LIVRE BLANC

L'HEBERGEMENT DES DONNÉES DE SANTÉ

[Certification ISO27001 - HDS - ASIP Santé]

ET BONNES PRATIQUES POUR SECURISER L'ECHANGE DE FICHIERS MEDICAUX VOLUMINEUX

WeSend santé

DropCloud santé

Solutions sécurisées du travail en ligne

La protection des données à caractère sensible, comme les données de santé, est un enjeu majeur à l'heure du « tout numérique ». **Les professionnels de santé** traitent une quantité toujours plus importante de fichiers médicaux, qui sont souvent communiqués à des tiers, confrères et autres organismes divers... Légalement, ils **sont responsables de la protection de toutes les informations recueillies auprès de leurs patients**.

Face au risque lié à la cybercriminalité, des solutions en ligne existent, proposant des fonctionnalités appréciables pour les professionnels de santé. L'outil WeSend Santé leur permet d'échanger en toute sécurité des fichiers patients volumineux avec peu de contraintes.

SOMMAIRE

L'importance d'échanger et de sauvegarder en ligne les fichiers médicaux, en toute sécurité

La sécurisation des échanges de données de santé : une priorité absolue

En matière d'échange de données personnelles de santé, **le Code de la santé publique** fixe un cadre juridique très strict[1], qui **protège le droit de chacun au respect de sa vie privée** et au respect du secret de ses informations personnelles. Au quotidien, les professionnels du monde de la santé traitent ces données sensibles, qu'ils doivent impérativement protéger. La loi rend le professionnel de santé responsable des informations personnelles de ses patients.

En pratique, notre système de santé coordonné donne lieu à des **échanges continus entre professionnels de santé**, du médecin traitant vers le spécialiste ou vers le praticien hospitalier… Les fichiers médicaux et les informations des patients sont évidemment échangés entre confrères, mais aussi au-delà, puisque transmis entre les différentes structures de santé et autres organismes que nous connaissons :

- Les groupements hospitaliers de territoire ;
- Les agences régionales de santé ;
- Les laboratoires d'analyse ;
- Les mutuelles…

Les données personnelles de chacun (maladies, handicaps ou encore allergies) passent ainsi entre de nombreux acteurs. Cela paraît indispensable pour **améliorer le suivi médical** du patient et pour optimiser son parcours de soins. Les communications dématérialisées ont grandement facilité ces échanges, mais elles exposent aussi les données de santé à des risques, liés à la cybercriminalité et à la cyber-malveillance.

La sécurisation des échanges de fichiers est donc une priorité absolue, d'autant que **les défauts d'une boîte mail classique sont bien connus** des pirates informatiques.

Choisir une solution en ligne pour l'envoi de fichiers

Un double défi est proposé aux professionnels de santé : échanger facilement et efficacement des fichiers médicaux et garantir leur sécurité. Pour y répondre, une solution en ligne d'envoi et de stockage de fichiers lourds a été développée par DropCloud : WeSend Santé. Cette plateforme professionnelle offre les meilleures garanties de sécurité :

- Chiffrement des données (cryptographie) ;
- Sécurisation SSL pendant l'envoi ;
- Double authentification
- Traçabilité des actions des destinataires.

Un système de transfert de fichiers en ligne sous-entend nécessairement un stockage desdits fichiers sur des serveurs extérieurs. **Les serveurs DropCloud sont localisés en France. Ils répondent à toutes les exigences requises pour l'hébergement des données de santé (certification ISO 27001-HDS).**

[1] Article L1110-4 du Code de la santé publique.

Comprendre la législation concernant l'hébergement des données de santé (HDS)

Comment le RGPD définit-il les données de santé ?

Entré en vigueur le 25 mai 2018, le Règlement général sur la protection des données (RGPD) donne la définition suivante des données concernant la santé[2]. Ce sont *« les données relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. »*

Comprise assez largement, la donnée de santé peut concerner les informations suivantes, qui sont aussi détaillées dans le RGPD[3] :

- Les informations relatives à une personne physique collectées en vue de services de soins ;
- Les informations obtenues lors du test ou de l'examen d'une partie du corps ;
- Les informations concernant une maladie, un handicap, un risque de maladie…

Le RGPD considère comme des données de santé toutes les **informations, explicites ou brutes, qui peuvent renseigner sur l'état de santé d'une personne**. Le résultat d'un bilan sanguin, d'un test à l'effort et le cliché d'une radiographie sont évidemment compris comme une donnée de santé. Mais c'est aussi le cas d'un *« numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé[4] ».*

La protection de ce type de données relève de la **responsabilité du praticien libéral ou de l'établissement qui les recueille**. Les échanges et la sauvegarde des données de santé doivent être assurés en toute sécurité. Si des violations aux dispositions du RGPD sont observées, le responsable de leur traitement s'expose à des sanctions de la part de l'**autorité de contrôle compétente, à savoir la CNIL en France**. Les amendes administratives prévues par le RGPD se veulent *« effectives, proportionnées et dissuasives[5] »*.

