PHARMONY

Les FOCUS

Comment assurer la sécurité informatique de votre officine ?

Document non contractuel - 31/01/24

Introduction

La protection des données est devenue l'une des principales préoccupations pour les officines françaises. En 2023, de nombreuses attaques informatiques sur les pharmacies ont exposé les informations personnelles de milliers de français, mettant en évidence la nécessité de faire face à la menace croissante de **l'insécurité informatique**.

Selon le Règlement Général sur la Protection des Données personnelles (RGPD), les officines sont considérées comme des **"responsables de traitement"** et elles doivent "prendre toutes les précautions pour garantir la confidentialité des données".[1]

Ce focus vous fait découvrir comment **assurer la sécurité et l'intégrité des données** au sein de votre officine, tout en examinant **les risques associés à l'hébergement local** et les avantages du Cloud.

Sommaire

1. Guide pratique : Le pharmacien d'officine et la protection des données personnelles, CNIL https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop_cnil.pdf

> *Le pharmacien titulaire est responsable des traitements informatiques mis en œuvre dans son officine.*[1]

8 Consignes RGPD pour les officines

Pour garantir la confidentialité des données, les officines doivent suivre huit consignes clés du RGPD :

1. Identifier les données personnelles traitées

Déterminez les données sensibles que vous manipulez, telles que les coordonnées, l'INS et autres informations des patients, clients et professionnels de la santé.

1. Guide pratique : Le pharmacien d'officine et la protection des données personnelles, CNIL https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop_cnil.pdf

Exemples de données personnelles[1]

- Identité et coordonnée du patient/client
- Coordonnée des profesionnels de santé
- Identifiant national de santé (INS)
- Données de santé (poids, taille, diagnostics, médicaments ...)
- Données d'habitudes de vie
- Traces fonctionnelles

2. Informer les personnes concernées

Communiquez clairement aux patients et clients l'utilisation de leurs données. Facilitez l'accès à l'information et assurez-vous de rendre les documents compréhensibles.

3. Déterminer la conservation des données

Choisissez judicieusement les durées de conservation en tenant compte des obligations légales et des règles d'archivage et de suppression. Cela garantit une gestion efficace et conforme de l'information.

1. Référentiel relatif aux traitements de donnés à caractère personnel destinées à la gestion des officines de pharmacie, CNIL https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_-_officines_de_pharmacie.pdf

4. Établir une procédure de traitement des demandes

Établissez une procédure claire pour répondre aux demandes d'exercice de droits dans un délai d'un mois, en assurant la conformité aux exigences du RGPD.

5. Désigner un DPO

Vous pouvez nommer un DPO pour superviser efficacement les questions liées à la confidentialité des données au sein de votre officine. C'est une démarche nécessaire pour les officines ayant une activité annuelle de plus de 2 600 000 €

> *Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme.*[1]

1. https://www.cnil.fr/fr/definition/delegue-la-protection-des-donnees-dpo

6. Sensibiliser ses employés

Assurez-vous que les employés de la pharmacie soient informés et conscients des responsabilités liées à leurs usages des données personnelles.

7. Protéger ses données

Veillez à avoir des processus rigoureux pour l'authentification, la gestion des habilitations, le traage des accès, la sécurité des postes de travail, la protection du réseau interne et la protection des locaux.

8. Choisir ses sous-traitants judicieusement

Établissez des contrats définissant et encadrant le traitement des données par vos sous-traitants. Assurez-vous que les outils que vous utilisez ne mettent pas les données de vos clients à risque.

> ***Le RGPD définit le sous-traitant comme l'organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.***[1]

1. Guide pratique : Le pharmacien d'officine et la protection des données personnelles, CNIL https://www.cnil.fr/sites/cnil/files/2023-09/guide-rgpd-cnop_cnil.pdf

Les risques liés à l'hébergement local

Dans cette section, vous verrez pourquoi l'hébergement local n'est pas idéal pour assurer une sécurité informatique de qualité.

Vous verrez également pourquoi ces risques liés à l'hébergement local sont évitables avec un hébergement Cloud de qualité.

> ***Avec le Cloud computing les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés et sécurisés.***[1]

1. https://www.cnil.fr/fr/definition/cloud-computing

Vulnérabilité accrue en cas d'incident

L'hébergement local a toujours présenter un **risque élevé de perte de données en cas de sinistre, panne matériel et rupture du système.**

Avec le Cloud, les serveurs sont distants et sécurisés, ce qui permet une grande robustesse face aux incidents.

De plus, en cas de défaillance d'un serveur ou d'un centre de données, les données sont automatiquement basculées vers des emplacements alternatifs et sécurisés.

Ainsi, le Cloud assure une continuité des services en cas d'incident.

A l'inverse, avec un hébergement local, l'absence de redondance automatique des serveurs rend parfois la reprise de l'activité complexe.

Le Cloud est entré dans tous les domaines informatiques et offre une sécurité inégalée. Les smartphones, ainsi que quasiment tous les domaines industriels et commerciaux fonctionnent avec le Cloud.[1]

Difficulté des mises à jour

Le deuxième défi réside dans la difficulté à maintenir à jour des systèmes hébergés localement. Des mises à jour régulières sont cruciales pour se protéger face aux menaces informatiques.

En revanche, le Cloud vous permet de **bénéficier de mises à jour régulières et à distance**, assurant la sécurité des données qui sont contenues dans votre LGO. De plus, vous êtes libérés de la tâche chronophage de sauvegarde de vos données LGO.

Coûts élevés de l'hébergement local

Le troisième défi réside dans les **coûts élevés associés à l'hébergement local**, notamment pour les serveurs, le stockage et l'archivage.

En choisissant le Cloud, vous vous libérez de l'obligation d'acheter ou de louer des serveurs, ainsi que des frais de maintenance et de sécurité associés. C'est **une solution économique**, éliminant les charges financières liées à l'hébergement local.

Comment le Cloud vous fait économiser ?[1]

1. Serveurs délocalisés : avec le Cloud, vous réduisez les coûts d'achat et de maintenance des serveurs, car ceux-ci sont délocalisés.

2. Sauvegardes et mises à jour gratuites : avec Pharmony, les sauvegardes ainsi que les mises à jour sont gratuites, rapides et automatiques.

3. Visibilité des coûts : fini la multitude de contrats et de factures. Vous disposez d'un seul contrat, d'une seule facture et d'une visibilité claire de vos dépenses !

1. Focus Pharmony : Comment économiser sur son système informatique ?

Logiciel d’officine en mode Cloud

Après avoir examiné les risques liés à l'hébergement local et constaté comment le Cloud résout efficacement les problèmes de sécurité informatique des officines, il est clair que choisir **le Cloud est la meilleure option pour contrôler et sécuriser les données** indispensables à l’exercice de votre activité officinale.

Cependant, peut-on considérer que le mode Cloud n'entraîne aucun risque ?

Évidemment, le risque zéro n’existe pas, mais il peut être réduit au maximum. C'est pourquoi il existe la certification des hébergeurs de données de santé (HDS) qui impose des **normes de sécurité rigoureuses et incontournables à l'hébergeur**. Elle garantit notamment la réalisation d'un audit de surveillance chaque année.

Pharmony, en tant que logiciel en **mode Cloud utilisant un hébergeur certifié HDS** assure la sécurité optimale de vos données informatiques.

Choisissez Pharmony pour une gestion sécurisée et efficace des données de vos patients et de l'officine.