

Honeysuckle Care Management: Security &

Compliance Statement Oct 14, 2026

Honeysuckle Care Management uses HTTPS throughout; encrypts residents' identifying details, care notes, staff records and family-portal messages field by field in the database; encrypts every uploaded file; requires authenticator-app two-factor login for platform Super Admins and supports it for every other role; locks a sign-in name after repeated wrong attempts; asks for the password again before sensitive actions; isolates each care provider's data through a central route map that every request must pass; and records care and security activity, including every sign-in and every record opened, in a tamper-evident audit log. This statement sets out those controls in technical detail and maps them to the NHS Data Security and Protection Toolkit (DSPT), Cyber Essentials, DTAC and UK GDPR, so customers can use it as evidence for their own assessments. This revision (13 October 2026) covers everything changed since the first issue on 29 September 2026, most recently resident correspondence, staff signatures on invoices and each person's light/dark display choice; section 12.4 lists the fixes.

1. Service overview and architecture

Honeysuckle Care Management is a multi-tenant web application: one installation serves many care providers (tenants), with each tenant's data separated in software and checked on every request.

Layer	Technology	Notes
Client	Single-page web app (HTML, vanilla JavaScript, CSS)	Runs in any modern browser; no app install. No inline scripts or styles, so a strict Content Security Policy applies.
Web server	Apache with .htaccess security headers and deny rules	Only api.php and cron_alerts.php can be requested as PHP. Server code, uploads, quarantine, logs, libraries' server code, hidden files and data or backup files are refused. Hosting provider and data-centre location: see section 13.

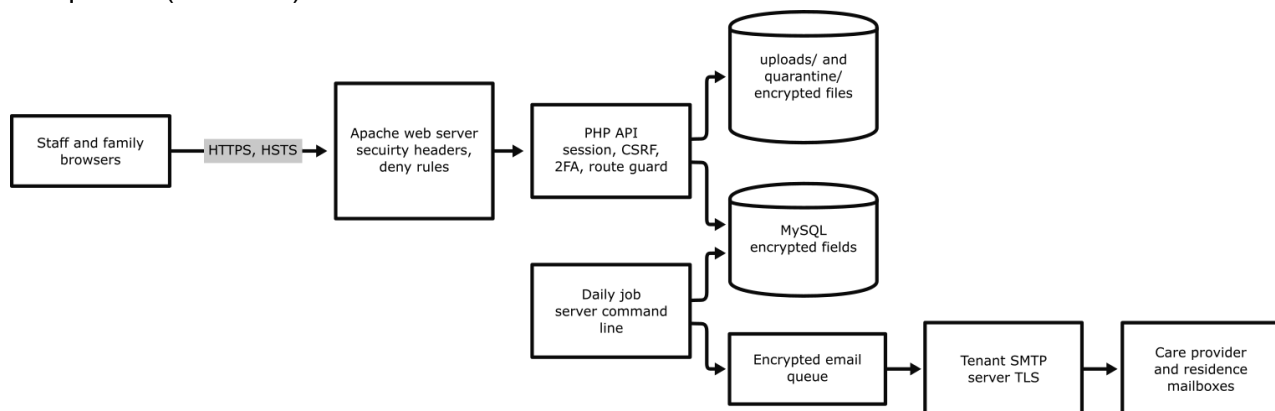
Application	PHP 8.4, single JSON API (api.php) with a central route map	Every action declares which roles may use it and which records the requester must own; the route guard refuses anything undeclared before any handler runs (section 4).
-------------	---	---

Layer	Technology	Notes
Database	Percona Server for MySQL 8.4.6-6	Accessed through PDO with native prepared statements.
File storage	Server file system (uploads/, quarantine/)	Uploaded files are encrypted when stored (section 3). Files removed from a record are kept encrypted in quarantine for the audit retention period (section 7).
Scheduled job	Daily job (cron_alerts.php), run from the server's command line	Four parts: alerts, housekeeping, invoicing and the email queue. It never deletes care records: records past retention wait for Admin approval (section 7). Housekeeping removes only items past their set period: audit entries and quarantined files beyond the audit retention period, and notifications after 90 days. No web token is configured, so it cannot be started over the web at all.

Email	PHPMailer 7.1.1 via each tenant's own SMTP server, through an encrypted outgoing queue	See section 9.
-------	--	----------------

No third-party scripts or tracking. Every JavaScript library is hosted on the same server, and pages load no scripts or stylesheets from other websites. There are no analytics, advertising or tracking services, and no personal data is sent to any third party by the application other than email sent through the care provider's own mail server (section 9). The app's icons are hosted on the same server too.

Tenancy model. All tenants share one database. Every record carries its tenant's ID, and requests are checked against the signed-in user's tenant on the server. Uploaded files are only served after the server looks up which tenant owns the file and confirms it matches the requester (section 4).



The browser only ever talks to the application server. The daily job runs on the server and sends alert emails through the tenant's own mail server.

2. Data held

The service holds health and care records, which are special category data under UK GDPR Article 9. The care provider is the data controller; Whitsend Studios processes the data on its behalf (Article 28).

Data subject	Data held	Stored encrypted
Residents	Name, NHS number, NI number, Adult Social Care number, finance reference, ethnicity, GP details, room number, emergency contacts	Yes: all listed text fields

Residents	Medical history, medications and dosages, allergies and reactions, dental records, appointments (with whom, reason, outcome)	Yes
-----------	--	-----

Residents Medication administration record (eMAR): each medicine's name, dose, instructions, when-required guidance and reason stopped; each dose recorded (what was given, notes, why a when-required dose was needed and its effect, who recorded and who witnessed it, why a record was struck through); controlled drug Yes (schedule times and days, dates, outcomes, quantities and balances are not)

Data subject	Data held	Stored encrypted
	register entries (notes, who recorded and witnessed)	
Residents	Daily care records (observations, care given, notes, plan for next shift), incidents (description, action taken, body-map locations, people involved), consent purposes	Yes
Residents	Care plans written in the app (content, reason for change, author), risk assessments (title and content), physiotherapy notes	Yes
Residents	Correspondence received about the resident (date received, who it was from, summary, notes)	Yes (the date is not)

Residents	Care plans, assessments, consent forms, correspondence and photos (uploaded files, and their original file names)	Yes: whole file encrypted
Residents	Financial entries (benefit and contribution names)	Names yes; amounts no
Residents and family	Family portal messages, updates and their photos, visit requests and staff notes, and each family member's recorded consent notes	Yes; photos whole file encrypted
Staff	Full name (including wherever it is recorded as the author of a record), contact number, email address, job title, LAS ID, car insurance provider, policy number and vehicle registration	Yes
Staff	Training and check records (reference, details, notes), rota entries (name, notes), and the profile kept for a leaver	Yes

Data subject	Data held	Stored encrypted
Staff and family	Username, role, password	Username and role no; password stored only as a bcrypt hash

Care provider	Registered office address, phone number, main contact, contact and accounts emails, accounts contact (name, email and number), bank account name, sort code and account number, SMTP username and password, invoice messages	Yes
Care provider	Invoice payment details (reference, notes, who recorded it), CQC evidence pack notes	Yes
Residences	Address, city, postcode; notes for staff (such as the wifi code or bin days), shown only to staff at that residence and never to family accounts; the carer's name printed on its invoices	Yes
Residents and staff	Shift handover notes and task descriptions	Yes
All users	In-app notifications	Yes; deleted after 90 days
Residences and staff	Residence compliance certificates, staff car-insurance documents and staff signatures (uploaded files)	Yes: whole file encrypted

Stored unencrypted, by design: dates (date of birth, record, incident and appointment dates), money amounts, category values (incident type, appointment type, shift, mood score), usernames, roles, residence names, the care provider's legal name, website, payment terms and public registration numbers (company, VAT, CQC, ICO and ODS), the text a residence prints on its invoices, each person's light/dark display choice, and on the medication record the schedule times and days, dose outcomes (such as given or refused), quantities and controlled drug balances. These are needed for searching, sorting, date-based retention and reporting. None of them is free text about a person's health. Earlier versions of amended records, and

the copy kept of any deleted care record (section 7), are stored encrypted as a whole. Emails waiting in the outgoing queue are stored with the recipient's address and name, the subject and the body encrypted.

