PacsPilot trust and security

PacsPilot. The same text is at https://pacspilot.com/trust.

Trust and security

How PacsPilot is built, how it protects data, and what is and is not done yet.

This page describes how PacsPilot stores and protects data, who processes it, and how we recover from problems. The facts here come from the same engineering documents we build the product from. Where something is planned but not done, we say so.

> PacsPilot is in early access. PacsPilot does not accept protected health information yet. Until a business associate agreement with our hosting provider is in place, accounts accept synthetic or de-identified data only, and no patient information goes to any AI service. PacsPilot has not been cleared by the FDA.

Sections

- Architecture and data residency (https://pacspilot.com/trust/architecture)
- Encryption and keys (https://pacspilot.com/trust/encryption)
- Access and audit (https://pacspilot.com/trust/access-and-audit)
- How we protect your data (https://pacspilot.com/trust/how-we-protect)
- Backups and recovery (https://pacspilot.com/trust/backups-and-recovery)
- Subprocessors and the BAA (https://pacspilot.com/trust/subprocessors)
- Penetration testing (https://pacspilot.com/trust/penetration-testing)
- Shared responsibility (https://pacspilot.com/trust/shared-responsibility)
- Uptime and status (https://pacspilot.com/trust/uptime)
- AI in PacsPilot (https://pacspilot.com/trust/ai)

A PDF copy of this page is at https://pacspilot.com/trust/pacspilot-trust.pdf.

Security questionnaires

We answer security questionnaires with a link to this page. It covers the topics most questionnaires ask about: hosting, data residency, encryption, access control, audit, backups, subprocessors and incident handling. If a question is not answered here, the answer is not something we have published.

Contracts and enterprise requests

PacsPilot has one set of terms for every customer:

- The Terms of Service (https://pacspilot.com/legal/terms), accepted by click-through at signup.
- The Business Associate Agreement (https://pacspilot.com/legal/baa), accepted by click-through by the practice owner in the app.

We do not negotiate custom contracts, master service agreements or order forms. Pricing is published at https://pacspilot.com/#pricing. Prices will be published there before general availability.

Single sign-on (SAML or OIDC, for example Entra ID or Okta) is part of the product. A practice owner sets it up in the app. It does not need a separate agreement.

The Terms of Service and the Business Associate Agreement are drafts today. A healthcare lawyer is writing

the binding text. Each page shows its version and status.

Reporting a security problem

See Security and Vulnerability Disclosure (https://pacspilot.com/security). Email security@pacspilot.com.

Architecture and data residency

PacsPilot runs entirely on Cloudflare, with customer data stored in the United States.

How PacsPilot is built

PacsPilot runs on Cloudflare. There are no servers of our own in the production path.

Part	Cloudflare service	What it does
Web app and API	Workers	Serves app.pacspilot.com, sign-in, the worklist, uploads, sharing and administration
Image gateway	Workers	Serves images on img.pacspilot.com after checking a short-lived view token on every request
Processing	Containers, Workflows, Queues	Verifies and stores uploaded studies, and builds the files the viewer reads
Practice database	Durable Objects	One separate database for each practice, holding its worklist, demographics, reports and audit trail
Account catalog	D1	Users, practices, sessions and tokens. No patient data by design
Image archive	R2	The archive of record for every image

Billing runs on Stripe, outside Cloudflare. Stripe never receives patient data. See Subprocessors and the BAA (https://pacspilot.com/trust/subprocessors).

Where data is stored

R2, D1 and Durable Objects are created in Cloudflare's us jurisdiction. Data in them is stored and processed only in the United States. The jurisdiction is set when each store is created and cannot be changed later.

Each practice's database is placed in one US location when the practice goes live, close to where its users connect from.

How images are stored

- Images are compressed losslessly (HTJ2K) before or during upload. No lossy compression is applied at any stage of ingest.
- The server checks every instance against a hash of its decoded pixels. A mismatch is rejected.
- Stored images are written once and never changed. Demographic corrections are kept as a separate, audited record and never modify the stored files.
- A practice can also keep bit-exact copies of the files as received.

How practices are kept apart

Every layer enforces the practice boundary on its own:

1. The practice comes from the signed-in session or a signed token, never from the request.

2. Each practice has its own database. There is no shared table of patient data to filter.
3. Every storage key starts with the practice ID.
4. An automated test suite creates two practices and checks that every endpoint refuses access to the other practice's data.

Clinic equipment

Modalities at a clinic send studies to a gateway or site agent on the clinic's network. It sends them to PacsPilot over HTTPS only, authenticated with a client certificate and a token. It needs no inbound internet ports.

