

## TECHNICAL SECURITY BRIEF

# Care Scan Security and Local Deployment

---

*Architecture, data locality, security controls, operational responsibilities, and residual risk for facility IT*

**Prepared for:** Facility IT, Information Security, Privacy, and Clinical Operations

**System basis:** Care Scan repository and deployment configuration

**Document date:** September 14, 2026

---

**Bottom line** Care Scan is designed as a facility-hosted, offline-first edge system. Core rounds, local administration, synchronization, reporting, and the authoritative database operate on an on-site appliance and do not require a public-cloud service. “Local” reduces external dependency and data movement, but does not eliminate the need for network segmentation, endpoint trust, physical security, backups, patching, monitoring, and formal pilot acceptance.

## 1. Purpose and assurance boundary

This document explains how Care Scan protects facility data and why the core system is local. It is written for an IT/security review and describes the current design and repository implementation as of the document date. It is not a penetration-test report, regulatory certification, business associate agreement, or guarantee that every deployment is secure regardless of configuration.

**Current maturity** The project README characterizes the current 1.0.20 release as a controlled pilot under validation. Controls described as requirements or release gates must be validated on the exact pilot build and installation before approval; this document is not a penetration-test report, regulatory certification, or production approval.

## 2. What “local” means

The facility edge appliance—currently a supported 64-bit Raspberry Pi—is the authoritative server for facility configuration, synchronized scan events, schedules, audit history, the web portal, and local reporting. PostgreSQL, the application API, scheduler, reverse proxy, and backup service run as a local container stack. Scanners communicate with this appliance over facility-controlled or appliance-managed local networking.

- Public internet availability is not required for routine scan capture. The handheld writes an event to a durable local outbox before showing it as saved.
- Public internet availability is not required for local portal access, event synchronization, scheduling, audit review, or on-appliance reporting.

- Public cloud and EHR/PCC integration are described as future, governed adapters—not dependencies of core rounds.
- The appliance can start from preloaded ARM64 container images without contacting a registry.
- Updates are transferred as signed offline packages and uploaded by an administrator through the local portal.

Local does not necessarily mean air-gapped. A deployment may use outbound DNS and NTP, an optional SMTP relay for emailed reports, a remote-mounted encrypted backup target, or future integrations. Those paths are disabled or absent unless configured and must be reviewed separately.

### 3. Local data flow and trust boundaries

1. A staff member authenticates on an enrolled scanner and presents an NFC checkpoint tag. The tag contains an opaque random checkpoint identifier, not resident information.
2. The scanner records the selection locally with a UUID idempotency key and original device timing evidence. It flushes the durable outbox before presenting a saved state.
3. A background task sends queued events to the facility appliance. Workflow input and NFC/client clocks are treated as untrusted; the server revalidates credentials, authorization, event shape, and domain rules.
4. The appliance commits accepted state, the canonical event, and audit evidence transactionally. Server receipt time is authoritative for audit ordering; duplicate retries return the original result.
5. Authorized staff use the HTTPS portal on the local appliance to administer devices and checkpoints, review activity, and generate reports.
6. Validated, encrypted backups are written locally and optionally copied to a separately mounted removable or remote destination.

**Data minimization** NFC tags identify locations or assets using opaque identifiers. They do not store resident records. Diagnostic output is designed to omit Wi-Fi passwords and device credentials, and sensitive setup values are excluded from API reads and audit metadata.

### 4. Security control summary

| Control area      | Care Scan design / implementation                                                                                                                                                                                 | IT implication                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Network transport | Production portal traffic is redirected from HTTP to HTTPS. Nginx permits TLS 1.2/1.3, disables session tickets, publishes HSTS, and uses factory-issued certificates under the shared Care Scan private root CA. | Install and verify the Care Scan root CA only on authorized endpoints; monitor certificate expiry. |
| Browser security  | Secure/HttpOnly/SameSite=Strict session cookies, CSRF tokens, no-store authentication pages, CSP, X-Frame-Options DENY, and no-referrer policy.                                                                   | Ensure production enables secure cookies and users access the HTTPS hostname.                      |