Family-member accounts only ever see the residents they are linked to (section 4). The family portal (messages, updates, photos and visit requests) is off for each family member until staff record that person's consent and its basis, separately for each part, and it stops as soon as the account is unlinked from the resident.

3. Encryption

Personal data is encrypted twice over: by TLS on the network, and by the application itself before it reaches the database or disk, so a copy of the database or file store on its own does not reveal the encrypted fields or files.

In transit

- All traffic uses HTTPS; redirecting plain HTTP to HTTPS is set on the hosting platform (section 13). The app page and the API both send Strict-Transport-Security: max-age=31536000; includeSubDomains, so browsers refuse plain HTTP for a year after a visit.
- The page's Content Security Policy includes upgrade-insecure-requests.
- The session cookie is marked Secure, HttpOnly and SameSite=Strict.
- TLS protocol versions and certificate management are handled by the hosting provider (section 13).

At rest: database fields

- Cipher for new values: AES-256-GCM (authenticated encryption) via OpenSSL, with a true 32-byte random key.
- A new random 12-byte nonce for every value, and a 16-byte authentication tag checked before anything is returned, so a changed value is rejected rather than decrypted.
- Stored format: ev2:<key id>: followed by the nonce, tag and ciphertext in base64. The key id is bound into the tag check, so a value cannot be passed off as belonging to a different key.
- Values written before the upgrade use AES-256-CBC with a random 16-byte IV and encrypt-then-MAC (HMAC-SHA256 over IV and ciphertext, checked in constant time). Strict mode (APP_REQUIRE_HMAC) is switched on, so an older value that fails its check is never decrypted. Re-encryption converts older values to the new format (below).
- The encrypt function refuses a value that is already encrypted, so nothing is ever wrapped

twice. At rest: uploaded files

- The whole file is encrypted with the same scheme as soon as it is received: it is read from PHP's temporary upload, encrypted in memory, and only the encrypted bytes are written to the upload folder. The file name's type must match its real content.
- Stored file names are random (UUID-based), web directory listing is switched off, and the web server refuses direct requests to the upload and quarantine folders.
- Readable file content is only returned through an authenticated endpoint that checks the

requester's tenant owns the file, logs the access, and decrypts in memory. Incident reports built from a Word template, and Subject Access Request and staff-document bundles, are assembled in a private temporary file outside the web folder, read into memory and deleted at once, so nothing unencrypted is ever written to the upload folder.

- A file replaced or removed from a record is moved, still encrypted, to the quarantine folder instead of being erased (section 7).

Keys and secrets

- The encryption keys, integrity key, database password and any scheduled-job token live in a secrets file stored outside the public web folder, and are read through environment variables rather than kept in the application code.
- Data keys are a numbered set of 32-byte keys (APP_DATA_KEYS), with one named as current (APP_DATA_KEY_CURRENT). New values are always written with the current key; older keys are kept, read-only, only to read values not yet re-encrypted. A separate 32-byte integrity key (APP_MAC_KEY) signs the audit chain and the look-up codes used for account lockout and two-factor set-up codes. The original key from the first release stays available read-only, because older values and older audit entries depend on it.
- **Rotation:** a new key is added and made current; a Super Admin then starts re-encryption under Settings > Encryption Keys (with their password re-entered). It re-encrypts every stored value and every file in the upload and quarantine folders in the background, in batches, and shows progress. The previous re-keying in September 2026 used a one-off script that has since been removed from the server.
- **Escrow:** the Encryption Keys screen shows a short fingerprint of each key, and a Super Admin records, with their password re-entered, that an offline copy of the current keys is held. The screen keeps warning until that is recorded for the current key.

Passwords and login secrets

Secret	How it is stored
User passwords	bcrypt hash (PHP password_hash), never reversible
Two-factor login secrets	AES-256 encrypted, as above
Two-factor recovery codes	bcrypt hash per code, each usable once
Two-factor set-up codes	Keyed hash only; single use, expire after 72 hours
Sign-in names tracked for lockout	Keyed hash only, never the name itself
Tenant SMTP passwords	AES-256 encrypted; not shown in the browser once saved

4. Identity and access

Every request is authenticated by a server-side session, checked against the user's role through a central route map, and restricted to their own care provider's data. Super Admin sign-in always needs a code from an authenticator app; for everyone else it is needed wherever the care provider switches it on. Sensitive actions also ask for the password again.

Two-factor login (TOTP)

- Standard time-based one-time passwords (RFC 6238): HMAC-SHA1, 6 digits, 30-second steps. Works with Microsoft Authenticator, Google Authenticator and similar apps.
- Each user's secret is 160 bits from a cryptographically secure random source, stored AES-256 encrypted.
- Set-up shows a QR code drawn in the browser by a self-hosted library, so the secret is never sent to another website. Set-up only completes after the user enters a valid code from their app. • **Set-up codes:** an Admin can issue a one-off set-up code to someone who has not yet set up two-factor login (for example a new starter). It works once, expires after 72 hours, is stored only as a keyed hash, and lets that person through to set-up only, not into the app.
- A code is accepted for the current 30-second step and one step either side (phone clock drift). A code that has already been used cannot be used again, including by two requests at the same instant.
- 8 one-time recovery codes are issued at set-up (10 characters each, about 49 bits of entropy), shown once and stored bcrypt-hashed.
- After a correct password the session is **not** signed in. It holds a pending sign-in, tied to that browser tab by a 256-bit token, that expires after 5 minutes. After 5 wrong codes the password must be entered again.
- **Super Admins:** two-factor login is always required, enforced in the code with no setting to switch it off.
- **Everyone else:** each care provider's Admins switch it on or off for all their staff. Switching off is always temporary: the Admin chooses 1 hour, 4 hours, 24 hours, 3 days or 7 days, and it switches itself back on at the end of that time.
- **Lost phone:** an Admin can reset one person's two-factor login. That person scans a new QR code at their next sign-in, and nobody else is affected. Admins cannot reset a Super Admin. • Every switch-on, switch-off, automatic switch-on, set-up, set-up code issued or used, reset and recovery-code sign-in is written to the audit log. Changing the setting, issuing set-up codes and resetting someone's two-factor login each need the Admin's password re-entered.

Passwords

The policy follows NCSC and NIST SP 800-63B guidance: length and a breached-password check rather than complexity rules or forced expiry.

