POUR LES PHARMACIENS

Tous les logiciels se disent « sécurisés ». Comment faire le tri ?

Avant de signer pour un outil qui manipule les données de santé, faites-lui passer ce **test**.

---

7 questions à faire remplir par l'éditeur ou le commercial **(page 2)**, puis un guide simple et sans jargon pour comprendre ses réponses **(pages 3 et 4)**.

LE QUESTIONNAIRE

Questionnaire de sécurité et de conformité des données de santé

À compléter par l'éditeur ou le commercial du logiciel.

	La question	Oui	Non	Ne sait pas	Preuve ou référence du document
1	**Hébergement et souveraineté** Mes données de santé sont-elles hébergées et traitées en France ou dans l'Espace économique européen, chez un prestataire certifié HDS 2.0 ?	☐	☐	☐	
2	**La certification de l'éditeur** Au-delà de l'hébergeur, l'éditeur du logiciel, celui qui exploite et manipule mes données de santé, détient-il sa propre certification HDS 2.0 ?	☐	☐	☐	
3	**Anonymisation / pseudonymisation** Si vous affirmez ne pas relever du HDS parce que les données seraient anonymisées ou pseudonymisées, pouvez-vous le justifier par écrit ?	☐	☐	☐	
4	**Chiffrement** Mes données sont-elles chiffrées, y compris vis-à-vis de l'éditeur, afin de rester illisibles en cas de vol ?	☐	☐	☐	
5	**Double authentification** L'accès exige-t-il une double authentification, appliquée à tous les accès aux données de santé et pas seulement à la première connexion ?	☐	☐	☐	
6	**Traçabilité** Le logiciel conserve-t-il un journal non modifiable (immuable) de toutes les actions sur les données de santé : qui a fait quoi, et quand ?	☐	☐	☐	
7	**Rôle et contrat RGPD** Indiquez-vous clairement votre rôle (sous-traitant ou responsable de traitement) et signez-vous le contrat RGPD correspondant (contrat de sous-traitance, dit DPA) ?	☐	☐	☐	

Éditeur / société : _____ Nom du signataire : _____

Date : _____ Signature : _____

À CONSERVER

Votre guide de lecture

Pourquoi ce document ?

On vous propose souvent des logiciels « sécurisés » et « conformes RGPD », logos à l'appui. Mais comment vérifier, quand on n'est pas informaticien ?

La sécurité des données de santé est un sujet compliqué. Et entre le comptoir, les nouvelles missions et la gestion de l'officine, vous portez déjà assez de casquettes : vous n'avez pas le temps d'en ajouter une de cybersécurité. Pourtant, votre responsabilité peut être engagée si les données de vos patients sont mal protégées.

Ce guide est là pour ça : vous n'avez rien de technique à comprendre. Faites remplir la page 2 par le commercial ou l'éditeur, puis lisez ci-dessous, sans jargon, ce que chaque réponse veut dire pour vous et vos patients. **Un logo n'est pas une preuve. Une réponse claire, si.**

1 Où sont stockées les données de vos patients ?

En clair : Un logiciel range les ordonnances et les infos de vos patients quelque part, sur des serveurs. Si ceux-ci ne sont pas locaux, la loi impose que ce soit en France ou en Europe, chez un prestataire certifié HDS 2.0, contrôlé.

OUI → Parfait, vous êtes en règle : vos données restent en France ou en Europe, chez un acteur à jour de la loi.

NON / ne sait pas → Méfiance. Et si on vous dit « c'est sur votre ordinateur, donc aucun souci », ce n'est pas si simple : le logiciel touche quand même à des données de santé.

2 L'entreprise elle-même est-elle contrôlée, ou juste ses serveurs ?

En clair : Beaucoup montrent le logo HDS de leur hébergeur. Mais l'éditeur, celui qui fabrique le logiciel et manipule vos données, doit lui aussi être certifié HDS 2.0 et contrôlé.

OUI → Très bon signe : toute la chaîne est protégée, pas seulement là où vos données dorment, mais aussi l'entreprise qui les manipule tous les jours.

NON / ne sait pas → C'est le piège le plus courant. Le logo de l'hébergeur ne vous protège pas si l'éditeur, lui, n'est pas certifié également.

3 Le piège du « pas de données de santé »

En clair : Certains disent « nous, on n'a pas de données de santé, on les a anonymisées / pseudonymisées ». Anonymiser, c'est rendre impossible, pour toujours, de retrouver le patient. Pseudonymiser, c'est juste remplacer le nom par un code : on peut encore retrouver la personne, donc ça reste une donnée de santé. La règle simple : anonymisé, c'est vraiment anonyme ; pseudonymisé, ça reste une donnée de santé.

OUI → Bonne nouvelle, il joue franc-jeu : il vous remet une justification écrite. Conservez-la, c'est votre preuve en cas de question.

NON / ne sait pas → Beaucoup confondent les deux, parfois exprès, pour échapper aux règles. La CNIL inflige des amendes de plusieurs millions d'euros pour ça.

4 Vos données restent-elles protégées même en cas de vol ?

En clair : « Chiffrer », c'est rendre les données illisibles en les brouillant. Seule la personne qui possède la bonne clé peut les déchiffrer.

OUI → Vous êtes bien protégé : même si on volait les serveurs, vos données resteraient illisibles.

NON / ne sait pas → Quelqu'un pourrait lire les ordonnances et les données de vos patients.

5 Un simple mot de passe volé suffit-il à tout ouvrir ?

En clair : La « double authentification », c'est quand, en plus du mot de passe, il faut un second code (sur votre téléphone par exemple) pour entrer.

OUI → Excellent réflexe de sa part : même si on vous volait votre mot de passe, personne ne pourrait entrer sans le second code.

NON / ne sait pas → Un seul mot de passe volé peut exposer tous vos patients. Depuis sa recommandation de mars 2025, la CNIL attend la double authentification pour les données de santé, et le vérifie lors de ses contrôles.

6 Saura-t-on qui a vu quoi, en cas de problème ?

En clair : Le logiciel doit garder une trace, impossible à effacer, de qui a consulté quoi et quand.

OUI → C'est rassurant : en cas de souci, vous aurez une preuve fiable de qui a fait quoi, et quand.

NON / ne sait pas → Aucune trace : vous ne pourrez rien prouver en cas de fuite.

7 Qui est responsable si ça tourne mal ?

En clair : Un contrat (appelé « DPA ») doit écrire noir sur blanc qui fait quoi et qui répond de quoi.

OUI → Vous êtes couvert : les responsabilités sont écrites noir sur blanc, vous ne portez pas le risque tout seul.

NON / ne sait pas → En cas de contrôle, vous, le pharmacien, êtes en première ligne. Certains « oublient » ce contrat. Exigez-le.

En résumé : pour chaque OUI, demandez la preuve écrite (une attestation, un contrat). Un OUI sans preuve, un NON, ou un « ne sait pas » mérite une explication claire avant de signer. Ce sont vos patients, et votre responsabilité.

Partagez ce document

Scannez ce code, ou rendez-vous sur **karukia.com/le-test**, pour le récupérer et le transmettre à vos confrères.

Offert par KARUK IA, éditeur de logiciels SaaS verticaux (Santé & Marchés réglementés) · karukia.com
parce qu'un pharmacien informé protège mieux ses patients.
Ces 7 questions, posez-les à tous vos prestataires. Y compris à nous.