

Setup & Security Checklist

Complete one product-specific checklist for the subscribed product, followed by the common checklist required for every product.

Document No.	CAV-SC-2026-001-EN	Select model
Version	1.0	
Issue Date	September 3, 2026	Verify security
Product	CAVIINET	
Intended Users	Hospital administrator, security/IT lead, deployment support	Prove recovery
Classification	Public Setup Checklist	

00

Separate product-specific items from common items

Confirm the subscribed product first, then complete its one product page and every common page.

Organization and verification information

Organization	_____	Installation site	_____
Administrator	_____	Security/IT lead	_____
Install date	_____	Product version	_____

CHECK STATUS

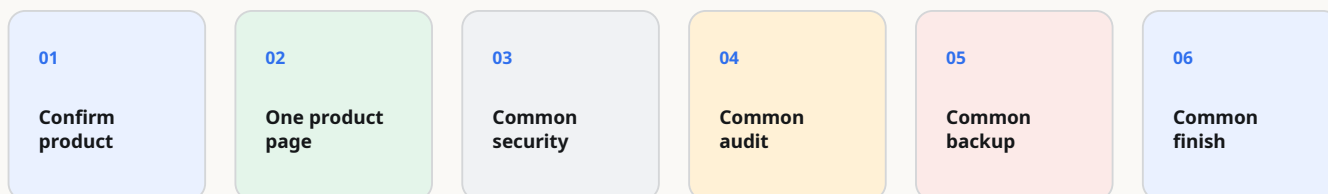
☒ Done☐ Review☐ N/A

Figure 1. Product-specific and common checklist sequence

WHICH PAGES SHOULD YOU COMPLETE?

Pages 4-6 are product-specific. Complete only the one page for the subscribed Single PC, Host/Client, or NAS Server product. Pages 7-10 are common and must be completed for every product.

Check the **PRODUCT-SPECIFIC** or **COMMON CHECKLIST** label at the top of each page before completing it.

- Do not complete all three product pages. Select only the page for the subscribed product.
- Patient-data security, audit evidence, backup, and recovery are common to every product.
- Use a demo patient and demo content, and retain observable verification evidence.

01

Confirm the subscribed CAVIINET product first

These are three separate products. Select the one that matches the contract or license.

PRODUCT CHECKLIST A · PAG☐

Single PC product

For small organizations. The application and all data operate on one designated PC.

Subscribed product: Single PC

PRODUCT CHECKLIST B · PAG☐

Host/Client product

For mid-sized organizations. Staff use Clients while all data remains only on the designated Host.

Subscribed product: Host/Client

PRODUCT CHECKLIST C · PAG☐

NAS Server product

For large organizations. Staff connect directly to NAS and all data remains only on NAS.

Subscribed product: NAS Server

Figure 2. Selecting a CAVIINET operating model by organizational scale

Decision factor	Single PC	Host/Client	NAS Server
Primary users	One designated PC	Multiple staff members	Staff across departments
Data location	Designated PC	Host PC only	NAS Server only
Data on staff PCs	PC is the storage system	None	None
Recommended scale	Small	Mid-sized	Large or multi-site
Additional protection	External backup required	Host backup required	Snapshots and immutability

Table 1. Operating-model selection criteria

CHECKLIST COMPLETION SCOPE

Complete only one product-specific page from pages 4-6. Pages 7-10 are the common checklist and must be completed by organizations using Single PC, Host/Client, or NAS Server.

PRODUCT A

Single PC Product Checklist

Complete this page only if the organization subscribed to the Single PC product. Verify that the application and data storage operate together on one designated PC.

SUBSCRIBED PRODUCT

Single PC product · application and data operate together on one designated PC

SINGLE PC ONLY

Status

☐ Done

☐ Review

☐ N/A

Area	Verification item	Done	Review	N/A
Operating device	● One designated PC has been selected for CAVIINET.	☐	☐	☐
	● The application is used only on that PC, with no Client connection.	☐	☐	☐
Data location	● The managed location for patient photos, consent records, and personal information is confirmed.	☐	☐	☐
	● No patient information remains on the desktop, in Downloads, or in other unmanaged folders.	☐	☐	☐
Account & access	● The administrator account and a secure password are configured.	☐	☐	☐
	● The Recovery Code is stored securely away from the operating PC.	☐	☐	☐
Patient workflow	● A demo patient can be registered, an image saved, and a consent record opened successfully.	☐	☐	☐
Audit evidence	● View, edit, and signature actions for the demo patient appear in the audit record.	☐	☐	☐
Backup	● The initial full backup and a recurring scheduled backup are configured.	☐	☐	☐
Recovery	● A deleted demo patient and image were restored and opened successfully.	☐	☐	☐
Restart	● Single PC mode, data, and backup settings persist after restart.	☐	☐	☐
Ownership	A responsible person is assigned to review backup status and storage capacity.	☐	☐	☐

Critical items must be completed before production use.

Verification notes and corrective actions

Reviewed by

Date

PRODUCT B

Host/Client Product Checklist

Complete this page only if the organization subscribed to Host/Client. Verify that staff work from Clients while all data remains only on the designated Host PC.