- At least 12 characters (up to 72 bytes, the most bcrypt uses). Three or four unrelated words are suggested.
- Checked against a block-list of about 73,000 real-world leaked passwords of 12 or more characters, drawn from the NCSC's list of the 100,000 most common passwords and other public breach lists. The check runs on the server; nothing is sent to any outside service.
- May not contain the person's username or name, or be one character repeated.
- Applies to every password: set by the person, set by an Admin, and the Super Admin.
- Existing passwords are checked when their owner signs in. Anyone whose password doesn't meet the policy must choose a new one before they can do anything else.
- A password an Admin sets for someone is temporary: the person must choose their own at their first sign-in.
- Changing or resetting a password signs that person out of every other open session at its next request.

Brute-force and abuse protection

Control	Limit
Failed sign-ins for one sign-in name (wrong password or wrong 2FA code), from any IP address	5 within 30 minutes lock that name for 15 minutes; each further lock doubles, up to 1 day. The doubling resets after a day without a lock, a successful sign-in, or an Admin unlocking the account (password re-entered, logged). Names are tracked as a keyed hash, and names that match no account are treated exactly like real ones, so the lock message never reveals whether an account exists.
Failed sign-ins from one IP address	5 in 15 minutes, then refused for 15 minutes
API requests	300 per IP address per 60 seconds
Wrong 2FA codes in one sign-in	5, then the password must be entered again

All limits are stored in the database, so clearing cookies does not reset them.

Sessions

- Server-side PHP sessions in strict mode (the server never accepts a session ID it did not issue). The session ID is regenerated at sign-in, which prevents session fixation.
- Signed out automatically after 30 minutes of inactivity, and after 12 hours in all however active, both enforced on the server. The background signal an open edit form sends

does not count as activity, so an unattended form doesn't keep a session open.

- The cookie is named `__Host-chm_session`, so browsers only accept it from this exact host over HTTPS with no domain widening. Flags: `HttpOnly` (not readable by scripts), `Secure` (HTTPS only), `SameSite=Strict` (not sent on requests from other sites).
- Every state-changing request (POST or DELETE) made while signed in must carry a 256-bit per-session anti-forgery token (CSRF) in an `X-CSRF-Token` header, compared in constant time.
- When a session ends (signing out, 30 minutes without use, the 12-hour limit, a password change or a deleted account), the page reloads rather than just showing the sign-in form. This clears every screen and cached list, so the next person to use that computer cannot see the previous person's data, even for a moment.
- Every signed-in API response carries a short identifier of the account, role and care provider it was prepared for. If it changes, for example because someone signed in to a different account in another tab of the same browser, the page reloads.

Password re-entry for sensitive actions

The following need the person's password entered again if they have not entered it in the last 10 minutes: creating an account or setting someone else's password; deleting an account; resetting someone's two-factor login, issuing set-up codes or changing the two-factor setting; unlocking someone's sign-in; changing a tenant's details or platform settings; deleting a client; downloading all of a resident's files or all of a staff member's documents; permanently deleting a resident's or a former staff member's records; purging old audit entries; re-encrypting stored data or confirming the offline key copy; and converting older saved times to UK time. Each re-entry is logged.

Controlled drug witness. A controlled drug dose, a stock entry, or striking through a controlled drug dose needs a second member of staff to confirm with their own username and password (or their current two-factor code). The witness must be a different person in the same care provider, working at the resident's residence or an Admin, with medication training in date. A wrong witness password counts towards that account's sign-in lockout and is audit-logged, and an unknown username gets the same answer as a wrong password, so nothing is revealed about other accounts. The witness password is cleared from the form whatever the outcome.

Roles

Role	Can access
Super Admin	Platform administration only: tenants, tenant set-up, platform settings, encryption keys, the platform audit log and the third-party software review. Super Admins have no access to any care provider's care records, staff records or files; the server refuses them. Two-factor login always required.

Admin	Everything in their own care provider, whatever residences they are assigned to: all residences and residents, staff accounts and records, settings (including the care provider's CQC, ICO and ODS numbers and accounts contact), two-factor policy, family consent, the CQC evidence pack, quarantined files and the audit log.
Care Provider	Care records for residents in the residences they are assigned to, replying to families, and adding, changing and stopping residents' medicines and recording controlled drug stock (witnessed). Of other staff, only colleagues who share one of those residences (staff list, car insurance and insurance warnings)
Support Worker	As Care Provider, with financial information removed on the server, without replying to families, with car insurance limited to their own, and without managing medicines (they record doses only if their medication training is in date)
Family Member	Only the residents linked to their account, and only the parts of the family portal their recorded consent allows. The NI number, Adult Social Care number, finance reference and fees are removed on the server. Staff choose, per family member and per resident, which parts of the record they may see (daily records, medical history, medications, dental, appointments, care plan, care plan files); risk assessments, assessments, consent forms, physiotherapy notes, correspondence, incidents, finances, residence history, the record of doses given and the controlled drug register are never shown to them, and their medicines

	list leaves out controlled drug stock details. The server refuses family accounts access to staff records and insurance details, tasks, handovers, policies and other residents' files.
--	---

Enforced on the server, not just hidden in the interface

- **Central route map:** every action the API offers is listed in one route map, with the roles allowed for each method and the records the requester must own. The route guard checks this before any handler runs; an action or method that is not declared is refused. Only the 334 named page handlers can be triggered from the page.
- **Tenant isolation:** a central access check confirms that a record belongs to the requester's care provider before it is returned or changed, covering every record type from residents to staff records, family-portal entries and insurance records; uploaded and quarantined files get their own ownership check.
- **Residence scoping:** Care Providers and Support Workers can only list, open, change or download files for residents, handovers, tasks, incidents, invoices, rota and analytics in their assigned residences, whether they go through a list or request a record directly by its ID. The same applies to other staff members' details: they see, and can add car insurance for, only themselves and colleagues at their residences.
- **Staff edit window:** for daily records, medical and dental records, allergies, financial entries, appointments, consent, physiotherapy notes, correspondence and incidents, staff below Admin can only edit or delete entries they created themselves (matched by user account, not by name), within a period the care provider sets (default 7 days). The same applies to deleting a resident's emergency contacts and care document versions, which can't be edited. Admins can correct any record. Medicines are added, changed, stopped or deleted only by Admins and Care Providers (Care Providers delete only those they added, within the edit window), and a medicine with any dose recorded can only be stopped, not deleted.
 - **Medication administration (eMAR):** only staff whose medication training is in date (a course recorded in their training record and not past its due date) can record a dose, and only for residents at their residences. Each scheduled dose can be recorded once, enforced by a unique database key, from an hour before its time up to three days after; anything written more than an hour after the dose is marked as a late entry. A when-required dose beyond the limits entered for that medicine (most in 24 hours, minimum hours apart) is refused. A controlled drug dose needs a witness (above) and enough stock on the register, whose balance can't go below zero; register updates are made under a database lock so two at once can't both use the same stock.
- **Record locking:** resident profiles, incidents and daily records show as locked while someone is editing them, so others are warned not to edit at the same time. The lock is released when the editor closes the form or is signed out, or 15 minutes after their browser stops responding, and Admins can release it. It is a warning in the interface

rather than a block on saving.

- Admins can hide sections and tabs from particular roles under Settings > Layout & Permissions. That controls what is displayed; the data restrictions above apply regardless.
- **Optional services (October 2026):** the Rota, eMAR, Family portal, resident invoicing, care plans and risk assessments, and the CQC evidence pack can be switched off for a whole care provider (by the Super Admin, as part of its subscription) or at individual residences (by the care provider's Admins). This is enforced on the server, not only hidden: after the route guard, every action belonging to a service is refused when the service is off for the care provider, or off at the residence of the record the request names, and lists that span residences leave those residences out. Switching a service off never deletes anything; records stay encrypted as before and come back when it is switched on. Admins and Care Providers can still read them for a Subject Access Request. Changes are audit-logged in the platform log and in the care provider's own log.

