Pharwiz

SECURITY & COMPLIANCE WHITEPAPER

Vos données pharmacie en sécurité, en France.

Architecture, chiffrement, sauvegardes et engagements RGPD de la plateforme Pharwiz. Document destiné aux DSI, RSSI et équipes de sécurité.

Souveraineté française
100% France/EU, zéro hyperscaler US

Chiffrement bout en bout
TLS 1.2+, AES-256, age (X25519)

Sauvegarde quadruple
Paris + Amsterdam + NAS local + clé hors infra

Zéro données patients
Filtrage strict côté agent, RGPD by design

VERSION
1.0 · Mai 2026

CONFIDENTIALITÉ
Public

CONTACT
contact@pharwiz.com

SOMMAIRE

Table des matières

Ce document est destiné aux DSI, RSSI et équipes de sécurité des groupements, éditeurs partenaires et clients institutionnels souhaitant valider la solution Pharwiz dans leur stack. Il a vocation à répondre à 80 % des questionnaires de sécurité standard.

01	Synthèse exécutive	p. 3
02	Souveraineté & localisation des données	p. 4
03	Chiffrement à tous les niveaux	p. 5
04	Authentification & contrôle d'accès	p. 6
05	Architecture & isolation des composants	p. 7
06	Protections réseau et applicatives	p. 8
07	Sécurité email & anti-usurpation	p. 9
08	Sauvegarde & continuité de service	p. 10
09	Politique zéro données patients	p. 11
10	Conformité RGPD	p. 12
11	Cycle de vie sécurisé du code	p. 13
12	Monitoring & observabilité	p. 14
13	Gestion des incidents	p. 15
14	Sous-traitants & DPA	p. 16
15	Engagements & contact	p. 17

SECTION 01

01 Synthèse exécutive

Pharwiz est une plateforme française de gestion intelligente pour pharmacies d'officine. Elle traite des données commerciales sensibles (achats, ventes, factures, marges) issues des Logiciels de Gestion Officinale (LGO) déployés en officine.

4 PILIERS FONDAMENTAUX

- Souveraineté française : toute la chaîne critique en France/EU, zéro dépendance hyperscaler US
- Chiffrement de bout en bout : TLS 1.2+ en transit, AES-256 + age (X25519) au repos
- Sauvegarde quadruple : Paris + Amsterdam + NAS local + clé hors infra
- Politique zéro données patients : implémentée techniquement par allowlist stricte

En chiffres

LOCALISATION DES DONNÉES **100 % France / EU**	CHIFFREMENT BACKUPS **AES-256 + age**
CHIFFREMENT TRANSIT **TLS 1.2+ HSTS**	RPO (PERTE MAX) **24 heures**
RTO (RÉTABLISSEMENT) **4 heures**	TEST DE RESTAURATION **Mensuel auto**
RÉTENTION SAUVEGARDES **35 j + 400 j**	DISPONIBILITÉ PUBLIQUE **status.pharwiz.com**

SECTION 02

02 Souveraineté & localisation des données

Toutes les données Pharwiz sont stockées et traitées sur des infrastructures situées en France et dans l'Union européenne, opérées par des fournisseurs européens. Aucune partie de la chaîne critique n'est hébergée chez un hyperscaler américain (AWS, GCP, Azure).

Cartographie des fournisseurs

Composant	Fournisseur	Localisation	Juridiction
Hébergement applicatif	Scaleway Serverless Containers	Paris (fr-par-1)	France
Frontend statique	Scaleway Object Storage	Paris (fr-par-1)	France
Base de données PostgreSQL	Scaleway VPS (self-hosted)	Paris (fr-par-1)	France
Sauvegardes principales	Scaleway Object Storage	Amsterdam (nl-ams)	EU
Sauvegarde 4ème copie	NAS local (France)	France	France
DNS	OVHcloud	Roubaix	France
Email transactionnel	Resend	Irlande	EU
Email professionnel	Google Workspace EU	EU	EU (DPA EU)
Paiements	Stripe	Irlande	EU