| Control area       | Care Scan design / implementation                                                                                                                                                              | IT implication                                                                                       |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Authentication     | Random per-appliance bootstrap credentials, 12-hour portal sessions, password hashing with salt, five-failure/15-minute application lockout, and Nginx login rate limiting.                    | Integrate account lifecycle with facility procedures; verify password and session policy acceptance. |
| Authorization      | Role-based portal permissions and explicit administrator approval for scanner enrollment. Suspended users lose sessions; revoked scanners cannot upload or refresh configuration.              | Assign least privilege and review administrator, DON, auditor, support, supervisor, and staff roles. |
| Scanner identity   | Factory Ed25519 identity, manufacturer-root validation, nonce replay rejection, pending discovery, printed-identity comparison, unique operational credential, revocation, and audit trail.    | Protect manufacturer trust material and perform the physical serial comparison during enrollment.    |
| Integrity          | UUID idempotency prevents duplicate canonical events. Scan records are append-only; audit records are append-only, hash-chained, and protected from UPDATE/DELETE by database triggers.        | Monitor and preserve ledgers and include reconciliation in restore tests.                            |
| Secrets            | Per-appliance keys/tokens are generated from system randomness, stored with restrictive permissions, mounted read-only where possible, and sensitive persisted state is encrypted.             | Protect recovery bundles and escrow keys separately from the appliance.                              |
| Workload isolation | Containers use no-new-privileges; API and scheduler filesystems are read-only with narrow writable mounts. The web container has no Docker or root access.                                     | Harden the host OS and restrict administrative access to the appliance.                              |
| Updates            | Signed .csu packages, pinned public verification key, SHA-256 manifest/digest checks, preflight, recent-backup requirement, staged install, health check, retained prior images, and rollback. | Keep the signing private key offline; archive SBOM and vulnerability-scan evidence per release.      |
| Backups            | PostgreSQL custom-format dumps are validated, AES-256 encrypted with an appliance-unique key, checksummed, and retained for 14 days by default.                                                | Use separate media/storage, protect the key, and run isolated restore drills.                        |

## 5. Network and infrastructure model

### Recommended topology

The preferred deployment connects the appliance to the facility by Ethernet and lets the appliance manage a private Wi-Fi network for scanners. This contains scanner traffic, reduces dependence on facility Wi-Fi changes, and gives IT a clear boundary around the edge appliance. A Wi-Fi-only appliance mode is supported but requires staged change management so enrolled scanners receive the replacement profile before the old network is removed.

- Place the appliance in a dedicated VLAN or otherwise restricted server/IoT segment.
- Permit administration only from authorized management endpoints and required scanner paths.
- Avoid guest networks that block necessary client-to-client traffic or expose scanners to untrusted peers.
- Use DHCP reservation and DNS/mDNS policy appropriate to the site; care-scan.local is the default facility hostname.
- Restrict outbound access to approved DNS/NTP, SMTP, backup, and support destinations. Core operation does not need general internet egress.

### Bootstrap and recovery exposure

On first boot the appliance requests Ethernet DHCP. If no wired lease is obtained within a bounded interval, it starts a restricted temporary setup access point at 192.168.4.1. Access requires a unique per-appliance setup secret; production application and clinical APIs are not available on that AP, and successful setup shuts it down. Re-enabling it after commissioning requires a physical recovery action and the appliance secret. Authorized service USB provides a final recovery path; SSH is key-only with root and password login disabled.

## 6. Data storage, retention, and recoverability

| Control area     | Care Scan design / implementation                                 | IT implication                                                         |
|------------------|-------------------------------------------------------------------|------------------------------------------------------------------------|
| Facility records | Authoritative PostgreSQL storage on the local appliance.          | Define retention, legal hold, access, and decommissioning procedures.  |
| Scan evidence    | Append-only local scan ledger with device/idempotency uniqueness. | Treat as sensitive operational record; reconcile counts after restore. |
| Audit evidence   | Append-only, hash-chained local audit ledger.                     | Limit access and preserve chain evidence in backup/restore procedures. |

| Control area     | Care Scan design / implementation                                                                       | IT implication                                                                            |
|------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Scanner queue    | Durable LittleFS outbox retains pending/synced/conflict/failed state and acknowledgement provenance.    | Lost devices may contain queued data; revoke promptly and apply physical/device security. |
| NFC tags         | Opaque random identifiers only; no resident data.                                                       | Manage tags as location credentials; cloned tags remain a residual risk.                  |
| Backups          | Encrypted, validated database dump; 14-day default retention; optional second copy on separate storage. | A second copy on the same storage device is not disaster recovery.                        |
| Logs/diagnostics | Correlation and operational details with sensitive-field exclusions; logs are size-limited.             | Forward only if approved; confirm no sensitive data enters local support workflows.       |

Suggested initial recovery objectives are a 24-hour recovery point objective (RPO) and four-hour recovery time objective (RTO). The pilot owner must formally accept or replace these targets. The recommended production platform uses qualified durable storage, a UPS or managed shutdown, validated cooling, clock monitoring, and a spare/replacement procedure.