Staff account creation and deletion are Admin-only and audit-logged, and an Admin cannot delete their own account. Only a Super Admin can grant the Super Admin role; the server rejects any other attempt, and any role name it does not recognise. Every account other than a Super Admin's belongs to one care provider: a Super Admin must choose it when creating an account, editing an account leaves it where it is unless the Super Admin changes it, and an account can never be linked to another care provider's

residences or clients. The account behind every session is re-checked on every request: a deleted account loses access at its very next request, and a change of role or care provider applies straight away. A staff member's signature (used on invoices) can be uploaded, viewed or removed only by that person or an Admin of their care provider; Care Providers and Support Workers never see a colleague's signature, and an invoice shows the signature of its residence's default Care Provider only while the care provider has the signatory section switched on.

5. Application security

The application is built so that common web attacks (script injection, SQL injection, request forgery, clickjacking and malicious uploads) are addressed by layered controls.

HTTP security headers

Response	Header	Value
App page	Content-Security-Policy	default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data: blob: https;; font-src 'self'; connect-src 'self'; worker-src 'self'; manifest-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'; frame-ancestors 'none'; upgrade-insecure-requests
App page	X-Frame-Options	DENY
App page	Referrer-Policy	same-origin
App page	Permissions-Policy	camera, microphone, geolocation, payment and USB all disabled
App page and API	X-Content-Type-Options	nosniff
API	Strict-Transport-Security	max-age=31536000; includeSubDomains
API	X-Frame-Options	DENY
Served files	X-Frame-Options	SAMEORIGIN, with the correct MIME type and Content-Disposition: inline

The policy allows scripts and stylesheets only from the application's own server, with no inline scripts or inline styles. Every screen was tested in a browser under this policy during development in September 2026, and the screens added since have been tested the same way, with no violations. The API also sends its own restrictive Content Security Policy on data

responses. The page, scripts and stylesheets are served with Cache-Control: no-cache, so browsers check for the current version after every update rather than running an old copy.

Cross-site scripting (XSS)

- All stored text is HTML-escaped before it is placed on a page.
- The pages contain no inline scripts, inline styles or inline event handlers. Actions are wired through a single delegated event handler, which is what allows the strict policy above.
- That handler only runs functions on a fixed list of 334 named page handlers; any other name in the page is ignored.
- If a script were injected anyway, the Content Security Policy stops it running.
- Dark mode is applied before the page is drawn by a small script file served from the application's own server, not an inline script, so the policy stays as strict. The choice is saved to the person's own account; it is a display preference, not personal data, and is not logged.

SQL injection

- Queries use PDO prepared statements with emulation disabled, so values are sent to MySQL separately from the SQL.
- Every value is passed as a bound parameter, including values taken from the server-side session.
- Table and column names used in dynamic queries come from fixed lists in the code and pass through a single check that accepts only plain SQL names, so nothing else can be placed in the query text.

Cross-site request forgery (CSRF)

- SameSite=Strict session cookie, plus a per-session token required on every signed-in POST and DELETE (section 4).
- The API only returns cross-origin credentials to an allow-list of the service's own web

addresses. **File uploads**

Upload	Allowed	Checks	Size limit
Photos, certificates, attachments	JPG, PNG, WebP, GIF, PDF	Extension allow-list and server-side content inspection (finfo MIME detection) must both pass	10 MB per file, or the hosting's PHP upload limit if lower
Care plans, assessments	PDF	Extension and detected content type	15 MB
Incident report templates	Word (.doc, .docx)	Extension and detected content type	15 MB

- Stored under a random name and encrypted (section 3). Logo images (PNG, JPG, WebP) get the same content check, must be a valid image and are limited to 2 MB.
- Family portal photos accept images only (no PDFs), with the same content checks.
- Staff signatures (for invoices) accept PNG, JPG or WebP only, content-checked, up to 1 MB. They are stored encrypted and served only through their own route, which applies the signature rules in section 4, never through the general file route.
- A file that is refused (wrong type, content that doesn't match its name, or too large) is never dropped silently: the person is told which file was not attached and why, and the rest of the entry is saved. A submission larger than the server accepts in one go is refused whole, with nothing saved.
- The file-serving endpoint only accepts paths matching `^uploads/[a-zA-Z0-9_.-]+/$`, which rules out path traversal. Quarantined files are only reachable through a separate Admin-only route that checks the care provider.
- PDFs are shown in the app with PDF.js 6, which draws them as images on the page. This version has no `eval()` code path, the mechanism behind CVE-2024-4367.

Abuse limits: per-IP request limits and the per-account sign-in lockout are in section 4.

Errors: when something goes wrong on the server, the person sees only a short reference code to quote. The details are written to a private monthly error log that the web server refuses to serve, so no code, queries or data are ever shown in the browser.

6. Audit logging

Well over 100 kinds of action are written to a tamper-evident audit log, including every sign-in, every resident record opened, every file viewed and every password re-entry. Each entry records the user's display name, the time, the care provider and a description. Changes to a resident's records (additions, updates and deletions) name the resident. Admins read the log in the app one day at a time, stepping back and forward through the days.

Area	Events recorded
Sign-in and sessions	Successful sign-ins (with method and IP address), wrong passwords and wrong two-factor codes (with IP address, including for unknown usernames), IP and account lockouts and Admin unlocks, sign-outs, automatic sign-out after inactivity or at the 12-hour limit, sessions ended because the account was deleted or the password changed, password changes, password re-entries

Viewing	Every resident record opened, every full-history view, every view or download of an uploaded care or staff file, every view of a record's amendment history, a deleted record or a quarantined file
Care records	Resident created or updated; daily records, incidents, medical history, medicines (added, changed, stopped or deleted), allergies, dental records, appointments, consent forms, care plans, risk assessments and reviews, physiotherapy notes, correspondence, care documents and residence history added, updated or deleted, and additions to an existing day's daily record, each naming the resident. A deletion's entry has a View deleted record button (section 7)
Medication (eMAR)	Each dose recorded (medicine, time, resident, outcome and witness), the effect of a when-required dose, records struck through, controlled drug stock received, given, returned, disposed of or corrected (with the new balance and the witness), wrong witness passwords, and every MAR chart or controlled drug register opened or printed
Staff	Staff training and check records, rota changes, signatures uploaded, viewed by an Admin or removed, leavers recorded, and leavers' records deleted with who approved it
Family portal	Consent recorded or changed, messages and updates posted or deleted, visit requests and decisions
Exports	Subject Access Request reports and file bundles, staff document bundles, PDF exports of record sections, incident report documents, invoice PDFs, the CQC evidence pack

Accounts and security	Staff accounts created, updated or deleted; two-factor login switched on or off (including automatic switch-on), set up, reset, set-up codes issued or used, or used with a recovery code; the care provider's CQC, ICO and ODS numbers and accounts contact changed; encryption re-keying and key escrow confirmations; audit log integrity checks
Records management	Resident records deleted at the end of their retention period, with who approved it
Settings	Tenant settings, global settings, layout and permissions, logos, platform settings, the invoice Service Provided and signatory switches, each residence's default signatory and carer's name, services switched on or off for a care provider (and its price) or at a residence, and the standard service prices
Operations	Handovers, tasks, invoices, invoices emailed and payments recorded, email delivery failures, compliance certificates, third-party software reviews, audit purges, repeated data-load failures