Conséquences pour les données client

- Aucune donnée n'est jamais soumise à des réglementations extra-européennes (CLOUD Act US, FISA…)
- Les transferts intra-services s'effectuent exclusivement au sein de l'Espace Économique Européen
- Les sous-traitants non-européens sont écartés par principe
- Le DNS, point d'entrée de l'infrastructure, est géré par un acteur français (OVH)

> **GARANTIE CONTRACTUELLE**
> Pharwiz s'engage dans son DPA à maintenir cette politique de souveraineté tant que cela est techniquement possible. Tout changement majeur fait l'objet d'une notification proactive à 60 jours minimum aux clients sous contrat groupement.

SECTION 03

03 Chiffrement à tous les niveaux

Toutes les données Pharwiz sont chiffrées au repos et en transit, avec des algorithmes modernes (TLS 1.2+, AES-256, ChaCha20-Poly1305) et une stricte séparation des clés cryptographiques.

Chiffrement en transit

- **TLS 1.2 ou 1.3 obligatoire** sur l'ensemble des endpoints HTTP
- **HSTS** avec `max-age=63072000` (2 ans) sur tous les sous-domaines
- **Certificats Let's Encrypt** renouvelés automatiquement (validation ACME)
- **HTTP/3 et QUIC** supportés via Caddy reverse proxy
- **Communication agent ↔ backend** chiffrée par AES-256-GCM avec rotation périodique des clés et anti-replay (nonces uniques)

Chiffrement au repos

- **Disques SSD Scaleway** chiffrés au niveau hardware avec LUKS
- **Sauvegardes doublement chiffrées** :
  - Couche 1 : Scaleway Server-Side Encryption (SSE) AES-256 sur le bucket S3
  - Couche 2 : chiffrement applicatif `age` (X25519 + ChaCha20-Poly1305)
- **Clé privée de déchiffrement** jamais stockée dans la même infrastructure que les sauvegardes (zero-knowledge), répliquée hors infra cloud
- **Mots de passe utilisateurs** hashés avec bcrypt (coût adaptatif, salt individuel)

Secrets & variables d'environnement

- Tous les fichiers `.env` sont chiffrés avec `age` avant commit Git
- Versioning intégral des secrets : rollback à n'importe quelle date possible via Git history
- Rotation programmée des clés API tous les 12 mois maximum
- Principe du moindre privilège : chaque service a sa propre clé IAM scopée

Algorithmes utilisés

Usage	Algorithme	Force
Sauvegardes au repos	age (X25519 + ChaCha20-Poly1305)	Très élevée
Stockage Scaleway	AES-256-GCM (SSE)	Très élevée
TLS	TLS 1.2/1.3 (ECDHE-RSA-AES256-GCM-SHA384)	Très élevée
Mots de passe	bcrypt (cost 12)	Adaptative
JWT signature	HS256 (256-bit secret)	Élevée
Communication agents	AES-256-GCM	Très élevée

SECTION 04

04 Authentification & contrôle d'accès

Le contrôle d'accès suit le principe du moindre privilège, avec des sessions courtes, des secrets non révocables stockés hors application, et une séparation stricte des rôles utilisateur, admin pharmacie, admin groupement et super-admin Pharwiz.

Authentification utilisateur

- **JWT signés HS256** via Supabase Auth (access token ~1h, refresh token rotatif)
- **Refresh tokens rotatifs** : un token utilisé est immédiatement invalidé
- **Mots de passe hashés bcrypt** (coût 12, salt individuel par utilisateur)
- **2FA (TOTP) obligatoire** pour les comptes admin pharmacie et super-admin
- **Lockout automatique** après 5 tentatives échouées sur 15 minutes
- **Email de vérification** obligatoire avant activation du compte

Modèle de rôles (RBAC)

Rôle	Périmètre d'accès
user	Accès aux données de SA pharmacie uniquement
admin pharmacie	Gestion utilisateurs & paramètres de SA pharmacie
admin groupement	Vue agrégée des pharmacies de SON groupement (via permissions explicites)
super-admin Pharwiz	Maintenance, accès temporaire, justifié, audité

