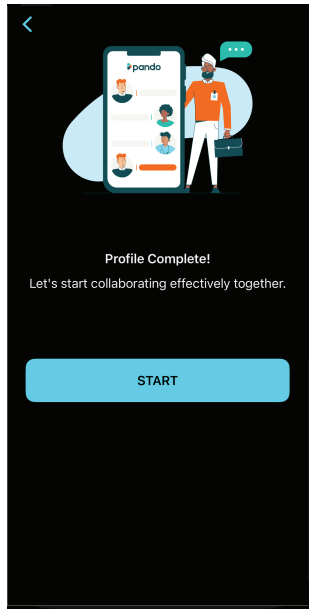
Step Overview: User enters mobile contact number

Touchpoints: Phone number input field

Potential Risks: Some users may be uncomfortable providing personal contact information

Mitigation: Purpose of mobile number collection explained during onboarding as well as being optional

Step 15: Profile Complete



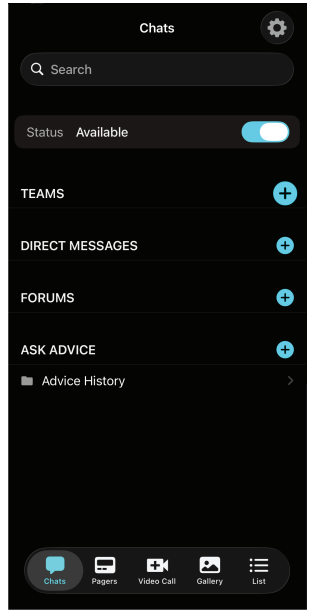
Step Overview: User completes onboarding and profile setup

Touchpoints: Profile completion confirmation screen

Potential Risks: User uncertain how to begin using the platform

Mitigation: Clear confirmation messaging and “Start” action presented

Step 16: Access Platform



Step Overview: User accesses the main chat dashboard

Touchpoints: Chats dashboard and navigation interface

Potential Risks: User unsure where to begin within the application

Mitigation: Simple default dashboard with key communication features immediately visible

Pando App User Flow: Invite colleagues to Pando

Goal:

To invite a colleague to join the Pando app via a secure shareable link.

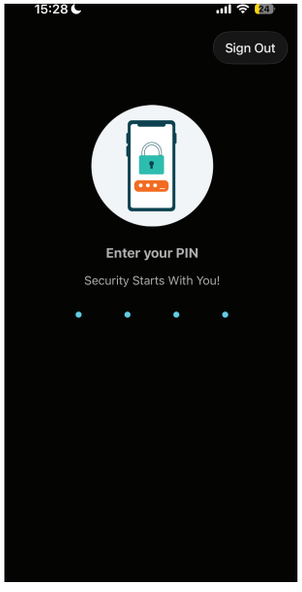
Preconditions:

User is registered and authenticated

User has access to the application settings

User has a valid method of sharing (e.g. email, messaging app) on their device

Step 1: User opens the app



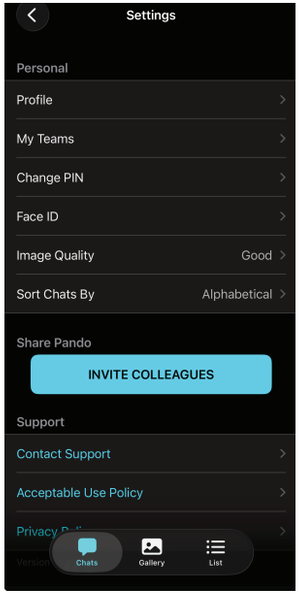
Step Overview: User opens the app

Touchpoints: Authentication prompt displayed (PIN / biometric)

Potential Risks: Delay accessing features due to authentication

Mitigation: Biometric login supported for faster access

Step 2: User accesses app settings



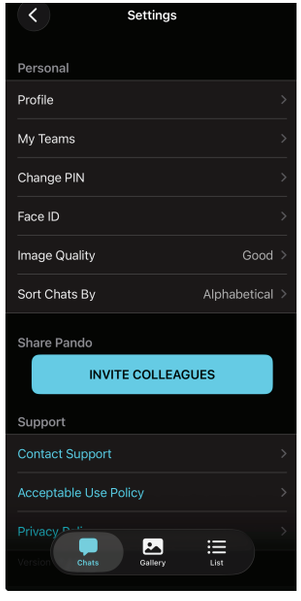
Step Overview: User accesses app settings

Touchpoints: Settings menu visible and accessible

Potential Risks: User unable to locate settings

Mitigation: Standardised navigation and clear iconography

Step 3: Invite Colleagues



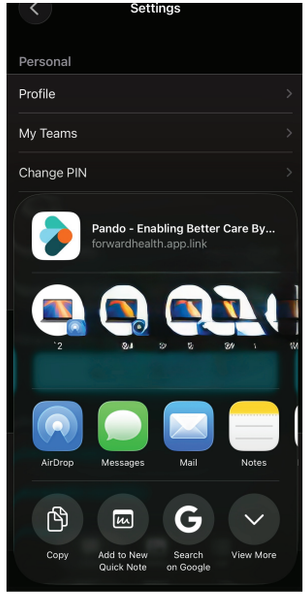
Step Overview: User taps “Invite Colleagues”

Touchpoints: Invite option within settings

Potential Risks: Feature not easily discoverable

Mitigation: Clear labelling and consistent placement within settings

Step 4: OS sharing window opens



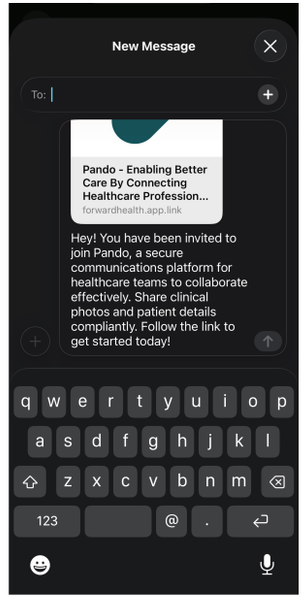
Step Overview: System generates invite link and pre-filled message

Touchpoints: Native OS share interface displayed

Potential Risks: User unable to edit invite message

Mitigation: Pre-defined message ensures consistency of invitation content

Step 5: Sharing methods



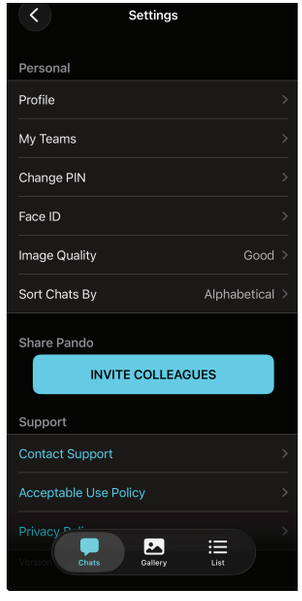
Step Overview: User chooses platform (e.g. email, messaging app) and sends invitation

Touchpoints: Device sharing options

Potential Risks: Invitation sent to incorrect recipient

Mitigation: User selects recipient within familiar device interface

Step 6: User returns to app



Step Overview: User is returned to the settings screen

Touchpoints: Navigation back to app

Potential Risks: No confirmation of invite being received

Mitigation: The selected sharing application (e.g. Mail or Messages) retains a record of the outbound invitation, allowing the user to confirm the invite was sent