## Sample Workflows

**Always:**

- **Encrypt data at rest (inputted data that needs to be stored on a device) with AES-256**
- **Data in Transport (data communicated between devices) using TLS 1.3**

| Step | Action | Cybersecurity Concerns |
|---|---|---|
| **1** | Create an Account: Sign up for the app by providing your information. | • Cloud to App - Check to ensure app version is valid and updated<br>• App to Cloud – Ensure connection, if receiving update information check via hashing or signatures that the update is valid<br>• App to Device – Ensure the device is running valid firmware<br>• Enforce Strong Password Policy (currently 15+ characters but no rules on symbols or capitals or numbers added)<br>• Enforce Multi Factor Authentication (Checking what device supports then one time password with phone number, biometric/voice/face recognition)<br>• Informing user of security concerns/tools they can use on their own app for cybersecurity (secure folders, their own |
| **2** | Profile Setup: Fill in your personal details and your doctor's information. | • Use Regex or other tools to verify inputs, this not only ensures data matches, but to ensure no data entered could be used for attempted SQL injection or other reasons<br>• Ensure data kept and transported is encrypted |
| **3** | Prescription Dosage Entry: Enter the dosage prescribed by your doctor. | • Use Regex or other tools to verify inputs, this not only ensures data matches, but to ensure no data entered could be used for attempted SQL injection or other reasons<br>• Ensure data kept and transported is encrypted |
| **4** | Activate Bluetooth: Enable Bluetooth on your smartphone. | • Ensure Bluetooth version 5.0+ with LE Secure Connections.<br>• Monitor and Block unexpected Bluetooth activity or pairing requests. Pairing should only be enabled when required |
| **5** | Pair with Main Pod: Connect the app to the main pod device. | • Ensure devices are not discoverable by default |

| | | |
|---|---|---|
| | | • Utilizing NFC for secure key exchange (assuming phone supports NFC, other secure pairing methods could be used)<br>• Ensure Bluetooth version 5.0+ with LE Secure Connections.<br>• Monitor and Block unexpected Bluetooth activity or pairing requests. |
| **6** | Cartridge Connection Check: Verify if the drug cartridge is securely connected to the main pod. | • Confirm pairing for scanning cartridges, ensure protection from QR code scanning (fake/wrong images used) |
| **7** | Cartridge Capacity Check: Determine the remaining drug capacity in the cartridge. | • Ensure regular security (device at rest/transport encryption) |
| **8** | Prepare the Pump: Perform the initial setup to ensure the pump is ready. | |
| **9** | Needle Mechanism Release: Release the needle mechanism by pressing the release button. | • Ensure secure, solid connection between smartphone and device before dosing process<br>• Depending on time since last verification, re-verify identity using MFA methods? |
| **10** | Start Dosing: Initiate the dosing process. | |
| **11** | Pre-Meal Data Input: Before a meal, input your carbohydrate intake and blood glucose levels. | • Use Regex or other tools to verify inputs<br>• [Note for future: Security for integration process with glucose monitoring system] |
| **12** | Dosage Calculation: Allow the app to calculate your dosage based on your doctor's prescription. | • Ensure regular security between device and cloud (or just device if prescription stays stored on device) (device at rest/transport encryption) |
| **13** | User Confirmation: Confirm the suggested dosage or make adjustments if needed. | |
| **14** | Injection Initiation: Press the button to start the injection. | • Ensure secure, solid connection between smartphone and device before dosing process |
| **15** | Track Drug Volume: Keep an eye on the remaining drug volume in the cartridge. | |
| **16** | Cartridge Replacement Alert: Receive an alert to replace the cartridge when it's empty. | |
| **17** | Dosing Completion: Stop the pump when the dosing process is finished. | • Log completed dosing to cloud |

## Special Cases

### App Initialization when User has Existing Account (lost/inaccessible or new phone)

| Step | Action | Cybersecurity Concerns |
|---|---|---|
| **1** | Request existing account information | • Use existing credentials and MFA to verify login information<br>• Ensure data is encrypted at rest and in transport<br>• Sending e-mail or other record to log to user and cloud that a new device has logged into the account<br>• Potential use of one time codes if regular MFA methods inaccessible, in which case only temporary use<br>• Log all attempts, successful or not to cloud |
| **2** | Ask what the device will be used for and whether it should be trusted | Temporary Use for Lost Device or Out of Battery (e.g. using a friend's phone)<br>• Register user/device for limited access and restrict features (what information they can pull from cloud that can contain personal identifiable information, ect.)<br>• Require more frequent verification and re-sign in procedures<br>• Prompt on main device to remove or disable additional trusted devices when no longer being used<br>New Device<br>• Register/record user as a patient and establish regular patient permissions |
| **3** | Pair with Main Pod: Connect the app to the main pod device. | • Ensure devices are not discoverable by default<br>• Utilizing NFC for secure key exchange (assuming phone supports NFC, other secure pairing methods could be used)<br>• Ensure Bluetooth version 5.0+ with LE Secure Connections.<br>• Monitor and Block unexpected Bluetooth activity or pairing requests. |
| | Continue regular process | |