OFFLINE-FIRST SYSTEM SPECIFICATION & INTERFACE DESIGN

Version 2.0 - Post-Validation Revision

INTRODUCTION

This document details the offline-first workflow and user interface for a health supply chain system designed for the realities of Uganda's rural and humanitarian settings. It is a direct response to the 2025 Baseline Assessment, which found that 89% of facilities have unreliable internet and power, staff have low to medium digital literacy, and health workers revert to paper as the authoritative record when digital systems fail.

The design prioritizes resilience over real-time connectivity, human judgment over rigid automation, and seamless integration with (not replacement of) existing paper-based workflows.

DESIGN PHILOSOPHY & CORE PRINCIPLES

- Offline-first is non-negotiable: Every critical function must be available without an internet connection.
- Human-in-the-Loop: The system provides recommendations; health workers make final decisions. Override is a feature, not a bug.
- Paper-digital harmony: The system must generate paper outputs that match existing MoH registers (e.g HMIS 105) to ensure continuity and serve as a trusted backup.
- Minimalist and guided UI: Interfaces must be simple, with clear language and visual cues to support users with varying levels of tech comfort.

DETAILED OFFLINE OPERATION SPECIFICATION

Core Components & Data Storage

Local Database Architecture

- Database Engine: SQLite configured in Write-Ahead Logging (WAL) mode to enable concurrent read operations during background sync processes.
- WAL Configuration: `PRAGMA journal_mode=WAL; PRAGMA synchronous=NORMAL`; for optimal performance and data integrity.
- Target Size: <50MB per facility to maintain performance on entry-level Android devices.
- Rationale for WAL: Standard SQLite journal mode blocks all reads during write operations. WAL mode prevents database locks during background sync, allowing facility staff to continue data entry while uploads occur.

Stored Data

- Facility profile and storage capacity rating
- Master list of essential medicines and commodities
- Last 12 months of facility-specific consumption data (active operational data)
- Current stock levels and pending orders
- User credentials for offline authentication (hashed using bcrypt)

Data Encryption & Security

- Encryption Standard: AES-256 encryption for entire SQLite database file.
- Key Management: Encryption keys are generated and stored using the Android Keystore System. Keys are generated within hardware-backed secure enclaves (where available on the device) and never appear unencrypted in application memory or file storage.

- Key Lifecycle: Keys are generated at first app installation. No file-based or plaintext key storage is permitted. Keys remain in Android Keystore exclusively.
- Implementation Note: This approach meets Uganda Data Protection and Privacy Act (2019) requirements and technical validation recommendations.

Data Persistence & Auto-Save
All data is saved instantly to the local database. Auto-save is continuous and invisible to the user. There are no explicit 'Save' buttons. This reduces cognitive load and prevents data loss if the app closes unexpectedly or the device loses power.

Data Archiving & Purging Policy
To maintain the <50MB target size while preserving data for compliance and audit purposes:
- Active Retention Period: Last 12 months of consumption data and stock counts stored in operational SQLite database.
- Automatic Archive Trigger: Automated monthly background job (runs during successful sync) moves data older than 12 months to compressed archive files (.zip format).
- Archive Upload: Compressed archive files are uploaded to district server during next sync, then deleted from device after successful upload confirmation.
- Emergency Purge Policy: If database size exceeds 45MB (90% of target), automated purge process is triggered:
    - User receives notification: 'Storage limit approaching. Archiving old data.'
    - Oldest archived data is removed first (if any archives remain on device)
    - If still over 45MB, oldest active data beyond 12-month window is archived and uploaded
    - Archive upload occurs before deletion to prevent data loss

Tier 1 Offline Forecasting Integration
The Tier 1 Rule-Based Forecast (as defined in the Predictive Demand Framework) is pre-loaded and runs entirely locally. This is the primary forecasting mechanism available offline.

Example Logic Displayed to User:
- *Forecast: 1,000 Coartem tablets*
- *Calculated from:*
    - *Your 3-month average (800 tablets)*
    - *Rainy season adjustment (+200)*
    - *Capped at 1,000 due to your 'Inadequate' storage capacity*

User Action: The user can easily adjust this quantity up or down directly from the dashboard using a slider or numeric input.

