SYMBEEO

PUBLIC

DESIGN STUDY

Clinical workplace for a hospital group: leavers designed to be cut in minutes, every workstation and room device in support

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Digital	Healthcare	Hospital group
DOCUMENT	**VERSION**	**DATE**
DIG-004	1.1	Oct 10, 2026

WRITTEN BY

Avinash Dhinakaran, Principal Integration Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	DIG-004	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Digital	Industry	Healthcare
Author	Avinash Dhinakaran	Role	Principal Integration Architect
Credentials	iSAQB Certified Professional for Software Architecture – Advanced Level (CPSA-A), Oracle Certified Consultant – Value Chain Planning, Master Data Management, SCM Cloud		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the standard owner's or vendor's own current page on Sep 24, 2026 · [S*] figure from the owner's page summary where the page itself could not be opened · [A] design assumption · [T] design target (the record's outcome figure and anything derived from it). Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Avinash Dhinakaran remains the author.

1 · Scope

Who it is for. The chief information officer or the head of end-user services of a hospital group whose staff move between wards, sites and shifts every day, whose shared workstations still run Windows 10 on paid extended updates, and whose meeting-room devices have lost their certification.

Typical buyer [A]. A hospital group of 4 hospitals, 6,500 staff, 1,400 shared clinical workstations on Windows 10 22H2 enrolled in Extended Security Updates year one, 60 Microsoft Teams Rooms on Android 10 and 11, one on-premises Exchange Server 2019 organization kept for patient-letter workflows, 12 clinical SaaS applications federated to the group's identity provider [A]. Staff turnover: 900 joiners and 900 leavers a year, plus 300 rotating resident doctors [A].

What is in. Joiner, mover and leaver propagation to every collaboration and clinical SaaS service; session revocation on disable; workstation and room-device lifecycle; mail platform decision; sanitization of replaced devices. **What is out.** The electronic health record's own access model; the identity provider product (SRA-SEC-001); clinical device networks (SRA-NET-001); the patient-letter application.

Assumptions. The collaboration suite is Microsoft 365 with Microsoft Entra ID as identity provider [A]. Each clinical SaaS application supports SCIM 2.0 inbound provisioning; 4 of 12 also accept Shared Signals Framework and CAEP events [A].

Related documents, read Sep 24, 2026. SRA-DIG-001, SDD-DIG-001, STP-DIG-001 v1.0 (issued Sep 27, 2026) · Continuous access evaluation in Microsoft Entra (https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation) · Extended Security Updates (ESU) program for Windows 10 (https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates) · Android versioning support for Teams devices (https://learn.microsoft.com/en-us/microsoftteams/devices/android-version-support) · Exchange Server 2019 and 2016 End of Support Roadmap (https://learn.microsoft.com/en-us/troubleshoot/exchange/administration/exchange-2019-2016-end-of-support) · OpenID Shared Signals, CAEP and RISC final specifications (https://openid.net/three-shared-signals-final-specifications-approved/) · SCIM 2.0 protocol, RFC 7644 (https://www.rfc-editor.org/rfc/rfc7644) · NIST SP 800-88 Rev. 2 (https://csrc.nist.gov/pubs/sp/800/88/r2/final).

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. Continuous access evaluation in Microsoft Entra	Microsoft · page dated Apr 8, 2026	Exchange, Teams and SharePoint Online subscribe to disable and password events; the goal is near real time, "latency of up to 15 minutes might be observed"; CAE sessions carry tokens of up to 28 hours. Microsoft calls CAE "an industry standard based on" OpenID CAEP, but documents no Shared Signals stream to or from its services (read Sep 27, 2026), so R6 falls under SRA-DIG-001 R15's second clause, the platform's own stated bound, not its 5-minute CAEP clause	https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation
Our own design, built from published documentation. Android versioning support for Teams devices	Microsoft · updated Sep 17, 2026	Android 10 and 11 certification ended Sep 3, 2026, Microsoft support ends Sep 3, 2027; Android 12 and 13 certified to Aug 15, 2028; Android 14 to Oct 4, 2029	https://learn.microsoft.com/en-us/microsoftteams/devices/android-version-support
Our own design, built from published documentation. Windows 10 ESU program	Microsoft · page dated Nov 17, 2025	ESU year one USD 61 per device, price doubling each year, three years at most; the business case in §4.3 is this price	https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates
Public deployment. A UK public hospital trust: shared iPads for clinical staff, managed in Microsoft Intune with single sign-on through Azure AD (now Microsoft Entra ID) into Teams	Microsoft customer story · Feb 8, 2023	§4.1 and §4.3: a hospital running shared clinical devices on the same identity and device platform. One trust, not a group, and iPads, not Windows workstations, so it settles the operating model only; no figure from it enters the register	https://www.microsoft.com/en/customers/story/1601658121961363219-milton-keynes-nhs-health-provider-microsoft-intune