[2] Article 4 du RGPD, « Définitions ».
[3] Article 4 du RGPD, « Définitions », Raison 35.
[4] *Ibid*.
[5] Article 83 du RGPD, « Conditions générales pour imposer des amendes administratives ».

La législation en vigueur : RGPD, loi Informatique et libertés et Code de la santé publique

Le Règlement général sur la protection des données (RGPD) est un **règlement** européen appliqué dans tous les États membres de l'Union européenne. En France, **la loi du 20 juin 2018** relative à la protection des données personnelles[6] a permis de conformer le droit national aux dispositions du RGPD. Elle **a ainsi modernisé la loi Informatique et libertés de 1978**, qui demeure la référence en matière de protection des données personnelles en France.

La loi de 1978 renvoie au Code de la santé publique sur le thème du traitement des données de santé. Le corpus législatif qui encadre et protège cet aspect, au niveau européen et en France, est le suivant :

- Le Règlement général sur la protection des données (RGPD) ;
- La loi Informatique et libertés ;
- Le Code de la santé publique.

La question précise de l'hébergement des données de santé (HDS) a été étudiée par la « loi Kouchner » de 2002[7]. Elle a enrichi le Code de la santé publique d'un nouvel article[8], qui précise le cadre juridique concernant les prestations d'hébergement des données de santé.

Hébergeurs des données de santé : de l'agrément vers la certification HDS

L'article L.1111-8 du Code de la santé publique identifie les prestataires HDS – Hébergeurs des données de santé – en ces termes :

« Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même ».

Le prestataire HDS a un ensemble de règles strictes à respecter, car **il reçoit et stocke des données à caractère sensible**. Il doit pouvoir :

- Conserver ces données en toute sécurité pour les seuls besoins du client ;
- Être capable de lui restituer en totalité ;
- Les protéger de manière optimale.

La loi est pensée pour rassurer les professionnels de santé qui confient leurs fichiers à un prestataire externe. C'est **la certification HDS qui donne l'assurance de la qualité des prestations** offertes par un hébergeur. Cette certification HDS est un indispensable gage de sécurité et de confiance.

En cas de défaut d'agrément ou de certification, l'hébergeur s'expose à des sanctions[9] :

- Jusqu'à 3 ans d'emprisonnement ;

[6] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
[7] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
[8] Article L.1111-8 du Code de la santé publique.
[9] Article L.1115-1 du Code de la santé publique.

- Jusqu'à 45 000 euros d'amende.

Depuis le 1er avril 2018, **l'ancien agrément HDS a été remplacé par la certification HDS**. L'agrément était délivré par le Ministère de la Santé, selon la procédure définie par le décret n°2006-6 du 4 janvier 2006. La certification HDS répond à une nouvelle procédure. Désormais, les hébergeurs candidats en font la **demande auprès de l'organisme** certificateur de leur choix, dès lors qu'il est **accrédité par le COFRAC** (Comité français d'accréditation).

Les principes de la nouvelle certification ISO 27001-HDS

Les candidats à la certification HDS doivent respecter un certain nombre de normes et d'exigences, **détaillées sur le référentiel de l'ASIP Santé (désormais ANS : Agence du Numérique de Santé)**. Il leur est notamment demandé d'être en conformité avec la norme internationale ISO 27001[10], qui porte sur la sécurité des systèmes d'information. Le référentiel HDS reprend toutes les exigences de cette norme et ajoute certaines règles issues des normes suivantes :

- ISO 27018, sur la protection des données à caractère personnel dans le cloud ;
- ISO 2000-1, sur la gestion de la qualité des services.

De plus, le référentiel HDS comprend quelques dispositions complémentaires, qui renvoient aux sujets suivants, tous relatifs à la protection des données personnelles :

- La responsabilité (notification au client en cas d'atteinte à la sécurité, période de conservation des politiques de sécurité, mise à disposition, restitution et destruction des données) ;
- La communication des données (période de rétention à définir, notification et traçabilité en cas de communication à un tiers) ;
- La finalité de traitement (conforme et limitée aux instructions documentées du client) ;
- La transparence (information au client en cas de sous-traitance) ;
- La localisation des données ;
- La sécurité des données ;
- Le droit des personnes.