Tamper evidence

- Each care provider's log is a hash chain. Every entry stores its position, the previous entry's hash and its own HMAC-SHA256, keyed with the server's integrity key, over its contents, timestamp and the previous hash.
- The newest position and, after a purge, the starting position are also recorded and signed with the same key.
- **Check Log Integrity** in the Audit tab re-checks the whole chain. It reports any entry that has been changed, any entry removed from the middle or the end, the starting point moved, or an entry added outside the chain. Admins check their own care provider's log; Super Admins check the platform log. Each check is itself logged.
- Entries are written one at a time under a database lock, and each entry and the chain's newest position are saved in a single transaction, so the chain cannot fork.
- The user name and description in every entry are encrypted, like the rest of the personal data.
- The application has no function to edit an entry. Entries are removed only by the retention purge, which removes entries older than the retention period. The daily job runs it,

and a Super Admin can run it on demand with their password re-entered. Each purge is itself logged. • What it protects against: someone with access to the database alone, who doesn't hold the key, cannot alter or insert entries, or remove entries from the start or middle, without the check showing it. Removing the newest entries is shown by the signed newest-position record; if that record is removed too, the next entry written records the gap. Someone with full control of the server, who can read the key, could rebuild the chain; that is covered by restricting server access (section 13).

Access and retention

- Admins see their own care provider's log. Super Admins see only the platform log, which records their own actions, the daily job's entries, lockouts and failed sign-ins for unknown usernames; since Super Admins no longer open care data, care providers' logs are seen only by their own Admins.
- Retention is at least as long as care records are kept: with the default 8-year care record period that is 2,922 days. A care provider can set a longer period, up to 50 years, but never a shorter one; the floor is enforced on the server when the setting is saved and again when the purge runs. The platform log uses the floor.
 - Failed sign-in attempts are also kept separately, for at least 24 hours, to drive the lockouts. The username typed is stored encrypted, and the account lockout keeps only a keyed hash of it.

7. Records management

A resident's whole record is kept until the retention period has passed since their care ended. It is then listed for an Admin to review, and deleted only when the Admin approves. Care records are never deleted automatically. Former staff members' records follow the same pattern (below).

Record	Retention	How it is enforced
A resident's care record: profile, daily records, incidents, medical, medication (including every dose recorded and the controlled drug register), dental, appointments, consent, care plans, risk assessments, physiotherapy notes and assessments, correspondence, family portal entries and photos, amendment history, copies	Platform setting, default 8 years, counted from the date care ended (the end date of the resident's last residence placement)	When the period has passed, the resident appears under Settings > Records Due for Deletion and as a dashboard reminder for Admins. An Admin checks there is no reason to keep it longer (a complaint, safeguarding enquiry, inquest or legal claim) and approves with their password re-entered. The whole record and its files are then deleted, and

of deleted entries, quarantined files and all uploaded files		the approval is logged with the care-ended date and retention period.
A former staff member's records (profile, training and checks, documents, car insurance and their earlier versions)	Kept read-only for 6 years after leaving (default)	Then listed for Admin review, and deleted only when an Admin approves with their password re-entered; logged.
Audit log	At least as long as care records (2,922 days with the 8-year default), up to 50 years	Entries older than the setting are removed by the daily job, or on demand by a Super Admin; each purge is logged, and the log still verifies afterwards (section 6)
Quarantined files (files replaced or removed from a record)	Same as the audit log	Removed by the same purge once the audit entry recording their removal passes the retention period, or earlier with the resident's whole record
In-app notifications	90 days	Deleted by the daily job
Invoices	Kept as financial records under the care provider's own finance retention	Deleting a resident's care record does not delete invoices. Invoice lines keep the resident's name (encrypted) but are unlinked from the deleted record.

The period follows the NHS Records Management Code of Practice, which sets a minimum of 8 years after the end of care for adult social care records. Residents who are still in a placement, or who have no placement end date recorded, are never listed. An Admin can still delete a resident's record at any time (for example, one created in error); that removes the whole record and its files and is logged.

Subject access requests: Admins can produce a Subject Access Request for any resident

in their care provider, and Care Providers for residents in their assigned residences. It downloads as two files:

- a PDF report of the resident's record: profile (including NHS and NI numbers, room, main emergency contact and care worker details), allergies, daily records, incidents (including body-map locations), medical history, medications (with their schedule), every dose recorded (struck-through records included), the controlled drug register, dental records, appointments, consent forms, financial entries, residence history, additional emergency contacts, care plans and risk assessments written in the app with their review history, physiotherapy notes, correspondence, family portal messages, updates and visits, and the list of care plans and assessments on file;
- a ZIP of every uploaded file held about the resident (care plans, assessments, daily-record photos, incident photos, consent forms, physiotherapy sheets, correspondence files, family portal photos, and files held in quarantine), decrypted, with a contents list giving each file's date and, for care plans and assessments, its original file name.

Earlier versions of amended records, copies of deleted entries, and task and handover notes that mention the resident, are not in the report; an Admin adds them where the request covers them. Both downloads are logged (the PDF when it is generated in the app), and the ZIP needs the requester's password re-entered. The ZIP is built in a private temporary file outside the web folder and deleted as soon as it has been sent.

Accuracy and amendments

- When a record is edited, the version it replaces is saved first, encrypted, with who changed it and when. Records that have been changed show an **Amended (n)** button, which opens every earlier version with the changed fields highlighted. This covers resident profiles, daily records, incidents, medical and dental records, medicines, appointments, consent forms, physiotherapy notes, correspondence, residence compliance records, staff training and check records and staff car insurance. A save that changes nothing adds no version.
- Earlier versions can't be edited or deleted in the app. They are kept even if the entry itself is deleted (below), and removed only with the resident's whole record, or with a former staff member's records for their car insurance. Family accounts can't see them.
 - For daily records, medical and dental records, allergies, financial entries, appointments, consent, physiotherapy notes, correspondence and incidents (and, for deletion, emergency contacts and care document versions), staff below Admin can only amend or delete their own entries (matched by user account), within the care provider's edit window (default 7 days). Admins can amend any record. Deleting an entry removes it from the record, but a copy is kept (below).
- Medication administration records are never changed or deleted in the app. A wrong record is struck through by the person who recorded it (within the edit window) or an Admin, with the reason, who and when, and stays on the MAR chart; for a controlled drug, the quantity goes back on the register as a witnessed correction. Register entries can't be changed. Both are erased only with the resident's whole record.
 - **Deleted entries are kept.** When a care entry is deleted (a daily record, incident,

appointment, medical, dental, medication, allergy or financial entry, consent form, physiotherapy entry, correspondence entry, emergency contact, care document entry, residence history entry,

residence compliance record or staff training or check record), a copy of it as it stood is saved first, encrypted, with who deleted it and when, alongside its earlier versions. The deletion's audit log entry has a **View deleted record** button for the care provider's Admins, and each viewing is logged. Copies are erased with the resident's whole record, and copies of residence compliance records when the deletion's audit entry passes the audit retention period.

- **Removed files are kept in quarantine.** A file replaced or removed from a record (including photos and certificate images) is moved, still encrypted, to a quarantine folder that the web server refuses to serve. Admins can open it from the audit log entry that recorded its removal, and each opening is logged. It is erased when that entry passes the audit retention period, or with the resident's whole record.
- An edit lock warns others when someone is already editing a resident profile, incident or daily record (section 4).
- Each resident has one daily record per day, enforced by the database. A second member of staff writing for the same day adds to that record under a line naming them and the time; the server refuses any change to what was already written, the earlier version is kept (Amended) and the addition is logged.