Cloisonnement multi-tenant

- **Filtrage applicatif systématique** par `pharmacy_id` dans toutes les requêtes
- **Workspace context middleware** qui rejette toute requête sans contexte tenant valide
- **Tests automatisés cross-tenant** qui vérifient l'absence de fuite
- **Architecture cible fork-per-tenant** pour isolation physique des données critiques (groupements premium)

> **ACCÈS SUPER-ADMIN PHARWIZ**
> Les super-admins Pharwiz ne peuvent accéder aux données client qu'à des fins de maintenance, sur demande explicite ou en cas d'incident. Tous les accès sont audités. La liste des super-admins est restreinte au strict minimum technique et journalisée.

SECTION 05

05 Architecture & isolation des composants

L'architecture Pharwiz applique le principe de défense en profondeur : chaque composant est isolé, les communications entre composants passent par des canaux authentifiés, et les zones publiques sont strictement séparées des zones privées.

Quatre niveaux de défense

1

Niveau réseau

Cloudflare WAF (option), rate limiting, geo-IP filtering, DDoS protection

2

Niveau applicatif

FastAPI strict, validation Pydantic, ORM paramétré (zéro SQL brut), CORS strict

3

Niveau base de données

Row-Level Security (RLS) PostgreSQL, schémas isolés, principe least-privilege

4

Niveau humain

2FA obligatoire, accès super-admin scopé et audité, formation continue

Architecture des composants

- Frontend statique servi par Scaleway Object Storage, aucune logique métier exposée
- Chunks protégés (pages /app et /admin) servis par le backend après vérification JWT
- Sourcemaps non publiques : uploadées à Sentry pour debug puis supprimées du bucket public, jamais exposées
- Backend FastAPI en Serverless Containers, avec autoscaling et isolation d'exécution par requête
- Base de données PostgreSQL self-hosted sur VPS dédié, accès uniquement depuis le backend (firewall strict)
- Agents pharmacie (poste local) communiquent via tunnel chiffré AES-256-GCM avec relay backend
- Kill switch global : bascule de la prod entière en mode read-only en moins de 10 secondes via flag DB

SECTION 06

06 Protections réseau et applicatives

Pharwiz implémente plusieurs couches de protection contre les attaques classiques (OWASP Top 10) et les abus de service (DDoS, brute force, scraping).

OWASP Top 10 mitigations

Risque	Mitigation
A01 · Broken Access Control	RBAC strict, filtrage tenant_id systématique, tests cross-tenant
A02 · Cryptographic Failures	TLS 1.2+, AES-256, bcrypt, age, rotation des clés
A03 · Injection	ORM paramétré, validation Pydantic, sanitization HTML, zéro SQL brut
A04 · Insecure Design	Threat modeling, principe least-privilege, defense in depth
A05 · Security Misconfiguration	Configuration as code, secrets versionnés chiffrés, audits réguliers
A06 · Vulnerable Components	Dependabot, audits npm/pip mensuels, mises à jour critiques en < 48 h
A07 · Authentication Failures	JWT court, 2FA admin, lockout, refresh rotatif
A08 · Software & Data Integrity	Signatures Git, CI/CD verrouillée, hash des artifacts, age signing
A09 · Logging Failures	Sentry + audits internes, alertes Slack instantanées
A10 · SSRF	Allowlist stricte des domaines sortants, validation URL

Limites de débit (rate limiting)

- Login : 5 tentatives par 15 minutes par IP/email
- API en lecture : 1000 req/min par utilisateur authentifié
- API en écriture : 100 req/min par utilisateur authentifié
- Endpoints publics (lead capture, contact) : 5 req/min par IP

SECTION 07

07 Sécurité email & anti-usurpation

Le domaine pharwiz.com est protégé contre l'usurpation par la triple chaîne SPF + DKIM + DMARC, avec une politique stricte (reject) et reporting actif.