## 7. Availability and offline behavior

Care Scan separates local capture from network delivery. NFC reading, touch input, staff feedback, and ending a round do not wait on an HTTP response. Reboots return interrupted uploads to pending without changing their UUIDs or event facts. Retries use ordered delivery and bounded exponential backoff. The server accepts exact duplicates idempotently and rejects reuse of the same idempotency key for different facts.

**Availability boundary** During an appliance outage, scanners can temporarily preserve new work locally, but canonical ingestion, supervisor dashboards, portal functions, and shared synchronization degrade. The appliance is a single failure domain. Care Scan is not an emergency alert or life-safety system, and downtime procedures remain required.

## 8. IT deployment and acceptance requirements

### Successful deployment prerequisites

Before installation, the facility IT team should reserve the physical network and wireless capacity needed for the Care Scan appliance and dedicated Android scanners. The following items are required for a successful deployment:

- One available Power over Ethernet (PoE) port on the facility network switch for the Care Scan appliance, with the port assigned to the approved server/IoT or Care Scan network segment.
- One dedicated Wi-Fi access point for the Care Scan scanners. The access point must provide reliable coverage in every rounding area and allow scanners to communicate with the local Care Scan server at care-scan.local.
- Firewall, client-isolation, VLAN, DNS/mDNS, and wireless policies that permit the dedicated scanners to reach care-scan.local and the required Care Scan service ports. Guest Wi-Fi or an access point that blocks client-to-client traffic is not suitable.
- A documented SSID and security configuration for the dedicated scanner network, with coverage and roaming tested from all planned scanner locations before enrollment.

**IT handoff checklist** Have the PoE switch port, dedicated scanner access point, approved SSID/security settings, and care-scan.local reachability ready before the installation appointment. Care Scan scanners should not be enrolled until the network path has been tested from the areas where rounds will occur.

- Review the exact production build, version, SBOM, vulnerability scan, signed release evidence, and documented exceptions.
- Place the appliance in protected physical space; record serial, storage model, image version, hostname, installation date, and key custodian.
- Use qualified durable storage, validated power/cooling, and preferably a UPS or managed shutdown.
- Approve the network segment, firewall policy, DNS/mDNS behavior, DHCP reservation, NTP source, and any allowed outbound services.
- Install the shared Care Scan root CA on authorized admin devices through managed trust distribution and verify its fingerprint out-of-band.
- Confirm secure cookies, production mode, unique passwords/tokens, key-only SSH, disabled root/password SSH, and no development fixtures/defaults.
- Enroll scanners by comparing discovered and printed identities; test revocation and replacement while preserving historical attribution.
- Configure separate encrypted backup storage, escrow the backup key separately, and complete an isolated restore/reconciliation drill.
- Monitor API/database health, disk use (>80%), backup age, clock skew, certificate expiry, scanner last-seen age, pending events, and container restarts.
- Document account lifecycle, incident response, lost-device response, downtime procedure, RPO/RTO, retention, decommissioning, and support access.
- Complete power-loss, network-loss, storage, thermal, capacity, update/rollback, certificate, and recovery acceptance tests.
- Obtain clinical, privacy, compliance, and risk-owner approval for the pilot and all residual risks listed below.

## 9. Residual risks and limitations

| Control area     | Care Scan design / implementation                                                                                                  | IT implication                                         |
|------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Product maturity | The repository states the system is not yet suitable for clinical or production use. Controls require build-specific verification. | Owner acceptance and mitigation required before pilot. |

