Healthcare Mobility Implementation Guide

Plan clinician, clinic and patient device programs around reliable handoffs, clear ownership and measurable readiness.



Illustrative image. Not a customer or ConnectUs facility photograph.

Who this guide is for

Healthcare systems, clinics, medical device organizations, remote patient monitoring teams and in-home nursing providers.

Use this framework to define owners, acceptance criteria and a controlled rollout. Subject matter expert review is pending. Validate the plan with your operational, IT and security owners before implementation.

1. Define the clinical workflow

Map who receives the device, which applications they use, whether it is shared, where it travels and how it returns. Separate clinician devices from patient kits and medical device accessories.

Accountable owner: Clinical operations and IT

Acceptance gate: Approved workflow map, device ownership, application inventory and patient support boundaries.

2. Agree on data and security responsibilities

Identify where electronic protected health information is stored or accessed. Have privacy and security owners evaluate access, encryption, identity, auditability, remote actions and whether a business associate agreement is required. Do not place patient details on shipment labels or in deployment spreadsheets.

Accountable owner: Security and privacy owners

Acceptance gate: Documented risk assessment, approved policies, role based access and a defined incident escalation path.

3. Design and test a standard kit

Validate the device, carrier, charging accessories, protective case, application compatibility, enrollment and approved cleaning process. For RPM, confirm pairing, connectivity and patient instructions with the platform owner. Device management does not validate clinical performance.

Accountable owner: IT, clinical operations and application owner

Acceptance gate: Versioned kit bill of materials, configuration profile and signed acceptance test.

4. Run a representative pilot

Include real shifts, shared device handoffs, weak connectivity areas and replacement scenarios. Test authentication, application launch, connectivity, lost device actions and return processing. Set acceptance thresholds before collecting results.

Accountable owner: Pilot lead and departmental champions

Acceptance gate: Pilot issues resolved or accepted; launch approval from clinical, IT and security owners.

5. Roll out in controlled waves

Match serial numbers to approved destinations, verify enrollment before shipment, schedule receiving staff and provide concise instructions. Track shipment, receipt and readiness separately. Keep an exception queue for failed enrollment or incomplete orders.

Accountable owner: Deployment lead and receiving teams

Acceptance gate: Reconciled asset register, receipt confirmation and completed readiness checks for each wave.

6. Operate, replace and recover

Define who receives support tickets, when they escalate and how approved spares are released. Validate wipe or data handling before redeployment. Measure readiness, ticket response, restoration time, replacement arrival and returns without publishing patient data.

Accountable owner: Service owner and security lead

Acceptance gate: Monthly operating review, documented exceptions and approved recovery records.

Measure before and after

• First use success = devices passing agreed readiness checks / devices issued.

• Time to ready = elapsed time from approved complete request to verified usability.

• Restoration time = elapsed time from incident to usable replacement or repair.

• Return completion = returned assets reconciled / assets expected back.

Record baseline dates, sample size, device population, target, actual result and exceptions. Keep response, restoration, shipment and arrival metrics separate. Labor capacity released is not automatically cash savings.

Agree on the service scope

Confirm support hours and severity levels; response and restoration targets; order completeness and shipping cutoffs; geography and carrier dependencies; stock and spare ownership; returns and data handling; fees and exit responsibilities.

Review and approval record

Operational owner / date: _____

IT and application owner / date: _____

Security and privacy owner / date: _____

Pilot acceptance decision / exceptions: _____

Review status: pending. No service timing, financial outcome or compliance certification is promised by this planning guide.

Source and next step

HHS mobile device and ePHI guidance. Appropriate safeguards and applicable business associate arrangements must be evaluated for the actual environment.

Discuss your implementation plan with ConnectUs