Configuration en place

Mécanisme	Configuration	État
SPF	`v=spf1 include:_spf.google.com include:mx.ovh.com ~all`	Soft fail (~all)
DKIM	Signatures Google Workspace + OVH (rotation périodique)	Actif
DMARC	`v=DMARC1; p=quarantine; pct=100; rua=mailto:adrien@pharwiz.com`	p=quarantine

Les emails sortants de Pharwiz (notifications, factures, alertes système) passent exclusivement par Resend (Irlande) avec signature DKIM. Les emails professionnels passent par Google Workspace EU avec DPA européen.

> **DÉTECTION D'USURPATION**
> Les rapports DMARC quotidiens sont analysés automatiquement. Toute tentative d'usurpation détectée (envoi non autorisé depuis un autre serveur) déclenche une investigation immédiate.

SECTION 08

08 Sauvegarde & continuité de service

Pharwiz applique la règle 3-2-1+ : trois copies des données, sur deux types de support différents, dont au moins une copie hors site, et même une quatrième copie supplémentaire chez un opérateur indépendant.

Quatre tiers de sauvegarde

1

Production live

PARIS (FR-PAR-1) · SCALEWAY VPS

PostgreSQL self-hosted avec WAL streaming, snapshots disque toutes les heures.

2

Sauvegarde principale chiffrée

AMSTERDAM (NL-AMS) · SCALEWAY OBJECT STORAGE

Dump pg_dump + zstd + age, uploadé chaque nuit. Versioning S3 actif. Rétention 35 jours quotidiens + 400 jours mensuels.

3

Réplication NAS privé hors cloud

FRANCE · SERVEUR DÉDIÉ ISOLÉ

Pull hebdomadaire depuis le bucket Amsterdam, sur un serveur NAS privé en France, hors infrastructure cloud. Clé IAM read-only dédiée.

4

Clé de déchiffrement hors infra

COFFRE-FORT HORS LIGNE

La clé privée age est conservée dans un gestionnaire de mots de passe + cold storage, jamais dans la même infrastructure que les sauvegardes.

Engagements RPO / RTO

RPO (PERTE MAX ACCEPTÉE)	RTO (RÉTABLISSEMENT CIBLE)
24 heures	**4 heures**
TEST DE RESTAURATION	DISPONIBILITÉ VISÉE
Mensuel auto	**99,9 %**

TEST DE RESTAURATION MENSUEL

Chaque 1er du mois, un script automatique restaure intégralement la dernière sauvegarde chiffrée dans un environnement PostgreSQL isolé, vérifie le nombre de tables, le nombre de lignes et l'intégrité référentielle. En cas d'échec, alerte immédiate.

SECTION 09

09 Politique zéro données patients

Pharwiz ne traite, ne stocke et ne transmet aucune donnée patient. Cette politique n'est pas une simple promesse contractuelle : elle est implémentée techniquement et auditable.

Implémentation technique

- Allowlist stricte côté agent pharmacie : seules les tables et colonnes commerciales (achats, ventes, factures, marges) sont accessibles à l'extraction
- Blocklist explicite des tables patients : toute tentative d'accès à une table contenant des données patients (noms, adresses, numéros de sécurité sociale, ordonnances) est bloquée au niveau de l'agent
- Chemins d'accès whitelistés : seuls les répertoires LGO connus sont lisibles par l'agent
- Code source de l'agent disponible pour audit sur demande sous NDA

Données traitées par Pharwiz

Catégorie	Statut
Données commerciales (achats, ventes, factures)	Traitées
Données fiscales (CA, marges, statistiques)	Traitées
Stock et catalogue produits (CIP, EAN, prix)	Traitées
Données nominatives utilisateurs Pharwiz	Traitées (RGPD)
Données patients (identités, ordonnances, secu)	JAMAIS
Données médicales (pathologies, traitements nominatifs)	JAMAIS

BÉNÉFICE POUR LES PHARMACIES

- Pas de qualification "donnée de santé" au sens de l'article 9 RGPD
- Pas de besoin d'hébergeur HDS (Health Data System) certifié
- Pas d'exposition au CLOUD Act sur des données patients
- Audit RSSI simplifié : périmètre commercial uniquement

SECTION 10

10 Conformité RGPD

Pharwiz est en conformité avec le RGPD pour les données nominatives utilisateurs (employés des pharmacies utilisateurs de la plateforme).