Il faut préciser que la nouvelle certification ISO 27001-HDS est délivrée aux hébergeurs pour deux types d'activité, un hébergeur pouvant être certifié HDS pour les deux activités, pour l'une ou pour l'autre :

- Hébergeur d'infrastructure physique ;
- Hébergeur infogéreur.

L'hébergeur HDS est certifié en tant que tel après un audit en deux temps, **un audit documentaire suivi d'un audit sur site**. Cette certification ISO 27001-HDS est délivrée **pour une durée de trois ans**. La procédure prévoit un **contrôle annuel**, effectué par l'organisme certificateur ayant conduit la phase d'audit.

[10] Norme ISO/CEI 27001 « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences ».

La société française DropCloud certifiée ISO 27001-HDS

DropCloud est un **éditeur français de solutions logicielles** pour entreprises, PME et TPE, collectivités et autres (associations, professionnels libéraux…). Les solutions DropCloud ont pour objectif de **faciliter la gestion des données en ligne**, de sécuriser les sauvegardes, les échanges et le partage de fichiers.

Les professionnels de santé sont notamment concernés, car DropCloud a développé une offre dédiée, qui intègre les exigences propres au secteur.

Les trois solutions DropCloud Santé sont :

- WeSend Santé pour l'envoi de fichiers volumineux ;
- WeDrop Santé pour le partage de fichiers ;
- NeoBe Santé pour la sauvegarde en ligne.

En 2019, la société **DropCloud s'est engagée dans la nouvelle démarche de certification HDS**. Elle souhaite ainsi accompagner au mieux les professionnels de santé, eu égard à leurs obligations légales et à leur responsabilité sur le thème du traitement des données personnelles.

Le 4 décembre 2019, l'Agence française de normalisation (AFNOR) a délivré à DropCloud sa **certification ISO 27001-HDS**. Elle porte sur les deux périmètres identifiés par l'ASIP Santé : l'activité d'hébergeur d'infrastructure physique et l'activité d'hébergeur infogéreur. Les différents logiciels DropCloud Santé bénéficient d'un environnement sécurisé et certifié ISO 27001-HDS.

Les bonnes pratiques en matière d'échange de données médicales

Comment choisir sa solution de transfert de fichiers médicaux en ligne ?

Le choix d'une solution d'envoi en ligne de fichiers médicaux est commandé par un critère principal et impérieux : **la sécurité**. Dans cette logique, l'utilisation d'une plateforme certifiée ISO 27001-HDS est un prérequis indispensable. Le professionnel de santé doit être certain de **confier ses fichiers à un tiers expert**, capable d'en assurer la protection.

Autour du thème général de la sécurisation des fichiers médicaux, le professionnel de santé peut rester attentif aux **différentes fonctionnalités offertes** par l'outil de transfert. Il peut s'intéresser aux critères suivants :

- Les options de gestion des fichiers envoyés (stockage et disponibilité) ;
- Les différentes options de sécurité au moment de l'envoi ;
- Le suivi des fichiers envoyés.

Le choix d'un outil de transfert de fichier est éclairé par un critère secondaire, mais très important : **la capacité d'envoi.** En effet, les professionnels de l'univers médical doivent **profiter d'un système efficace** qui ne pose pas, ou peu de limites en la matière, car les dossiers médicaux à envoyer peuvent contenir des documents très lourds, comme des clichés d'imagerie médicale.

Les limites des messageries classiques

Les boîtes mail classiques et les plateformes de transfert de fichiers en libre accès ne sont pas adaptées au traitement des données de santé. **Leur niveau de sécurité et leurs fonctionnalités sont insuffisants**. Il faut bien comprendre que la phase d'envoi ou de transfert d'un courrier électronique est un moment critique, qui **rend vos données vulnérables** si des dispositifs de sécurité ne sont pas mis en place pour les protéger.

Les pirates du web le savent bien et **exploitent cette faiblesse pour accéder à des données**, de santé ou autres, **qui auraient dû rester confidentielles**. Crypter des fichiers en chiffrant leurs données est un exemple de protection avancée, qui ne fait pas partie des fonctionnalités de base offertes par les messageries courantes.

Les limites des messageries classiques ne concernent pas seulement la sécurité des fichiers envoyés. Évidemment, **la capacité d'envoi de ces messageries est assez faible**, les fichiers en pièces jointes ne pouvant pas excéder un certain poids, entre 10 et 25 Mo, selon les systèmes.