Development and test systems

Development and staging systems hold synthetic data only and are not in the production path.

Encryption and keys

Data is encrypted in transit and at rest, and credentials are stored only as hashes.

In transit

- All connections to PacsPilot use TLS 1.2 or later, terminated at Cloudflare's edge.
- Traffic between PacsPilot's Workers and its processing containers stays on Cloudflare's network.
- Clinic gateways and site agents send studies over HTTPS only, with a client certificate (mutual TLS) and a token. Images are never sent over the internet with DIMSE.
- Every response from app.pacspilot.com sends HSTS. The image host img.pacspilot.com sends HSTS too.

At rest

- R2 storage, D1 and Durable Object storage are encrypted at rest by Cloudflare, with keys Cloudflare manages.
- The image cache is encrypted at rest by Cloudflare.
- Processing containers use temporary disk only. It is wiped when the container stops.

PacsPilot does not offer customer-managed encryption keys.

Credentials and tokens

- Session tokens, API tokens and sign-in link tokens are stored only as SHA-256 hashes. The raw values exist only in transit.
- Share links use 256-bit random tokens, stored as hashes. A share can have a PIN with lockout, lasts at most 30 days and can be revoked.
- Image view tokens are signed (Ed25519) and last 15 minutes. They are refreshed while the user is active.
- Users sign in with passkeys or an emailed sign-in link. Owners and administrators must have a passkey.

Secrets

- Signing keys and storage keys are kept in Cloudflare Secrets Store, which keeps a log of who changed what.
- Secrets are never committed to source code.
- Storage keys are scoped to a single bucket, with separate keys for the web app and for processing.

What stays out of logs and email

Patient information never goes in logs, URLs, error messages, analytics or email. Emails carry a link and the practice name only.

Access and audit

Who can reach a practice's data, how sign-in works, and what the audit trail records.

Sign-in

- Each person has their own account. There are no shared accounts.
- Users sign in with a passkey or an emailed sign-in link. Passkeys resist phishing.
- Owners and administrators must have a passkey.
- Single sign-on with SAML or OIDC (for example Entra ID or Okta) can be set up by the practice owner, and can be enforced for the practice.

Sessions

- A session ends after 15 minutes without activity and after 12 hours in total.
- A practice can set shorter limits, require passkeys for every member, and limit how many sessions a member may have.
- The image viewer locks after 15 minutes idle.

Roles and permissions

- Every member has a role: owner, administrator, physician, technologist or viewer.
- A practice can define custom roles from a list of permissions. Custom roles cannot manage users, billing or security settings.
- A practice can limit members to visibility groups, so they see only the studies in their scope.
- Downloads are limited to physician roles and above, and each download is audited. Share links do not allow downloads unless the sender turns it on.

Provisioning and access reviews

These features are built and off by default. A practice turns each one on in its settings.

- SCIM 2.0 provisioning, so the practice's identity provider creates, updates and deactivates members.
- Quarterly access reviews, where each member is confirmed, changed or removed, and the review is completed with a passkey.
- Flagging of members with no activity for 90 days, and optional automatic disabling.
- Break-glass access: a physician can open a study outside their group in an emergency. A reason is required, the access is time-limited, and administrators are alerted at once.

Audit trail

The audit trail records sign-ins, study views, downloads, shares, deletions and administrative actions.

- Views are recorded once per user, study and 15 minutes.
- Owners and administrators can view the audit trail in the app and export it.

- Audit records are kept for 6 years. After 90 days they move to an archive in write-protected storage (a bucket lock), which prevents deletion or change for the retention period.
- Legal acceptances, such as the Terms and the BAA, are recorded with the version accepted and the time.

PacsPilot staff access

- Staff work through an operations page that only staff accounts can open, and staff actions are logged.
- There is no shell or SSH access to production.
- Removing a misfiled study needs approval from two staff members and is fully audited.
- When a practice's owner is unavailable, staff do not grant themselves access to clinical data. They help the practice's authorized contact regain the owner account after verifying identity.

Backups and recovery

How images, databases and audit records are backed up, and how we restore them.

What is backed up

Data	How it is protected	Kept for
Images	Written once to the R2 archive. For each live practice, a bucket lock prevents deletion or overwrite	At least 7 years from go-live
Bit-exact originals (optional)	Same archive and the same bucket lock	At least 7 years
Practice database	Point-in-time recovery, plus a nightly export of each practice that changed that day	30 days of point-in-time recovery, 90 days of nightly exports
Account catalog	D1 Time Travel, plus a nightly export	30 days of Time Travel, 90 days of nightly exports
Audit records older than 90 days	Archive under a bucket lock	6 years

Each practice's database can also be rebuilt from the image archive, because every image carries its own DICOM headers.