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	6,500 staff · 1,400 shared workstations · 60 rooms · 12 clinical SaaS apps	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Joiner and mover reach every in-scope service	≤ 15 min, over SCIM 2.0	[S] RFC 7644; [T]
R3	Leaver loses access to clinical SaaS apps that receive CAEP	≤ 5 min, live sessions included	[S] OpenID CAEP; [T]
R4	Leaver loses access to clinical SaaS apps without CAEP	≤ 15 min, by SCIM deactivation and session expiry	[T]
R5	Access-token lifetime at those 8 apps	≤ 15 min	[T]
R6	Leaver loses access to Exchange, Teams and SharePoint Online	vendor figure: near real time, up to 15 min; SRA-DIG-001 R15's platform-stated bound, not its CAEP path	[S] Microsoft
R7	Workstation OS	Windows 11 on 1,400 of 1,400 before ESU year three	[T]
R8	ESU cost avoided	USD 61 per device year one, doubling: USD 122 year two, USD 244 year three	[S] Microsoft
R9	Room devices	Android 12 or later; certified to Aug 15, 2028 or later	[S] Microsoft
R10	Room devices past certification on Sep 24, 2026	60 on Android 10 and 11; certification ended Sep 3, 2026	[S] Microsoft; [A] count
R11	Mail	off Exchange Server 2019, unsupported since Oct 14, 2025; Exchange Server SE or the online service	[S] Microsoft
R12	Replaced devices	sanitized to NIST SP 800-88 Rev. 2, certificate per device	[S] NIST

Twelve rows; eight carry a vendor's or standard's figure (three with a design target or count beside it), one is a design assumption, three are design targets.

3 · Architecture overview

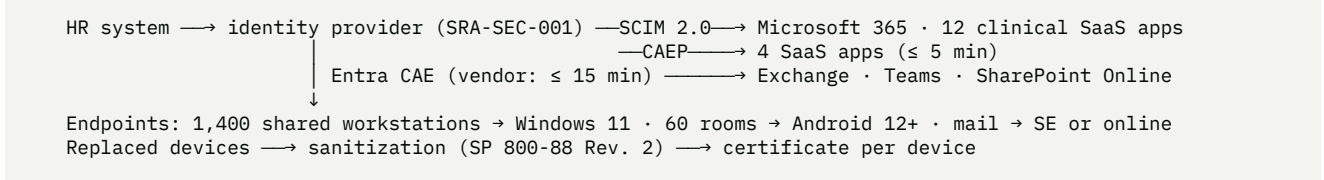


Figure 1. Workplace identity and device lifecycle

One identity source, three revocation paths with three stated times, one lifecycle floor. The parts table lists standards and support dates rather than hardware models.

© 2026 Symbeeo. All rights reserved. · Public

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Provisioning	SCIM 2.0, RFC 7644	13 connectors (Microsoft 365 + 12)	2,100 lifecycle events a year [A]	SRA-DIG-001 R14 [S]
Revocation, Microsoft services	Microsoft Entra continuous access evaluation	1 tenant	6,500 users	vendor-stated latency up to 15 min [S]
Revocation, other apps	OpenID Shared Signals Framework with CAEP, Final	4 receivers	—	Final since September 2, 2025 [S]
Workstation OS	Windows 11	1,400	—	Windows 10 support ended Oct 14, 2025 [S]
Room OS	Microsoft Teams Rooms on Android 12 or later	60	—	certified to Aug 15, 2028 [S]
Mail	Exchange Server SE or Exchange Online	1 organization	—	successor to 2019 [S]

4 · Design by subsystem

4.1 Provisioning.

The HR system is the source of joiners, movers and leavers; the identity provider pushes each change to 13 SCIM 2.0 connectors, target ≤ 15 min (R2) [T]. Rotating resident doctors are movers, not new identities, so their access follows the rota without a new account [A]. Rejected: nightly CSV imports per application — 24 h worst case (R2).