Six principes appliqués

- Minimisation : seules les données strictement nécessaires sont collectées (email, prénom, nom, rôle)
- Limitation des finalités : les données ne sont utilisées que pour le service Pharwiz, jamais revendues, jamais utilisées pour du profilage commercial externe
- Exactitude : l'utilisateur peut modifier ses données à tout moment depuis son compte
- Limitation de conservation : suppression sur demande, suppression automatique après 24 mois d'inactivité
- Intégrité & confidentialité : voir sections 03 (chiffrement) et 04 (auth)
- Responsabilité : DPO désigné, registre des traitements à jour, DPA disponible sur demande

Droits des utilisateurs

- Droit d'accès : export complet des données disponibles depuis l'app
- Droit de rectification : modification directe depuis l'app
- Droit à l'effacement : suppression complète sous 30 jours sur simple demande
- Droit à la portabilité : export JSON/CSV à tout moment
- Droit d'opposition : désinscription des emails marketing en un clic
- Délai de réponse : sous 30 jours maximum (typiquement < 5 jours ouvrés)

> **DPO & CONTACT**
> Toute demande RGPD peut être adressée au DPO de Pharwiz à l'adresse dpo@pharwiz.com. Le registre des traitements et le DPA complet sont disponibles sur demande pour les clients sous contrat groupement.

SECTION 11

11 Cycle de vie sécurisé du code

Pharwiz applique un cycle SDLC sécurisé : revue de code, tests automatisés, audit de dépendances et déploiement reproductible.

Pratiques de développement

- **Revue de code systématique** avant merge sur main, avec tests obligatoires verts
- **CI/CD verrouillée** : seuls les agents CI signés peuvent déployer
- **Tests automatisés** (pytest backend, vitest frontend) avec gates de couverture
- **Audit dépendances** via Dependabot (alerts hebdomadaires)
- **Mises à jour critiques sécurité** appliquées en moins de 48 heures
- **Pas de déploiement le vendredi** sauf hotfix critique
- **Rollback en 1 clic** via Scaleway container revisions

Outils utilisés

Étape	Outil
Versioning	Git (GitHub privé)
CI/CD	GitHub Actions + Scaleway Container Registry
Tests backend	pytest + pytest-asyncio + pytest-cov
Tests frontend	Vitest + Testing Library
Lint	ruff (Python), ESLint (JS/TS)
Audit dépendances	Dependabot, npm audit, pip-audit
Monitoring erreurs	Sentry (EU region)

SECTION 12

12 Monitoring & observabilité

L'observabilité de Pharwiz est continue : disponibilité publique, monitoring erreurs applicatives, alertes proactives et page de statut publique.

Stack monitoring

Couche	Outil	Localisation
Uptime monitoring	Hyperping	EU
Page de statut publique	`status.pharwiz.com`	EU
Erreurs applicatives	Sentry	EU region (Frankfurt)
Logs serveur	Scaleway Logs	Paris
Alertes incidents	Slack + Email	EU

Métriques surveillées

- **Disponibilité** : checks toutes les 60 s sur API + frontend + DB
- **Latence p95** sur les endpoints critiques (login, upload, dashboard)
- **Taux d'erreur 5xx** avec alerte si > 1 %
- **Tentatives d'auth échouées** avec alerte si pic anormal
- **Sauvegardes** : alerte si pas de backup les 24 dernières heures

SECTION 13

13 Gestion des incidents

En cas de breach ou d'incident de sécurité, Pharwiz applique une procédure standardisée et notifie les clients et la CNIL dans les délais légaux.