Trial data is not under a bucket lock. Trial data that is not converted to a paid plan is deleted after the trial ends.

Recovery points and targets

- Images: the recovery point is effectively zero, because an image is written to the archive before its upload is acknowledged.
- Practice database: the recovery point is seconds, from point-in-time recovery.

System	Recovery time target
Viewing	4 hours
Practice database	4 hours, or a rebuild from the archive within 24 hours
Account catalog	4 hours
Ingest of new studies	8 hours. Clinic gateways and site agents keep studies until they are received

These are internal targets, not contract terms. The Terms of Service (https://pacspilot.com/legal/terms) do not offer service credits. There are no servers of our own, so availability also depends on Cloudflare's.

How we restore

- A recent mistake in one practice's database (up to 30 days): point-in-time restore by staff from the operations page. The restore itself can be undone.

- Older damage: restore a nightly export into a separate store, compare it, then switch.
- A lost practice database: rebuild it from the image archive, then re-apply corrections.
- Every restore is a staff action recorded in the operations log.

Testing

Our contingency plan calls for a monthly restore drill on staging: a point-in-time restore, a catalog restore with Time Travel, and a rebuild from the archive with a comparison of row counts. The contingency plan is a draft, and no drill is recorded in it yet.

Planned

An optional nightly copy of the image archive to a second storage provider is built and not yet turned on. It will be turned on only after that provider signs a business associate agreement.

Subprocessors and the BAA

The providers that process data for PacsPilot, and the business associate agreement practices accept.

Subprocessors

The full list is on the Subprocessors (https://pacspilot.com/legal/subprocessors) page. Today it has two providers.

Provider	Service	Patient data	Location
Cloudflare	Hosting, storage, email delivery, bot protection	Yes, once patient data is allowed	United States
Stripe	Payments	No	United States

Stripe receives the practice name, billing contact, plan and usage counts only. It never receives patient data, study identifiers or report text.

Practices get 30 days' email notice before we add a provider that will handle protected health information.

AI providers are listed the same way. Amazon Web Services (Transcribe Medical for dictation, Bedrock for language models) is planned and not yet in use. No AI provider receives patient information until its business associate agreement is signed and it is on the list. See AI in PacsPilot (https://pacspilot.com/trust/ai).

Business Associate Agreement

PacsPilot acts as a business associate of the practices that use it. The Business Associate Agreement (https://pacspilot.com/legal/baa) is a click-through agreement. The practice owner accepts it in the app, and a PDF copy is emailed to the owner.

The BAA is a draft today. A healthcare lawyer is writing the binding text. Its exhibit states how PacsPilot handles data:

- Data is stored with Cloudflare in the United States.
- Data is encrypted in transit with TLS and at rest by the hosting provider.
- Original images are kept in write-protected storage for the practice's retention period.
- The audit trail is kept for 6 years.
- The practice can export its studies and audit trail from the app at any time.
- Emails never contain patient information.

When patient data is allowed

PacsPilot does not accept protected health information until both of these are true:

1. Cloudflare's business associate agreement with PacsPilot is signed. This is not done yet.
2. The practice has accepted PacsPilot's Business Associate Agreement.

The app enforces this. A practice's "PHI allowed" setting cannot be turned on until both conditions are met. Until then, accounts accept synthetic or de-identified data only.

Questions about subprocessors: privacy@pacspilot.com.

Penetration testing

No third-party penetration test has been performed yet; this page says what is planned and what we do now.

Status

No third-party penetration test of PacsPilot has been performed yet. No testing firm has been engaged. When a test is done, this page will give its date, the testing firm, the number of findings by severity, and whether a retest confirmed the fixes.

Planned scope

The scope for the first external test is written. It covers:

- The web app and API on app.pacspilot.com: sign-in (sign-in links, passkeys, single sign-on), sessions, roles, practice isolation, share links, upload links, uploads, billing and staff endpoints.
- The image gateway on img.pacspilot.com: view tokens, cache isolation between practices, and storage key handling.
- DICOMweb, HL7 and FHIR intake: token scope, size limits and malformed input.
- Gateway and site agent ingest with client certificates.
- Processing of malformed and oversized DICOM files.
- The clinic gateway image and the Windows site agent.

The main objective is any read or write of one practice's data from another practice's account, and any staff-only action from a non-staff account. Testing uses synthetic practices and synthetic data only.