SUBSCRIBED PRODUCT

Host/Client product · Clients perform work while all data remains only on the Host

HOST/CLIENT ONLY

Status ☐ Done ☐ Review ☐ N/A

Area	Verification item	Done	Review	N/A
Host selection	The administrator's designated Host PC has been confirmed.	☐	☐	☐
	The Host remains powered on, stable, and available during operating hours.	☐	☐	☐
Network	The Host and all Client PCs are connected to the authorized hospital network.	☐	☐	☐
Client connection	Each Client connects to the intended Host PC successfully.	☐	☐	☐
Data boundary	All patient data created from Clients is stored on the Host.	☐	☐	☐
	No patient data remains on Client desktops, Downloads folders, or local storage.	☐	☐	☐
Accounts	Doctors, nurses, and counselors use individual rather than shared accounts.	☐	☐	☐
Roles	Each role is limited to the patient information and functions required for the job.	☐	☐	☐
Workflow test	A demo patient, image, and consent created from a Client are visible on the Host and another authorized Client.	☐	☐	☐
Audit evidence	The Client user's account, time, target, action, and result appear in the audit record.	☐	☐	☐
Backup	Full, incremental, and scheduled Host backups are configured and show success.	☐	☐	☐
Recovery	A demo patient and image were restored from a Host backup.	☐	☐	☐
Restart	Host mode and Client connections persist after restart.	☐	☐	☐
Device handling	Loss, repair, or replacement of a Client PC does not expose local patient files.	☐	☐	☐

Critical items must be completed before production use.

Verification notes and corrective actions

Reviewed by

Date

PRODUCT C

NAS Server Product Checklist

Complete this page only if the organization subscribed to NAS Server. Verify that staff connect directly to NAS with no Host PC and all data remains only on NAS.

SUBSCRIBED PRODUCT

NAS Server product · all staff connect directly to NAS with no Host PC

NAS SERVER ONLY

Status

☐ Done

☐ Review

☐ N/A

Area	Verification item	Done	Review	N/A
Model	NAS Server mode is selected and no Host PC is used as the data store.	☐	☐	☐
Connection	The NAS address or IP, port, and HTTPS setting are correct.	☐	☐	☐
Storage	The shared folder and UNC path are verified and a dedicated CAVIINET location is selected.	☐	☐	☐
Permissions	The NAS connection account has only the required read/write permissions.	☐	☐	☐
TLS	The certificate and fingerprint are verified as a trusted connection.	☐	☐	☐
Connection test	Test and Save succeeds for connection, sign-in, and storage access.	☐	☐	☐
Data boundary	All data created by staff PCs is written directly to NAS.	☐	☐	☐
	No patient information remains on doctor, nurse, or counselor PCs.	☐	☐	☐
Accounts & roles	Every staff member has an individual account and least-privilege role.	☐	☐	☐
Workflow test	A demo patient, image, and multilingual consent are stored on NAS and open for authorized users.	☐	☐	☐
Audit evidence	Patient, configuration, and backup actions in NAS mode appear in audit records.	☐	☐	☐
Snapshots	The snapshot schedule and retention standard are configured.	☐	☐	☐
Immutability	An immutable-retention period prevents unauthorized change or deletion.	☐	☐	☐
Recovery	Demo data was restored from a snapshot or backup.	☐	☐	☐
Restart	NAS connection details and the operating mode persist after restart.	☐	☐	☐

Critical items must be completed before production use.

Verification notes and corrective actions

Reviewed by

Date

COMMON 01

[COMMON] Verify global patient-data security for every product

Required for Single PC, Host/Client, and NAS Server. Verify storage boundaries and access rights for photos, multilingual consent, and personal information.

Status

☐ Done

☐ Review

☐ N/A

Area	Verification item	Done	Review	N/A
Classification	Patient photos, consent records, and personal information are classified as sensitive information requiring strong protection.	☐	☐	☐
Centralization	Patient information previously scattered across PCs has been identified and moved to the designated store.	☐	☐	☐
Unmanaged copies	No separate copies remain on desktops, personal folders, removable drives, or personal cloud storage.	☐	☐	☐
Accounts	Every user signs in with an individual account and does not share credentials.	☐	☐	☐
Least privilege	Each user can access only the patient information and functions required for the assigned work.	☐	☐	☐
Admin access	Administrator and operational-staff privileges are clearly separated.	☐	☐	☐
Offboarding	An owner and process exist to promptly disable accounts for departed employees, employees on leave, or inactive users.	☐	☐	☐
Screen security	Automatic screen lock and physical access control apply to PCs in shared areas.	☐	☐	☐
Export	Approval rules exist for exporting, copying, or externally transferring patient information.	☐	☐	☐
Recovery Code	The Recovery Code is stored away from operating devices and accessible only to authorized administrators.	☐	☐	☐
Device lifecycle	A process confirms that no local patient files remain before repair, replacement, or disposal.	☐	☐	☐
Periodic review	An owner and schedule are defined for recurring account, permission, and storage reviews.	☐	☐	☐

Critical items must be completed before production use.