Tier 2 Statistical Forecasts (Informational Only)
When facilities sync with the district server, they receive Tier 2 hierarchical statistical forecasts generated by district-level models. These forecasts are stored separately from the operational SQLite database to prevent concurrent write conflicts during background sync.
- Storage Location: Separate read-only JSON files in the app's internal storage, not in the SQLite database.
- User Interface: Tier 2 forecasts are displayed in a read-only 'District Insights' section of the app. Users can view them for context but cannot directly use them for order generation.
- Rationale: SQLite WAL mode enables concurrent reads during writes, but separating informational forecast data from operational transaction data prevents potential conflicts and keeps the sync process simple and reliable.

Synchronization Logic

Automatic Sync Triggers

- Network Detection: Background service checks for connectivity every 15 minutes.
- Battery Threshold: Automatic sync only occurs when device battery is above 20% to preserve battery health.
- Device Activity: Sync processes run only when the device is not in active use (screen off or app in background) to avoid interrupting user work.
- Manual Override: Users can trigger 'Sync Now' from the app at any time if connectivity is available, bypassing battery and activity checks.

Upload Process

- Payload: Batched JSON packets containing new stock counts, adjusted orders with override justifications, consumption data, and sync metadata (last sync timestamp, facility ID, user ID).
- Compression: All data is compressed using GZIP to minimize data transfer costs.
- Retry Logic: Failed uploads are retried automatically with exponential backoff (initial delay 30 seconds, maximum delay 15 minutes).

Download Process

- Payload: Updated delivery schedules, budget status notifications, Tier 2 statistical forecasts (stored as separate JSON files), system messages, and credential refresh tokens.
- Processing: Downloaded data is validated for schema compliance and plausibility before being written to local storage.

Conflict Resolution Principle

Local User Edits Always Win. The system is designed to trust the health worker on the ground. If a user adjusted an order offline and the central system also modified it, the user's version is preserved and the conflict is logged to the override audit trail for review by district officers.

Offline Authentication & Credential Management

- Credential Storage: User credentials are cached locally (hashed using bcrypt with salt) for offline authentication.
- Credential Sync: During each successful connection to the district server, the app checks for credential updates (password changes, role modifications, account status).
- Offline Validity Period: Local credentials remain valid for 90 days of offline operation. This accommodates extended periods without connectivity.
- Expiry Enforcement: If no sync occurs within 90 days, the user must connect to verify credentials before continuing. A warning appears at 75 days (15 days before expiry).
- Permission Changes**:** Role or permission changes made at the district level sync immediately upon next connection and take effect on the device.

Paper Backup Integration

Paper-digital harmony is a core design principle. The system does not replace paper, it augments it.

- Printable Forms: Every data entry and order generation screen includes a 'Print' button.
- Output Format: A pre-populated paper form that mirrors the layout of official MoH paper registers (e.g HMIS 105). This ensures data can be transported physically if needed, staff have a familiar trusted record, and continuity of operations during prolonged power failure or device issues.

USER ROLES & PRAGMATIC WORKFLOWS

Role	Primary Offline Tasks	Key Interface Features
Facility Staff	Conduct weekly stock counts, place orders, report stockouts	Home dashboard with stock alerts, one-tap order adjustment, offline data entry forms
Store Manager	Manage stock ledger, review expiry dates, approve facility orders	Expiry alert screen, stock ledger view, order approval queue (synced when online)
District Supply Officer	Review facility status, approve bulk orders, plan redistributions	District dashboard (requires sync), facility risk list, override pattern reports

UI WIREFRAME DESCRIPTIONS

Login Screen

- Feature: Clear, large 'Work Offline' button prominently displayed. Persistent visual indicator showing 'Offline Mode' or 'Last Synced: 2 days ago'.
- Justification**:** Addresses the baseline quote: 'Right now, unless you buy MBs, you can't open anything.' Users should never feel blocked by connectivity.

Home Dashboard (Facility Staff)

Key elements:

- Color-coded Stock Alerts: Red for stockout, amber for low stock (below safety threshold), green for adequate stock.
- This Week's Forecast: A simple, editable box showing the Tier 1 forecast for top 5 essential commodities with adjustment sliders.
- Quick Actions: Large buttons for 'Stock Count', 'Place Order', 'View Pending Syncs'.
- Sync Status Bar: Always visible at top of screen, showing number of pending uploads/downloads and last sync time.

Order Adjustment Screen

Key elements:

- System Recommendation: Clearly displays the Tier 1 forecast and the reasoning (3-month average, seasonal adjustment, storage constraint).
- Adjustment Slider/Input: Allows user to easily increase or decrease the order quantity. Slider has min/max bounds based on storage capacity.
- Override Reason Dropdown: Mandatory field with options: Disease Outbreak, Delivery Delay, Budget Change, Clinical Judgment, Other (with free text).
- District Insights (Optional): Small collapsible section showing Tier 2 statistical forecast for context if available from last sync.
- Print Paper Order Button: Generates the paper form matching HMIS 105 format for physical records.