Critical and high findings are to be fixed before the first clinical customer, and medium findings within 90 days.

What we do now

- An automated test suite creates two practices and checks that every endpoint refuses access to the other practice's data.
- Every API endpoint validates its input.
- DICOM files are processed in containers with size and time limits, running as a non-root user with a read-only file system apart from temporary storage.
- Dependencies are checked for known vulnerabilities in continuous integration, and container images are scanned. High and critical findings fail the build.
- Anyone can report a problem under our Security and Vulnerability Disclosure (https://pacspilot.com/security) policy. We acknowledge reports within 3 business days.

Shared responsibility

What PacsPilot does and what the practice does to run a PACS safely.

Running a PACS safely is shared work. The full table is the Shared Responsibility Matrix (https://pacspilot.com/legal/responsibility). It is an exhibit to the Terms of Service (https://pacspilot.com/legal/terms) and the Business Associate Agreement (https://pacspilot.com/legal/baa). It is a draft for lawyer review today.

Summary

Area | PacsPilot | Practice

HIPAA role | Business associate, with its own safeguards and subcontractor BAAs | Covered entity, with its own risk analysis, notices and patient authorizations

Users and access | Authentication, passkeys, single sign-on support, audit trail, session controls | Who gets an account, roles, removing leavers, regular access reviews

Data entered | Lossless storage, integrity checks, corrections | Correct demographics, right patient, right study

Sharing | Expiring links, PINs, watermark, audit | Deciding who receives a share and whether it is a permitted disclosure

Clinical use | Intended use stated in the product | Clinical judgment, diagnostic displays, checking measurements

Retention | Write-protected archive, retention settings, export tools | Choosing retention periods that meet state medical-record laws, and legal holds

On-site equipment | Site agent and gateway software, signed builds, updates | Workstations, full-disk encryption, network, modality configuration

Patient requests | Export and audit tools | Answering patient access, amendment and accounting requests

Breach | Detect, investigate and notify the practice under the BAA | Notify patients, HHS and the media as a covered entity

Backups and availability | Archive, point-in-time recovery, contingency plan | Downtime procedures in the clinic

Intended use

PacsPilot is for image review, communication and referral. It is not intended for primary diagnostic interpretation. Clinical judgment stays with the practice's licensed professionals.

Uptime and status

How we watch availability today, and the public status page that is planned.

Status page

A public status page at status.pacspilot.com is planned. It is not live yet. It will run on a separate domain, so it stays up when the app has a problem. When it is live, this section will show uptime from its feed.

We do not publish uptime figures yet.

How we watch availability today

- An external check calls the health endpoints of app.pacspilot.com and img.pacspilot.com every hour from

outside Cloudflare. A failed check alerts the owner.

- This check adds to Cloudflare's own health checks. It does not replace them.

Availability commitment

The Terms of Service (https://pacspilot.com/legal/terms) say we aim to keep the service available at all times, apart from planned maintenance that we announce in advance where we can. They do not offer service credits.

PacsPilot runs on Cloudflare with no servers of our own, so availability follows Cloudflare's. Processing containers restart and reschedule automatically. For recovery targets, see Backups and recovery (https://pacspilot.com/trust/backups-and-recovery).

During an incident

- Clinic gateways and site agents keep studies until they are received, so new studies wait and are not lost.
- If viewing is down, practices use their modality or local copies, under their own downtime procedures.
- We post an update for affected practices at the start, at each material change, and at the end.

AI in PacsPilot

Which features use AI, what data they see, and the rules every AI feature follows.

PacsPilot uses artificial intelligence (AI) in some of its features. This page lists them and the rules they follow. The same commitments are in the Terms of Service (https://pacspilot.com/legal/terms), the Privacy Policy (https://pacspilot.com/privacy) and the Business Associate Agreement (https://pacspilot.com/legal/baa).

> No patient information goes to any AI service today. PacsPilot does not accept protected health information yet, and no AI provider has signed a business associate agreement with us.

Features that use AI

Feature	What the AI does	Where it runs
Voice dictation	Turns a radiologist's speech into report text	AWS Transcribe Medical
AI impression draft	Drafts the Impression section from the radiologist's Findings	A language model on Amazon Bedrock
Reading cockpit	Summarizes prior reports, checks a report for gaps and answers questions with sources	A language model on Amazon Bedrock
AI apps	Analyzes studies with an AI product the practice chooses and connects	The AI vendor the practice connects
Support assistant (in progress)	Helps answer support requests, citing the help articles it used	A language model on Amazon Bedrock
Engineering	Helps our engineers write and test code	AI coding tools, on code and synthetic data only

A practice's administrators can turn each AI feature on or off in Settings. Report consistency rules, HL7 mapping, charge coding and dashboards work by fixed rules, not AI.