End of contract: see section 13 for how a care provider's data is returned and deleted.

8. Third-party software and vulnerability management

The service depends on seven third-party components, all on supported release lines (versions as read by the in-app review on 25 September 2026, apart from PHP, upgraded since). One needs action: the database, which is several patch releases behind within its supported line. PHP was upgraded from 8.2 to 8.4 in September 2026, well before 8.2's security support ends on 31 December 2026.

Component	Version	Used for	Licence	Support status
jsPDF	4.2.1	PDF exports	MIT	Latest release
Chart.js	4.5.1	Analytics charts	MIT	Latest release
PDF.js (legacy build)	6.3.289	Viewing PDFs in the app	Apache-2.0	Latest release
qrcode-generator	2.0.4	Two-factor set-up QR code	MIT	Maintained
PHPMailer	7.1.1	Alert and invoice emails	LGPL-2.1	Latest release

PHP	8.4	Application runtime	PHP licence	Supported: bug fixes to 31 Dec 2026, security fixes to 31 Dec 2028. Upgraded from 8.2 in September 2026
Percona Server for MySQL	8.4.6-6	Database	GPL-2.0	Long-term support line, supported to April 2032. Newer 8.4 patch releases exist; applied by the hosting provider

Supply-chain controls

- Browser libraries are hosted on the application's own server, each in a folder named with its exact version, so the running version is fixed and visible. No content delivery network is used.
- The Content Security Policy only allows scripts from the application's own server (section 5).

Monthly review, built into the application

- The platform's Super Admins complete a Third-Party Software Review every 30 days. A reminder appears on their dashboard when it is due, overdue, or something needs attention.
- The review screen reads the versions actually running (from the library folders, PHP, the database and PHPMailer) and shows how close PHP and MySQL are to end of support: amber within 12 months, red within 90 days.
- It runs automatic checks: no scripts or stylesheets loaded from other websites, the security header is present, no one-off maintenance scripts are left on the server, and every Super Admin account has two-factor login set up.
- Every component must be ticked as checked against its release notes and security advisories before the review can be completed. Each completed review stores who did it, when, a snapshot of every version, anything still open, and notes. It is also written to the audit log.

Patch targets

Situation	Target
Critical or high-severity fix released for a component	Applied within 14 days of release (the Cyber Essentials requirement)
Component approaching end of support	Replacement planned 12 months ahead, completed before the end date
Any component	Always one of: maintained upstream, covered by a support arrangement, or scheduled for replacement by a set date

Recent remediation (September 2026)

Change	Reason
PDF.js 3.11.174 upgraded to 6.3.289	3.11.174 is affected by CVE-2024-4367 (CVSS 8.8): script execution from a malicious PDF
jsPDF 2.5.1 upgraded to 4.2.1	2.5.x is a superseded line; 10 advisories published against jsPDF in 2026
Chart.js pinned to 4.5.1	Previously loaded as "latest" from a CDN, with no fixed version
All libraries moved from CDNs onto the application server	Removes third-party script hosts from the supply chain
Content Security Policy added to the app page	Blocks injected or third-party scripts
Password check added to leftover maintenance scripts	They could previously be run by anyone who found their address

9. Email and notifications

The application sends email through each care provider's own mail server: one daily alert email to the address the provider chooses, and client invoices only to the saved invoicing email (a residence's single invoicing address, or each resident's own; stored encrypted), with the server refusing any other recipient. Both contain residents' or staff members' names, so the mail server and mailboxes should be secured to the provider's own standard for personal data.

Email	Personal data included
Alert: missing, expiring, expired or stale residence compliance records (fire, gas, electrical, insurance)	None: residence name and certificate type
Alert: staff car insurance missing, expiring or not business class	Staff member's name
Alert: staff training and checks overdue or due soon	Staff member's name and the item due
Alert: care plan and risk assessment reviews due	Resident's name, and the risk assessment's title
Alert: upcoming appointments	Resident's name, appointment type (e.g. GP, Hospital) and date
Alert: leavers due for review	Counts only, no names
Client invoice, with the invoice PDF attached	Residents' names and the amounts charged for each. If the care provider switches on the signatory section (off by default), also the residence's default Care Provider's name, job title, email, phone number and signature, and the carer's name

How it is sent

- By PHPMailer through the SMTP server the care provider configures (e.g. Microsoft 365, Gmail or their own).
- Always encrypted: implicit TLS (port 465) or STARTTLS (port 587). There is no unencrypted option, and a mail server that can't encrypt is refused rather than used in plain text. Platform invoice emails follow the same rule.
- Every email goes through an outgoing queue in the database, with the recipient's address and name, the subject and the body stored encrypted. Failed sends are retried automatically, and emails that still fail are shown to Admins.
- The SMTP password is stored AES-256 encrypted and is never shown again in the browser once saved.
- The daily job runs from the server's command line, which no one on the web can reach. No web token is configured, so it cannot be started over the web at all.

No other resident personal data leaves the application by email. Separately, the platform emails each care provider its own subscription invoices and payment reminders through Whitsend Studios' mail server; these are about the care provider's account, not residents.

Exports are downloaded by the signed-in user in their browser. Subject access reports and file bundles, record exports, incident reports and invoice PDFs are all logged.

10. Standards mapping

The tables below show how the application's controls support the frameworks NHS commissioners and care providers most often ask about. **Supplier** means the control is delivered by Honeysuckle Care Management itself or by Whitsend Studios. **Customer** means it depends on how the care provider runs its own organisation; the application may help, but it cannot meet the standard for you. Each status is written to be quoted in your own evidence.

10.1 Data Security and Protection Toolkit (National Data Guardian's 10 standards)

Care homes complete the DSPT as Category 3 organisations. The 2025/26 target is "Standards Met" and the submission deadline is 30 June 2026; check the current year's deadline on the DSPT site.

NDG standard	Who	How Care Home Manager supports it	Status
1. Personal confidential data	Both	Sensitive fields are encrypted with AES-256-GCM (older values AES-256-CBC with an HMAC-SHA256 check) (section 3). Uploaded files are encrypted at rest and can only be opened through the authenticated file route; removed files are kept encrypted in quarantine. Access is restricted by tenant, role and assigned residence through a central route	Supported

		map (section 4). A Subject Access Request export is built in (section 7).	
2. Staff responsibilities	Customer	Each user has their own named account and role; there are no shared logins. Every create, update and delete, every file opened and every password re-entry is written to the audit log against the user's name (section 6).	Customer policy; app supplies evidence
3. Training	Customer	Not an application function, though staff training and checks can be recorded and tracked in the app. The customer must train staff in data security each year.	Customer
4. Managing data access	Both	Five role levels, with server-side enforcement through a central route map. Care	Supported. Customer must review user lists regularly

NDG standard	Who	How Care Home Manager supports it	Status
--------------	-----	--------------------------------------	--------

		staff only see residences they are assigned to, and only colleagues who work there. Family members only see their linked resident, and only what their recorded consent allows. Financial fields are removed on the server for Support Workers. Super Admins have no access to care data. Admins can delete user accounts, unlock sign-ins and reset two-factor login, with their password re-entered.	
5. Process reviews	Both	The audit log shows who did what and when. The Super Admin runs a monthly third-party software review inside the app (section 8). The CQC evidence pack gathers the care provider's own figures for review.	Supported