Procédure d'incident

Étape	Délai	Action
1. Détection	Immédiat	Alerte automatique (Sentry, Hyperping, audits internes)
2. Confinement	< 1 h	Isolation du composant impacté, activation du mode read-only si nécessaire
3. Investigation	< 24 h	Analyse logs, évaluation périmètre des données potentiellement exposées
4. Remédiation	Selon gravité	Patch, rollback, rotation des secrets, restauration backup si nécessaire
5. Notification clients	< 48 h	Email aux administrateurs des pharmacies impactées + post sur status.pharwiz.com
6. Notification CNIL	< 72 h	Si incident à risque pour les droits et libertés (RGPD art. 33)
7. Post-mortem public	< 14 j	Analyse des causes racines et plan d'amélioration publié

ENGAGEMENT DE TRANSPARENCE

Tout incident affectant la disponibilité ou l'intégrité des données fait l'objet d'une communication publique sur `status.pharwiz.com`, suivie d'un post-mortem détaillé. Aucun incident n'est caché.

SECTION 14

14 Sous-traitants & DPA

Pharwiz s'appuie sur un nombre restreint de sous-traitants techniques, tous couverts par un DPA conforme au RGPD.

Liste exhaustive des sous-traitants

Sous-traitant	Rôle	Localisation	DPA
Scaleway	Hébergement applicatif & stockage	France / EU	Oui
OVHcloud	DNS & domaine	France	Oui
Stripe	Paiements en ligne	Irlande	Oui (EU)
Resend	Emails transactionnels	Irlande	Oui (EU)
Google Workspace	Email pro & collaboration interne	EU region	Oui (DPA EU)
Sentry	Monitoring d'erreurs applicatives	EU (Frankfurt)	Oui (EU)
Hyperping	Monitoring uptime	EU	Oui (EU)

La liste complète des sous-traitants ainsi que les DPA correspondants peuvent être communiqués sur demande aux clients sous contrat groupement. Tout ajout d'un nouveau sous-traitant majeur fait l'objet d'une notification préalable de 30 jours minimum.

SECTION 15

15 Engagements & contact

Pharwiz maintient et fait évoluer continuellement sa posture de sécurité. Voici nos engagements opérationnels et les canaux pour nous joindre.

Engagements opérationnels

- **Notification proactive** de tout changement majeur d'architecture (60 j minimum pour les clients groupement)
- **Mise à jour de ce document** au minimum deux fois par an, ou à chaque changement structurel
- **Réponse aux questionnaires DSI / RSSI** sous 5 jours ouvrés (15 jours pour audits complets)
- **Pentests externes** envisagés annuellement (à partir de 100 pharmacies actives)
- **Programme de divulgation responsable** documenté à `https://www.pharwiz.com/.well-known/security.txt` (RFC 9116)

Vérifications publiques

La posture de sécurité de Pharwiz est auditable à tout moment via des outils tiers, sans nous demander quoi que ce soit :

Test	Couverture	URL
SSL Labs	Qualité TLS du backend	`ssllabs.com/ssltest/analyze.html?d=api.pharwiz.com`
Mozilla Observatory	Headers HTTP de sécurité	`observatory.mozilla.org/analyze/www.pharwiz.com`
security.txt	Programme de divulgation responsable (RFC 9116)	`www.pharwiz.com/.well-known/security.txt`
status.pharwiz.com	Disponibilité historique 12 mois (Hyperping)	`status.pharwiz.com`

Contacts

SÉCURITÉ TECHNIQUE

contact@pharwiz.com

Vulnérabilités, incidents, questions techniques RSSI/DSI

DÉLÉGUÉ À LA PROTECTION

dpo@pharwiz.com

Demandes RGPD, registre, DPA, exercice des droits

AUDIT & CONFORMITÉ

compliance@pharwiz.com

Questionnaires DSI, certifications, due diligence

STATUT & INCIDENTS

status.pharwiz.com

Disponibilité temps réel et historique des incidents

Pharwiz SAS. Le copilote de la rentabilité des pharmaciens d'officine.
Document v1.0 · Mai 2026 · © Pharwiz · pharwiz.com
Pour la dernière version, consulter pharwiz.com/securite.