Rules every AI feature follows

- Training on de-identified data only. We may use data from PacsPilot to train and improve our own AI models in the future. Before any data is used for training, it is de-identified: patient names, dates of birth, medical record numbers, accession numbers, addresses, phone numbers and any other details that could tell one

patient from another are removed. Information that identifies a patient is never used to train AI models. Our outside AI providers do not train their models on the data we send them.

- Patient information only under a BAA. An AI feature can process protected health information only after that AI provider has signed a business associate agreement with us and is listed on the Subprocessors (https://pacspilot.com/legal/subprocessors) page. Practices get 30 days' email notice before that happens. Until then, these features work on synthetic or de-identified data only.
- Identifiers removed. Before report text goes to a language model, the patient's name, medical record number, accession number and date of birth are replaced with placeholders.
- Your clinicians are responsible. AI output can be wrong, and PacsPilot does not review it. The practice's licensed professionals decide whether to rely on it, and clinical decisions stay with them.
- Labeled. AI drafts and AI findings are marked as AI in the app, with the vendor's regulatory label. Research and investigational apps show "Not for clinical use".
- Audited. AI requests are recorded in the practice's audit trail.

AI apps from other vendors

When a practice connects an AI app, PacsPilot sends the matching studies to that vendor. The vendor is the practice's own choice. Before turning an app on, the practice's administrator confirms that the practice has a business associate agreement with the vendor and has read the vendor's intended use. PacsPilot does not make findings itself and does not send clinician feedback to the vendor.

Questions about AI: privacy@pacspilot.com.

How we protect your data

The controls between the internet and a practice's data, from the network edge to sign-in, uploads, logs and monitoring.

This section lists the protections added in our October 2026 security hardening. Where a protection is not yet on in production, we say so.

At the network edge

- Requests reach PacsPilot through Cloudflare's network. Firewall rules block requests that do not match how PacsPilot is used, and public pages such as sign-up and sign-in are rate limited before they reach our code.
- Automated bot traffic is challenged.
- The edge settings are kept as code in our repository. They are checked against the live settings every week and after every production deploy, and any difference is reported to us.
- The PacsPilot staff console is behind Cloudflare Access, separate from customer sign-in.

Sign-in

- Bot checks on public forms fail closed: if the check cannot run, the form is refused.
- Sign-in link requests are limited per email address and per network address.
- Owners and administrators confirm sensitive actions with their passkey again.
- Every sign-in attempt, including attempts for addresses that have no account, is recorded in a log where each entry is linked to the one before it, so a changed or removed entry is detected. The log holds hashes, never the email address.
- API tokens expire and can be limited to the practice's network addresses.

Limits that keep one user from slowing everyone

- Each user, each practice and each upload has request limits.
- When a practice's database answers slowly, dashboards, analytics and exports wait briefly so the worklist, viewer and reports keep working.
- Plans have storage and study caps, and paid work such as emails and PDFs has daily caps.

Uploaded files

- Every uploaded file is checked against a content safety policy before it is stored. Files that would expand far beyond any real scan, nest too deeply or claim impossible image sizes are refused as unsafe.
- Images are decoded one file at a time in a separate thread with memory and time limits, so a hostile file fails on its own.
- Scripts, automatic actions and attached files are removed from PDFs.
- Processing containers get a one-time storage link for each job and hold no standing storage keys.
- These upload protections are on in staging and are being switched on in production.

In the browser

- The app sends strict security headers, including HTTPS-only, no framing by other sites and no content sniffing.
- A Content Security Policy limits what the app page may load. It reports violations today and will be enforced after a week with none from our own code.

Code and changes

- Dependencies are locked to exact versions, and every build step is pinned to a fixed release.
- Every change is scanned for leaked secrets and by static analysis, and each production deploy records a software bill of materials.
- Database changes only add; a check refuses changes that drop or rename data.

Logs and monitoring

- Logs record an error's type and code, never its message, because a message could contain patient information. A code check stops new code from logging error text.
- Failed sign-ins, refused requests, busy-database pauses, unsafe uploads and edge blocks are counted every 5 minutes, as numbers only.
- Practice owners and administrators are alerted when an account fails to sign in 10 or more times in an hour, when more than 1,000 requests are refused in an hour, when the database is busy, and when 5 or more files are refused as unsafe in a day.
- PacsPilot staff review these counts, edge changes and the sign-in log check every week.