6. Responding to incidents	Both	Incident records within the app for care incidents. For a data breach, the supplier notifies the customer (timescale in section 13), and the customer, as data controller, decides whether to report to the ICO within 72 hours.	Partly: supplier breach process to be confirmed in section 13
7. Continuity planning	Both	Hosted web application reachable from any device with a browser. Backups are provided by the hosting platform. An offline escrow copy of the encryption keys is recorded in the app.	Supplier backup details to be confirmed (section 13). Customer needs a paper fallback plan
8. Unsupported systems	Supplier	All third-party components are listed with versions and end-of-life dates, and checked every 30 days inside the app. The application runs on PHP 8.4, which receives security fixes until 31 December 2028.	Supported

9. IT protection	Both	HTTPS with HSTS, a strict Content Security Policy, CSRF protection, rate limiting, per-account and per-IP sign-in lockout, password re-entry for sensitive actions, and two-factor login, always required for Super Admins (sections 4 and 5).	Supported for the application. Customer is responsible for its own devices and network
10. Accountable suppliers	Supplier	This document, the component inventory and the confirmations in section 13 are the supplier's evidence.	Pending the confirmations in section 13

10.2 Cyber Essentials (v3.3, from 27 April 2026)

Cyber Essentials certifies an organisation, not a product. The table shows how the application helps the supplier's and the customer's certification.

Control	How the application relates	Status
Firewalls	Hosting platform firewall. The application exposes only HTTPS.	Hosting provider; to confirm
Secure configuration	Directory listing is switched off and secrets are held outside the web root. The web server	Supported

	refuses every PHP file except the two entry points, and refuses server code, logs, uploads, quarantine and data or backup files. Errors show the user a reference code only. One-off maintenance scripts are removed after use, and the monthly review checks for leftovers. The daily job runs from the server's command line.	
Security update management	Critical and high-severity fixes are applied within 14 days. Components past end of life are replaced beforehand. Tracked by the in-app review.	Supported. Database patch level depends on the host (section 12)
User access control	Named accounts, least privilege, a 12-character minimum with a breached-password block-list, per-account lockout, password re-entry for sensitive actions, and two-factor login from an authenticator app, always required for Super Admin (administrator) accounts. v3.3 treats missing MFA as an automatic fail wherever a cloud service offers it: this application offers it to every role, so customers should keep it switched on.	Supported. Customer must keep 2FA on
Malware protection	Upload allow-lists by file type and size, with	Supported for the application. Customer

	content-type checks on the server. Files are stored encrypted and never run on the server.	devices need their own protection
--	--	-----------------------------------

10.3 UK GDPR

Article	How it is met	Status
Article 5(1)(e) storage limitation	Each resident's whole record is kept until 8 years (configurable) after their care ended, in line with the Records Management Code of Practice, then listed for an Admin to review and delete. Former staff members' records are kept read-only for 6 years, then listed the same way. The audit log and quarantined files are kept at least as long as care records and then purged by the daily job; notifications are deleted after 90 days.	Supported. Customer must review and approve deletions
Article 15 right of access	Built-in Subject Access Request export: a PDF report covering the whole record, including care plans, risk assessments, physiotherapy notes, correspondence and the family portal, and a ZIP of every file held, including quarantined files.	Supported
Article 25 data protection by design	Encryption by default, minimum-access roles, financial data removed on the server for roles that do not need it, no care data access for Super	Supported

	Admins, family portal off until consent is recorded, and the CQC evidence pack uses figures and initials only.	
Article 32 security of processing	Encryption, access control, two-factor login, account lockout, audit logging, patch management and regular review, as described in sections 3 to 8.	Supported. Penetration test to be confirmed
Article 33 breach notification	Supplier informs customer without undue delay; customer reports to the ICO within 72 hours where required.	Supplier timescale to be confirmed
Articles 44 to 49 international transfers	Hosting location to be confirmed (UK expected). No third-party analytics, fonts, scripts or content delivery networks are loaded by the application.	Hosting location to be confirmed

10.4 DTAC version 2 (mandatory from 6 April 2026)

NHS organisations use the Digital Technology Assessment Criteria before buying digital products. These are the sections of version 2.

Section	Position	Status
C1 Clinical safety	Honeysuckle Care Management records care information and appointments and, since 13 October 2026, each medicine's schedule and every dose given or not given (eMAR). It shows	To be assessed

	when doses are due or overdue and refuses when-required doses beyond the limits staff enter from the prescription. It does not calculate doses, check interactions or allergies against medicines, make clinical decisions or give clinical advice. Because the eMAR supports giving medicines, it is more likely to bring the product within DCB0129, so this assessment is now a priority (section 13). Whether it is a medical device, and whether DCB0129 applies, needs to be decided with the DTAC decision tree.	
C2 Data protection	Covered by sections 2, 3, 7 and 10.3. DTAC v2 asks for privacy information, terms and conditions, and a DPIA on the NHS England template.	DPIA template and terms to be supplied
C3 Technical security	Covered by sections 3 to 8. DTAC v2 asks the supplier to confirm it meets the government's Software Security Code of Practice, and extends MFA requirements to administrator and remote-access accounts. Two-factor login is available for every role and is always required for Super Admin accounts, enforced in the	Penetration test and Cyber Essentials certificate to be confirmed

	code.	
C4 Interoperability	No NHS integrations (such as NHS login, GP Connect or FHIR APIs) today. NHS numbers are validated with the standard check digit. Data can be exported as PDF.	Not currently applicable; roadmap item
D1 Usability and accessibility	Responsive design for phones, tablets and desktops. An internal WCAG 2.2 AA review was carried out on 1 October 2026, with automated checks showing no remaining violations and keyboard-only tests passing. The dark mode added on 12 October 2026 passes the same automated checks, colour contrast included. A formal independent audit has not yet been carried out.	Independent audit to be carried out

10.5 DCB0129 and DCB0160

DCB0129 applies to manufacturers of health IT systems and requires a named Clinical Safety Officer, a hazard log and a clinical safety case. DCB0160 applies to the organisation that deploys the system. If the DTAC decision tree finds that DCB0129 applies, Whitsend Studios will appoint a Clinical Safety Officer and publish a safety case; this is listed in section 13. Care providers using the system in an NHS-funded setting should record their own deployment risks under DCB0160. For the eMAR these include a medicine copied wrongly from the prescription (the app does not check it against the prescription), a dose recorded against the wrong resident (the record window names the resident and shows their allergies; wrong records are struck through), and the app being unavailable during a round (a paper fallback is needed).

11. Customer responsibilities

The application's controls only work if they are used. As data controller, the care provider is

responsible for the following. Most of these are also DSPT evidence items.