Sync & Conflict Resolution Screen

Key elements:

- Simple List: Shows sync items as Pending (yellow), Successful (green), Failed (red).
- For Conflicts: A clear message: 'Your local change was saved. The district suggestion was logged for review.' This embodies the Local Wins principle without technical jargon.
- Retry All Button: For failed syncs, allows user to manually retry without waiting for automatic backoff.

District Dashboard (Pharmacists)
Key elements:

- Cached Map View: Shows facility status using pre-downloaded map tiles. Facilities color-coded by stock status.
- Trend Graphs: Simple line charts for stock levels and consumption patterns across facilities.
- Override Log: Accessible to managers to see the 'why' behind order changes, fostering accountability and learning rather than punitive oversight.

TECHNICAL SPECIFICATIONS

Function	Implementation Detail
Development Framework	Native Android (Kotlin/Java). Minimum SDK: Android 8.0 (API level 26).
Offline Storage	SQLite in WAL mode (`PRAGMA journal_mode=WAL; PRAGMA synchronous=NORMAL;`). Schema mirrors central PostgreSQL database for seamless sync.
Data Sync Protocol	RESTful JSON over HTTPS (TLS 1.3). Batched, compressed (GZIP) payloads. Automatic retry with exponential backoff (30s initial, 15min max).
Security	AES-256 encryption for local database using Android Keystore System. TLS 1.3 for data in transit. Bcrypt for password hashing.
Battery Optimization	Background sync only when battery >20% AND device not in active use. Manual sync bypasses these checks.
UI Responsiveness	Single-column layouts for all screens. Minimum supported: 5-inch display (480x800px). Adaptive sizing using ConstraintLayout with density-independent pixels (dp). Touch targets: 48dp x 48dp minimum. Tested on: Samsung Galaxy A series, Tecno Spark series, Infinix Hot series.
Offline Credential Expiry	90-day offline validity. Warning at 75 days. Credential refresh occurs during each successful sync.

CHANGE MANAGEMENT & CAPACITY BUILDING

- Training Focus: How to use the app when the internet is down. Scenario-based training on overrides (e.g what to do during a malaria outbreak).
- Digital Literacy Support: Embedded video guides and interactive tutorials within the app itself. Text instructions use simple, jargon-free language.
- Phased Rollout: Start with facilities that conduct weekly counts (baseline showed they are more successful) to build early wins and champions.

Addressing Stakeholder Concerns
Based on November 2025 validation feedback:

- Frontline Worker Burden: Auto-save eliminates explicit save actions. Single-tap order adjustments reduce cognitive load. Paper backup ensures staff aren't forced to abandon familiar workflows.
- System Integration: Opportunistic sync eliminates duplicate entry across multiple systems. Facility staff only use this app; integration happens automatically in background.

- Trust Building: Local edits always win policy shows system trusts health workers. Override logs foster learning, not punishment. Paper backup serves as trusted audit trail.

CONCLUSION

This offline-first design is not a fallback or compromise. It is the primary architecture, deliberately chosen to match Uganda's operational reality. By placing core functionality on the device, encrypting data with hardware-backed security, maintaining paper-digital harmony, and trusting health workers to override system recommendations, we create a system that works with the grain of existing workflows rather than against them.

The system operates at full capacity with zero connectivity, and gains additional insights when connectivity permits. This is resilience by design.

Document Version: Final (post-technical validation)
Date: November 2025
Authors: Gideon Abako, Timothy Kavuma, International Foundation for Recovery & Development
Validator: Ojok Ivan, Kyambogo University Department of Data Science, Networks & Artificial Intelligence

DOCUMENT REVISION HISTORY

Version	Date	Changes
1.0	Oct 2025	Initial workflow specification and wireframes based on baseline assessment
2.0	Nov 2025	Posts-validation revision incorporating: - SQLite WAL mode specification with PRAGMA commands - Android Keystore System implementation for AES-256 encryption - Complete data archiving and purging policy (12-month retention, automated monthly archiving) - Tier 2 forecast storage clarification (separate JSON files, informational only) - Battery optimization conditions (>20%, not in active use) - Offline credential management with 90-day expiry policy - UI responsiveness specifications (5-inch minimum, tested devices) - Stakeholder concern responses added to change management section