Verification notes and corrective actions

Reviewed by

Date

COMMON 02

[COMMON] Evidence for every action reveals cause and accountability fast

Required for every product. Connect patient-data and system actions to the actor, time, target, and result so the facts can be reconstructed.

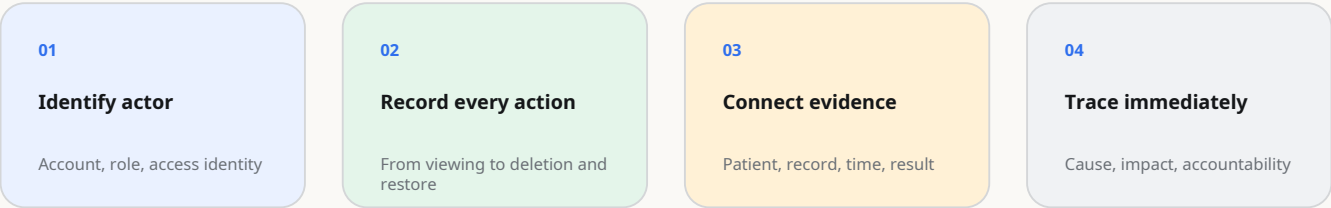


Figure 3. Turning operational actions into accountable evidence

Status ☒ Done ☐ Review ☐ N/A

Area	Verification item	Done	Review	N/A
Patient data	Create, view, edit, delete, and export actions are recorded separately.	☐	☐	☐
Actor	The user account, role, and access identity can be identified.	☐	☐	☐
Time & device	The exact time and device or access location can be identified.	☐	☐	☐
Target	The affected patient, image, consent record, or setting can be identified.	☐	☐	☐
Consent & signature	Document type, language, patient review, e-signature, and completion state are connected.	☐	☐	☐
Access changes	Sign-in, role, permission, and security-setting changes are recorded.	☐	☐	☐
Data protection	Backup, restore, and migration retain operator, time, target, and result.	☐	☐	☐
Result	Success, failure, and resulting changes can be reviewed for each action.	☐	☐	☐
Access control	Only authorized administrators can review audit records.	☐	☐	☐
Incident trace	A demo incident was reconstructed to show who handled what, when, and how.	☐	☐	☐

EXPLAIN WITH RECORDS, NOT MEMORY OR ASSUMPTION

Audit evidence helps identify cause, impact scope, and accountability quickly while objectively demonstrating the organization's response and recovery actions.

COMMON 03

[COMMON] Verify actual recovery, not merely backup-file presence

Required for every product. Run full, incremental, and scheduled backups, then restore and open demo patient data successfully.

COMMON TO ALL PRODUCTS

Single PC, Host/Client, and NAS Server must all verify backup and demo-data restore

COMMON · RECOVERY

Status ☒ Done ☐ Review ☐ N/A

Area	Verification item	Done	Review	N/A
Full backup	The initial full backup includes the demo patient, images, and consent records.	☐	☐	☐
Incremental	Changes made after the previous backup appear in the next backup.	☐	☐	☐
Scheduled backup	The schedule is configured and the automatic run shows success.	☐	☐	☐
Persistence	Backup schedules and history persist after application and device restart.	☐	☐	☐
Backup access	Backup location and administrator access are appropriately restricted.	☐	☐	☐
Restore test	A demo patient was deleted and then restored from backup.	☐	☐	☐
Data review	Restored patient information, images, and consent records open and match the source.	☐	☐	☐
Operation	The selected operating mode and authorized access work after restoration.	☐	☐	☐
NAS protection	For NAS, snapshots and immutable retention operate according to configuration.	☐	☐	☐
Migration	If an operating-location change is planned, migration between Local Server and NAS has been verified.	☐	☐	☐
Failure response	An owner is assigned to review backup failure, low capacity, or connection loss.	☐	☐	☐
Recurring test	A schedule and evidence method are defined for repeating restore tests.	☐	☐	☐

Critical items must be completed before production use.

Verification notes and corrective actions

Reviewed by

Date

COMMON 04

[COMMON] Confirm the subscribed product and essential settings

Confirm that one applicable product checklist and every common checklist page have been reviewed without omission.

☐ Subscribed product One subscribed product is confirmed: Single PC, Host/Client, or NAS	☐ Data boundary Data remains only on the designated PC, Host, or NAS	☐ Accounts & roles Individual accounts and least privilege are applied
☐ Patient workflow Registration, images, consent, and e-signature are completed successfully	☐ Audit evidence Actor, time, target, action, and result are visible	☐ Recoverability Demo data was restored successfully from backup

Figure 4. Essential CAVIINET setup-completion items

HOW TO CONFIRM SETUP COMPLETION

Verify each item using actual test screens, audit records, and restore results. Record anything that needs review below, complete the action, and verify the related checklist item again.

REVIEW AND ACTION NOTES

Record only incomplete items or details that require additional verification.

Item to review	_____
Required action	_____
Target date	_____

Complete any required action, then verify the related checklist item again.