Le cas particulier des messageries de santé MSSanté

L'État, via l'ANS (Agence du Numérique en Santé, Anciennement ASIP Santé) a développé un **service de messageries sécurisées pour les professionnels du secteur : MSSanté.** MSSanté est un dispositif de messageries électroniques réservé aux professionnels de santé au sein d'un espace de confiance.

Ces messageries doivent permettre à tous les professionnels de santé **d'échanger entre eux par email**, rapidement et en toute sécurité, des données personnelles de santé de leurs patients, dans le respect de la règlementation en vigueur. Les messageries de **l'Espace de Confiance MSSanté** possèdent un annuaire commun et certifié de l'ensemble des professionnels de santé.

L'ANS avec les Ordres de santé, a développé sa propre messagerie MSSanté baptisée **Mailiz**. Cette messagerie a l'avantage d'être **gratuite**. Elle est intégrée à l'Espace de confiance MSSanté, qui réunit des professionnels, des structures et des industriels de santé.

Offrant les garanties de sécurité indispensables au traitement des données personnelles, cette messagerie reste contrainte par ses caractéristiques techniques :

- La taille maximale des pièces jointes : 10 Mo ;
- Le nombre maximal de destinataires : 40 ;
- Un espace de stockage limité à 2 Go.

La sécurité et la confidentialité sont les atouts de cette solution. **En revanche, elle reste limitée, comme toute boite email traditionnelle à des envois de petits volumes et dans le cas de la messagerie MSSanté à des échanges entre professionnels.**

Les avantages et les fonctionnalités de la solution WeSend Santé

WeSend Santé est la solution proposée par DropCloud aux professionnels de santé, pour **le transfert des fichiers médicaux jusqu'à 10 Go de façon totalement sécurisée**.

Cette offre repose sur la **double certification ISO 27001-HDS**. Les fichiers envoyés sont hébergés sur des **serveurs localisés en France, en mode SaaS**. Très facile à prendre en main, l'outil propose une **interface utilisateur simple et intuitive**.

La solution WeSend Santé permet d'envoyer des fichiers contenant des données de santé en toute sécurité. Elle s'appuie pour cela sur des technologies avancées :

- Certificat SSL pour sécuriser le transfert des fichiers ;
- Chiffrement des données AES256 (Cryptographie) ;
- Double authentification.

L'outil facilite l'envoi des fichiers lourds, avec une **prise en charge de pièces jointes jusqu'à 10 Go**. Parmi toutes les fonctionnalités et options proposées, WeSend Santé permet notamment d'inviter un autre utilisateur à déposer et envoyer des fichiers. D'autres dispositifs de sécurité et de gestion sont appréciables :

- La traçabilité des fichiers envoyés, le suivi en temps réel des actions des destinataires ;
- Le stockage des fichiers (temporaire ou permanent).
- Un annuaire des contacts

DropCloud santé

Solutions sécurisées du travail en ligne

Solutions du travail en ligne des professionnels de santé.

WeSend santé

Envoi de fichiers volumineux

Envoyez vos documents médicaux de façon totalement sécurisée. Ils sont mis à la disposition de vos destinataires via un lien de téléchargement. En environnement certifié ISO27001 HDS, WeSend Santé propose de nombreuses fonctionnalités d'intégration et sécurisation.

Partage et synchronisation de fichiers

Partagez vos documents et collaborez en ligne de façon simple et sécurisée. Accordez des droits à chaque interlocuteur, créez des répertoires pour organiser l'activité. Chacun peut visualiser, déposer, commenter les documents et fichiers.

WeDrop santé

NeoBe santé

Sauvegarde en ligne sécurisée

Sauvegarde et restitution des données médicales professionnelles. Vos fichiers et bases de données sont stockés sur vos postes ou vos serveurs, votre environnement est Mac ou Pc, NeoBe en garantit la sauvegarde sur ses infrastructures exclusivement françaises. certifiées ISO27001 HDS

Solutions cértifiées ISO27001 HDS : Hébergeur des Données de Santé

DropCloud et l'ensemble de ses solutions bénéficient du certificat ISO27001 HDS pour l'hébergement de données de santé.

Certification HDS ISO 27001 - HDS

afaq ISO 27001 Sécurité de l'information AFNOR CERTIFICATION

afaq HDS Hébergeur de Données de Santé AFNOR CERTIFICATION

DropCloud
11 av du Val de Fontenay
94120 FONTENAY SOUS BOIS
01.46.08.83.70 - dropcloud-sante.fr - info@dropcloud.com