| Control area            | Care Scan design / implementation                                                                                                                                                                                                                                                                      | IT implication                                         |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Legacy HTTP exception   | The formal threat model records legacy scanner HTTP access as a release exception during migration, while current handheld documentation specifies provisioned-CA HTTPS with no insecure fallback. Pilot approval must confirm that every deployed scanner uses the intended HTTPS/CA-validation path. | Owner acceptance and mitigation required before pilot. |
| Private CA operations   | Authorized browsers must trust the shared Care Scan root CA. Incorrect trust distribution or fingerprint verification can enable interception or operational failure.                                                                                                                                  | Owner acceptance and mitigation required before pilot. |
| Physical compromise     | Theft of an unlocked appliance can expose local data unless physical controls and optional full-disk encryption are appropriate to unattended-boot requirements.                                                                                                                                       | Owner acceptance and mitigation required before pilot. |
| NFC cloning             | Tags prove possession of an identifier at a location, not cryptographic presence. Anomaly review and physical inspection are still required.                                                                                                                                                           | Owner acceptance and mitigation required before pilot. |
| Disconnected revocation | A disconnected scanner cannot receive revocation immediately; offline authorization windows must be defined and accepted.                                                                                                                                                                              | Owner acceptance and mitigation required before pilot. |
| Local denial of service | Segmentation and rate controls reduce exposure but do not eliminate facility-LAN denial of service, power loss, hardware failure, or deliberate physical disruption.                                                                                                                                   | Owner acceptance and mitigation required before pilot. |
| Single appliance        | The edge appliance is a single failure domain. Scanner outboxes provide temporary capture continuity, not full high availability.                                                                                                                                                                      | Owner acceptance and mitigation required before pilot. |
| Optional egress         | SMTP, remote backup, support, or future integration changes the data-flow boundary and requires an additional security/privacy review.                                                                                                                                                                 | Owner acceptance and mitigation required before pilot. |
| Not life safety         | The system supports care-round documentation; it is not an emergency alert system. Clinical operations must maintain independent escalation and downtime procedures.                                                                                                                                   | Owner acceptance and mitigation required before pilot. |

## 10. Recommended IT decision statement

Care Scan may be evaluated as a facility-hosted edge application whose core workflow and authoritative data plane remain local by default. Conditional pilot approval should require completion of the deployment

checklist, closure or explicit acceptance of release exceptions, verification of HTTPS and appliance trust on every endpoint, tested encrypted backup/restore, network and physical controls, and confirmation that the exact release meets the facility's security, privacy, clinical, and operational requirements.

## Appendix A — Evidence basis

The statements in this brief were derived from the following repository artifacts. IT should review the exact released artifacts and configuration because implementation and documentation may change.

**README.md** — product status, local architecture, onboarding, production image, and deployment caveats

**docs/03-ARCHITECTURE.md** — system context, trust boundaries, offline model, enrollment, and security architecture

**docs/11-HANDHELD-SYNC.md** — durable outbox, retry/idempotency, time semantics, device credentials, and CA validation

**docs/12-PRODUCTION-OPERATIONS.md** — health monitoring, backup/restore, update/rollback, recovery, and physical appliance operations

**docs/13-SECURITY-THREAT-MODEL.md** — primary threats, implemented/planned controls, release exception, and residual risks

**adr/0001-offline-first.md** — offline-first decision, consequences, and delayed-revocation tradeoff

**adr/0002-raspberry-pi-primary-server.md** — facility-hosted authority, public-cloud independence, appliance tradeoffs, and release gates

**compose.yaml** — container services, no-new-privileges, read-only filesystems, health checks, secrets mounts, and backup service

**deploy/nginx/nginx-production.conf** — HTTPS redirect, TLS versions, HSTS, request limits, and login rate limiting

**deploy/README.md** — production image, SSH policy, setup networking, filesystem privilege boundary, and encrypted backups

**deploy/security/care-scan-init-secrets** — per-appliance secret generation and filesystem permissions

**database/schema.sql** — credentials/sessions, scanner identity, append-only ledgers, and database immutability triggers

**backend/internal/web/auth.go** — login logout, session cookies, CSRF, password derivation, and trust-anchor presentation

**backend/internal/web/server.go** — browser security headers and request handling

**backend/internal/web/persistence.go** — transactional persistence, audit hash chaining, and encrypted sensitive state

**scripts/release-security-check.sh** — release digest, SBOM, and vulnerability-scanning requirements

## Appendix B — Definitions

**Edge appliance:** The on-site Raspberry Pi that runs the API, portal, scheduler, database, reverse proxy, backup process, health functions, and update agent.

**Offline-first:** The scanner durably records work locally before network acknowledgement and synchronizes it later without creating duplicate canonical events.

**Authoritative:** The system component that determines the canonical facility state and audit ordering; for synchronized Care Scan data, this is the local edge appliance/PostgreSQL database.

**Care Scan root CA:** The shared private trust anchor used to verify factory-issued HTTPS certificates across Care Scan appliances.

**Idempotency key:** A stable UUID attached to a client event so an exact retry returns the original result rather than creating a duplicate.

**RPO / RTO:** Maximum acceptable data-loss interval / target time to restore service after a failure.