4.2 Revocation.

Three paths, three times, stated separately rather than averaged. Microsoft services: CAE, vendor figure up to 15 min (R6) [S]. The 4 clinical apps that receive CAEP: session-revoked event on disable, target ≤ 5 min (R3) [T]. The other 8: SCIM deactivation plus 15-minute access tokens, target ≤ 15 min (R4, R5) [T]. For a leaver flagged high-risk, service desk also revokes all refresh tokens at once [A].

4.3 Workstations.

1,400 shared workstations on Windows 10 ESU year one [A]. Year two costs USD 122 per device [S], USD 170,800 for the estate [A], and is paid; year three would cost USD 244 per device, USD 341,600 [A], so the upgrade to Windows 11 completes before year three starts (R7) [T]. Devices that cannot run Windows 11 are replaced [A]. Shared workstations sign in by badge tap to the identity provider [A].

4.4 Room devices.

60 room systems on Android 10 and 11 lost certification on Sep 3, 2026 and lose Microsoft support on Sep 3, 2027 [S]. Each is updated to certified Android 12 firmware where its maker publishes it, otherwise replaced (R9) [A]. Replacement order: rooms used for multidisciplinary team meetings first [A].

4.5 Mail.

Exchange Server 2019 has been unsupported since Oct 14, 2025 [S]. The group records one of two decisions (SDD-DIG-001 P8): in-place upgrade to Exchange Server SE on premises, which Microsoft describes as a cumulative upgrade to 2019 [S], or mailboxes to Exchange Online [S]. The patient-letter workflow's data-residency need decides it [A].

© 2026 Symbeeo. All rights reserved. · Public

4.6 Sanitization.

Every workstation, room device and mail-server disk leaving the group's control is sanitized to NIST SP 800-88 Rev. 2 with a certificate per device (R12) [S]; the certificates go into the handover pack (SDD-DIG-001 §8.5).

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
SCIM connector down	joiners lack access to that app; leavers still cut by CAEP or token expiry; connector alert ≤ 15 min	[A] SRA-DIG-001 F10
CAEP receiver rejects events	fall back to SCIM deactivation and 15-min tokens (R4)	[A]
Identity provider unreachable	new sign-ins fail, badge tap included; issued tokens valid to expiry; downtime procedure for clinical access	[A] SRA-DIG-001 F6
Room device firmware unavailable	device replaced; room booked out until then	[A]
Workstation upgrade fails	device reimaged or replaced; kept on ESU until then	[A]

6 · Limits

- R6 is Microsoft's stated figure, up to 15 minutes. Entra CAE is Microsoft's own implementation, described by Microsoft as based on CAEP, with no Shared Signals stream documented, so it is not the CAEP path of SRA-DIG-001 R15; it meets R15's other clause (≤ 15 min, the platform's own stated bound). The 5-minute figure applies only to the 4 apps that receive CAEP events (R3).
- Microsoft's page states CAE does not support guest accounts; visiting clinicians on guest accounts fall under R4, not R6.
- Which clinical SaaS apps accept CAEP is an assumption until each vendor confirms it at design.
- Room-device firmware availability is each device maker's decision, per Microsoft's page; the replacement count is not known until inventory.
- No figure here has been measured; every time and count is an assumption, a target or a vendor figure.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

8 · The author

WRITTEN BY

Avinash Dhinakaran

Principal Integration Architect

iSAQB Certified Professional for Software Architecture – Advanced Level (CPSA-A), Oracle Certified Consultant – Value Chain Planning, Master Data Management, SCM Cloud

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

DIG-004 · Version 1.1 · Oct 10, 2026