SPÉCIAL PHARMACIENS • OFFICINE

Et moi, ma pharmacie est-elle réellement protégée ?

Faites votre auto-évaluation cybersécurité et RGPD en 5 minutes.

26 questions • Sans engagement • Résultat immédiat

Les cyberattaques récentes visant des éditeurs de logiciels, des services cloud et des acteurs de la santé le démontrent : **aucune organisation n'est à l'abri.** Une pharmacie peut être victime d'un incident **sans avoir commis la moindre erreur**, simplement parce qu'un fournisseur, un sous-traitant ou un collaborateur a été compromis.

Comment faire le test ?
Pour chaque question, répondez simplement : **Oui** **Non** **Je ne sais pas**

1 Qui peut entrer dans votre système sans être dans votre pharmacie ?

- ☐ Savez-vous si votre **éditeur de logiciel de gestion** peut accéder à distance à vos systèmes, et dans quel cadre ?
- ☐ L'accès à distance de votre **fournisseur de robot** est-il connu et encadré ?
- ☐ L'accès à distance de votre **installateur d'alarme ou de caméras** est-il connu et encadré ?
- ☐ L'accès à distance de votre **prestataire informatique** est-il connu et encadré ?
- ☐ Savez-vous quels prestataires **hébergent ou traitent vos données dans le cloud** ?

● **À retenir :** chaque accès à distance est une porte d'entrée potentielle vers votre officine et les données de vos patients.

2 Savez-vous réellement qui a accès à vos données ?

- ☐ Chaque collaborateur dispose-t-il de **son propre compte utilisateur** ?
- ☐ Les accès des **anciens collaborateurs** ont-ils tous été supprimés ?
- ☐ Les visiteurs et intervenants externes sont-ils **exclus du réseau professionnel** ?
- ☐ Les ordinateurs de l'officine sont-ils réservés à un usage strictement professionnel (aucun proche, aucun usage familial) ?
- ☐ Savez-vous précisément **qui peut accéder à l'ensemble de vos données** ?

● **À retenir :** de nombreuses violations de données proviennent d'un accès légitime qui n'aurait plus dû exister.

3 Votre équipe est-elle un rempart… ou un risque ?

- ☐ Vos collaborateurs savent-ils **reconnaître un e-mail frauduleux** ?
- ☐ Savent-ils qu'ils ne doivent **pas installer eux-mêmes des logiciels** ?
- ☐ Savent-ils **comment réagir** face à un comportement informatique suspect ?
- ☐ Si des outils d'IA (ChatGPT, Copilot, Claude…) sont utilisés à l'officine, un **cadre d'usage** est-il défini ?
- ☐ Êtes-vous certain qu'**aucune donnée patient** n'y est saisie ?

● **À retenir :** l'erreur humaine reste l'une des principales causes d'incidents de sécurité.

CABRI.EU

Un outil proposé par CABRI.EU, à votre service pour la suite
Consultant IT en cybersécurité certifié, DPO externe et copropriétaire d'officine.
www.cabri.eu • 0475/64 88 31 • pcayphas@cabri.eu

4 Pourriez-vous récupérer vos données ?

- ☐ Les données de votre officine sont-elles **sauvegardées régulièrement** ?
- ☐ Savez-vous si ces sauvegardes permettraient **réellement de redémarrer** après une cyberattaque ?
- ☐ Avez-vous déjà **vérifié qu'une restauration était possible** ?

● **À retenir :** une sauvegarde non testée est souvent une sauvegarde dont on découvre les limites le jour où l'on en a besoin.

5 Votre pharmacie peut-elle continuer à fonctionner ?

- ☐ Pourriez-vous **travailler une journée entière** sans votre logiciel métier ?
- ☐ Savez-vous où retrouver rapidement **les informations indispensables** à l'activité ?
- ☐ Savez-vous **qui contacter en premier** en cas de cyberattaque ou de fuite de données ?
- ☐ Pourriez-vous continuer à **délivrer des médicaments pendant 24 h** sans informatique ?

● **À retenir :** la vraie question est de savoir comment vous continuerez à servir vos patients lorsqu'une panne surviendra.
Bon à savoir : une fuite de données doit en principe être notifiée à l'Autorité de protection des données (APD) sous 72 h.

6 Sur quoi repose votre sentiment de sécurité ?

- ☐ Connaissez-vous les **principaux risques cyber** de votre officine ?
- ☐ Avez-vous déjà fait **évaluer votre niveau de sécurité** par un tiers ?
- ☐ Connaissez-vous le **coût d'un arrêt complet** de votre activité pendant plusieurs jours ?
- ☐ Sur quels **éléments objectifs** vous basez-vous pour considérer votre pharmacie comme suffisamment protégée ?

● **À retenir :** la plupart des victimes pensaient, elles aussi, être suffisamment protégées avant l'incident.

Votre résultat

Comptez vos réponses **Non** et **Je ne sais pas**. Un score élevé ne signifie pas que votre pharmacie est mal protégée : il signale des risques **non identifiés, non documentés ou non maîtrisés**.



0 à 4 — Bonne base
Fondamentaux apparemment maîtrisés. Un regard extérieur permet de les valider.

5 à 12 — Zones d'ombre
Des risques ne sont sans doute pas identifiés. Un audit ciblé s'impose.

13 et + — Exposition élevée
Une évaluation rapide est prioritaire pour sécuriser l'officine.

UNE DERNIÈRE QUESTION…

Êtes-vous certain de connaître les risques auxquels votre pharmacie est réellement exposée ?

Fin octobre 2026, trois pharmacies françaises ont été visées en moins de 48 h par des cyberattaques revendiquées par des pirates, après plusieurs incidents chez des éditeurs et des acteurs de la santé. **La question n'est plus de savoir si votre officine sera touchée, mais si vous serez prêt.**

1 Un confrère de l'officine
Copropriétaire de pharmacie et consultant cyber certifié, 25 ans d'expérience : je connais vos logiciels et vos urgences.

2 Cyber + RGPD, de A à Z
Audit, registre « Officine », accès du personnel et des remplaçants, transferts (mutuelles), DPO externe.

3 75 % pris en charge
Si votre officine est éligible aux Chèques-Entreprises. Audits conçus pour ne pas perturber votre comptoir.

Parlons-en : demandez un échange ou une remise de prix

Philippe CAYPHAS • CABRI.EU
0475/64 88 31 • pcayphas@cabri.eu • www.cabri.eu