- **Switch on two-factor login and keep it on.** It is always on for Super Admins. Admins can turn it off for their staff for troubleshooting, but it switches itself back on automatically after the chosen period (at most 7 days). Record every time it is switched off, and why. The audit log records it too.
- **Give each person their own account** and the lowest role that lets them do their job. Never share logins.
- **Assign care staff only to the residences they work in.**
- **Remove leavers' access the same day** and record them as leavers, so their records are kept read-only for the retention period. Review the user list at least every quarter.
- **Reset two-factor login, issue set-up codes or unlock a sign-in only after confirming who is asking**, for example by a call back to a known number, never on the strength of an email alone. Give set-up codes to the person directly, not by email.
- **Record family consent carefully.** Record each family member's consent and its basis before switching on any part of the family portal, and review it when circumstances change.
- **Use strong passwords.** The application enforces 12+ characters and blocks breached passwords; your own policy should also prohibit reusing passwords from other services.
- **Protect your devices.** Screen locks, supported operating systems and browsers, security updates, and malware protection on every phone, tablet and computer used to sign in. Do not use public or shared computers.
- **Configure email securely.** Use a mail server that supports SSL (port 465) or STARTTLS (port 587); unencrypted sending is not possible. Check that residence invoice contacts are correct, because invoices name residents.
- **Tell staff before their details go on invoices.** If you switch on the invoice signatory section, the residence's default Care Provider's name, job title, email, phone number and signature are printed on invoices sent to residents' invoicing contacts. Make sure that person knows, and that the details are ones they are happy to share.
- **Set retention to match your policy.** Records are kept until 8 years (the default) after care ends. Record an end date when a resident leaves (Residence History), and review Records Due for Deletion and leavers due for review regularly, keeping any record needed for a complaint, safeguarding enquiry or legal claim.
- **Handle Subject Access Requests** within one calendar month, using the built-in export.
- **Train staff** in data security and protection every year.
- **Have a fallback.** Keep a paper-based or offline process for continuing care if the system cannot be reached.
- **Complete your own DSPT** and, where you deploy in an NHS-funded setting, your DCB0160 clinical risk assessment.
- **Report suspected breaches** to Whitsend Studios immediately, and decide whether to report to the ICO within 72 hours.

12. Known limitations and improvement plan

Seventeen of the twenty limitations identified in the September 2026 review have been fixed,

six more issues found since have also been fixed (12.3), and further hardening through October 2026 is listed in 12.4. The three still open (L8, L11, L13) need action outside the code, on the hosting platform or by independent testers. They are listed first, with one residual risk (R1).

12.1 Open items

#	Limitation	Risk	Current mitigation	Planned action
L8	All care providers share one database, separated in the application (logical multi-tenancy).	A coding error could expose one provider's data to another.	Every request re-checks the account and its care provider on the server; a central route map declares the roles and record ownership for every action, and undeclared actions are refused; a central access check covers every record type plus files; automated tests cover the cross-provider cases. Sensitive fields are encrypted.	Independent penetration test of tenant separation (L13).

L11	The database server is several patch releases behind (Percona 8.4.6; latest in the 8.4 line is 8.4.11-11, released 20 August 2026).	Known database bugs may be unpatched.	Database not reachable from the internet (to confirm).	Hosting provider to confirm a patch date.
L13	No independent penetration test yet. No formal accessibility audit (an internal WCAG 2.2 AA review was done on 1 October 2026).	Unknown weaknesses. DTAC evidence gap.	Internal testing, independent code review, Automated security and accessibility tests.	Commission a CREST-accredited penetration test and an independent WCAG 2.2 AA audit.
R1	The encryption and signing keys are held on the application server.	Someone with full control of the server could read data and rebuild the audit chain.	Keys held outside the web folder, with a separate integrity key; an offline escrow copy is recorded; keys can be rotated in the app; server access restricted to the supplier (section 13).	Consider a hosted key-management service.

13. Supplier details to confirm

The items below are not decided by the application's code, so they cannot be stated from it. Whitsend Studios will complete them before this document is issued to NHS customers.

Item	Detail needed	Status
Hosting provider	Company name and data-centre location. UK hosting is expected.	SiteGround London (UK)
TLS	Protocol versions (TLS 1.2 minimum, TLS 1.3 preferred), certificate provider, SSL Labs grade.	Protocol: TLS v1.3 Certificate Provider: Let's Encrypt SSL Labs: Grade A+
Disk and backup encryption	Whether server disks and backups are encrypted at rest.	Yes
Backups	Frequency, retention period, storage location, and date of the last successful restore test.	Automatically backs up daily, keeping up to 30 daily copies. Last backup/restore test: 10/10/2026
Recovery targets	Recovery Point Objective and Recovery Time Objective.	RPO: 24 hours RTO: 1 hour
Database exposure	Confirmation that the database accepts connections only from the application server.	Confirmed, only access from the application server is allowed.
Penetration test	Tester, date, scope and summary of findings.	To arrange
Cyber Essentials	Certificate number and expiry (Cyber Essentials Plus preferred for NHS).	To confirm
Supplier DSPT	Whitsend Studios' own DSPT status and organisation code.	Not Applicable (Yet)
ICO registration	Registration number.	To confirm

Data Processing Agreement	Article 28 terms, including sub-processors (hosting provider, email provider).	Whitsend Studios incorporates standard, fully compliant Article 28 UK GDPR terms within our master terms of service and Data Processing Agreement (DPA). We act as a Data Processor and strictly operate under the documented, written instructions of the Data Controller. Regarding sub-processors, we maintain flow-down data protection agreements that mirror our Article 28 obligations with all core infrastructure providers. Our primary sub-processors include SiteGround (for cloud hosting infrastructure), alongside Microsoft 365 and Google Workspace (for corporate business communications and email routing). We maintain an up-to-date sub-processor inventory and notify clients of any proposed infrastructure changes prior to onboarding new vendors.
Breach notification	How quickly the supplier informs customers of a breach (for example within 24 hours of becoming aware).	1 Hour
Support	Contact details, hours, and response times for security issues.	rob@whitsendstudios.co.uk Response: 1 Hour
Clinical safety	Outcome of the DTAC medical-device decision tree. If DCB0129 applies: Clinical Safety Officer,	To assess

	hazard log and safety case.	
Offboarding	How data is returned (format) and deleted when a customer leaves, and how deletion is confirmed.	To confirm
Supplier access to live data	Who at the supplier can access production, how that access is controlled, and whether it is logged.	To confirm
Software Security Code of Practice	Supplier's confirmation of compliance, required by DTAC v2.	To confirm
September 2026 security update	The update and its database migration have been applied, the migration scripts removed from the server, and strict integrity checking (APP_REQUIRE_HMAC) switched on. Dates the later updates in 12.3 and 12.4 were applied to be recorded. Sections 3 to 9 and 12 describe the application after all of these updates.	Confirmed; dates to record
Super Admin two-factor login	Required for all Super Admin accounts, enforced in the code with no setting to switch it off (section 4).	Confirmed
Encryption key upgrade	The new data keys and separate integrity key are in the secrets file, re-encryption has completed, and the offline escrow copy is	Confirmed

	recorded in Settings > Encryption Keys.	
Daily job	The hosting cron runs the job from the server's command line, and the web token has been removed from the secrets file, so the job can no longer be triggered over the web.	Confirmed

14. Sources

- [Records Management Code of Practice: retention schedule for care records \(NHS England\)](#) • [Data Security and Protection Toolkit](#)
- [Digital Care Hub: DSPT and Cyber Essentials for social care](#)
- [NCSC: Cyber Essentials overview](#)
- [NHS England: DCB0129 clinical risk management](#)
- [Digital Technology Assessment Criteria \(DTAC\)](#)
- [Burges Salmon: new DTAC, what health tech suppliers need to know](#)
- [Adult social care: assured digital solutions](#)
- [ICO: UK GDPR guidance](#)
- [RFC 6238: TOTP time-based one-time passwords](#)
- [CVE-2024-4367 \(PDF.js\) advisory](#) • [jsPDF security advisories](#)
- [PHP supported versions](#)
- [MySQL end-of-life dates](#)
- [Percona Server for MySQL 8.4 release notes](#)