# Cloud collaboratif santé certifié HDS et 100% français !

**Medical Cloud est une solution en ligne de sauvegarde, de synchronisation et de partage de documents médicaux. S'appuyant sur les serveurs de son partenaire certifié « hébergeur de données de santé » (HDS) par la HAS et certifié ISO 27001, les données de santé restent physiquement 100% en France.**

Vos éléments sauvegardés sont ainsi accessibles de partout via un simple navigateur web sans aucune installation. La connexion au service se fait via une connexion HTTPS avec une double authentification : un code à usage unique vous est envoyé par SMS en plus de votre login/mot de passe pour chaque nouvelle connexion ou tout nouvel appareil associé à votre compte.

Pour simplifier votre utilisation au quotidien, des logiciels de synchronisation MacOS et Windows sont mis à disposition pour répliquer en temps réel vos dossiers souhaités dans notre cloud et sur tous vos autres appareils disposant également de l'application de synchronisation. Tout document modifié avec l'un de vos appareils est instantanément synchronisé et disponible sur vos autres appareils. Nos applications pour mobiles et tablettes iOS ou Android vous permettent également de consulter et/ou éditer vos documents lorsque vous êtes en déplacement hors de votre cabinet.

Outre la sauvegarde des données sensibles de votre cabinet médical, Medical Cloud permet également de réaliser le partage facile de documents vers vos confrères ou vers vos patients. Finis les documents transférés par SMS, en pièce-jointe d'emails, ou via des messageries non sécurisés. Avec Medical Cloud, le partage d'une photo ou d'un autre document est simplissime : partagée par un lien et sécurisée par un mot de passe, la donnée reste hébergée dans notre cloud sécurisé. Cela laisse libre court à de nombreuses utilisations : le partage d'une photo à un confrère pour avoir un avis médical, la transmission d'une ordonnance à un patient, la collaboration avec une secrétaire médicale exerçant à distance… Il est également possible de créer un dossier où le patient peut déposer des documents à vous transmettre !

Vos documents étant synchronisés à chaque modification, les évènements inattendus au cabinet entraînant une perte des données deviennent moins anxiogènes : vous pouvez récupérer vos données en quelques minutes (durée variable en fonction du volume) pour une reprise rapide de votre activité sur un nouveau poste informatique.

Enfin, l'ensemble de nos serveurs sont protégés par un PRA (Plan de Relance d'Activité) et copiés toutes les 30 minutes sur 2 sites géographiquement distants permettant une reprise des services sous 4h en cas de destruction physique de ces derniers (ex : incendie). Nos serveurs bénéficient également d'une redondance de 14 jours à raison de 2 sauvegardes complètes par jour : cette approche permet de vous protéger des conséquences d'un ransomware/rançongiciel en restaurant vos données dans un état sauvegardé avant le préjudice. Enfin, tous nos serveurs présentent un chiffrement côté serveur de type « Encryption at rest » sur l'ensemble de nos disques afin de renforcer la confidentialité des données déposées.

Medical Cloud devient le vrai compagnon du professionnel de santé pour la gestion de ses données sensibles : documents, photos, scanners, bases de données de logiciels de gestion, documents comptables, etc.

## A PROPOS DE MEDICAL CLOUD

*Fondée en 2013, Medical Cloud est une entreprise 100% française qui développe des solutions logicielles dans le domaine de la santé.*

**Pour en savoir plus**

www.medicalcloud.fr
MedicalCloudFr
MedicalCloud.SaaS

**CRÉEZ VOTRE COMPTE GRATUIT**

## RGPD et Données de Santé

# De la collecte à l'usage des données de santé






### QU'EST-CE QU'UNE DONNÉE DE SANTÉ ?

Le Règlement Européen sur la Protection des Données, entré en vigueur en mai 2018, prévoit que les données de santé à caractère personnel sont les « données relatives à la santé physique ou mentale, passée, présente ou future, 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 ».

### SUIS-JE CONCERNÉ DANS LE CADRE DE MON EXERCICE ?

En tant que professionnel de santé, vous collectez ou échangez des informations sur vos patients pour assurer leur suivi que ce soit dans le dossier « patient » (papier ou informatique) ou dans le cadre de l'utilisation d'un service en ligne de gestion des rendez-vous.

Tout professionnel de santé est donc concerné par la gestion et la sécurité des données de santé de ses patients : il est responsable de la collecte et du traitement de ses données.

### QUELLES INFORMATIONS PUIS-JE COLLECTER SUR MES PATIENTS ?

Les données que vous collectez sur les patients doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.

### QUELLES SONT MES OBLIGATIONS ?

Vous devez prendre toutes les précautions nécessaires pour empê-cher l'accès aux données de santé à des tiers, que vous hébergiez vos données en local, à votre cabinet, ou à distance.

### QUELLES OBLIGATIONS SI J'HÉBERGE LES DONNÉES À MON CABINET ?

Vous devez vous assurer de limiter l'accès aux données de santé en maintenant à jour vos environnements de travail et en les sécurisant. L'Agence Nationale de la Sécurité des Système d'Information (ANSSI) publie un très bon guide de bonnes pratiques sur le sujet. Attention également à bien veiller à ce que vos prestataires informatiques n'accèdent pas aux données et de limiter l'accès à vos personnels administratifs aux seules données indispensables au suivi de vos patients et à la qualité des soins prodigués.

### QUELLES OBLIGATIONS SI J'HÉBERGE LES DONNÉES À DISTANCE ?

Vous hébergez déjà peut-être vos données à distance sans le savoir : en effet si vous utilisez un logiciel « en ligne » pour la gestion de vos patients (ou RDV patient) vous êtes concernés. En qualité de propriétaire des données, vous devez respecter des règles de sécurité pour protéger les données des patients contre des accès non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle. Ainsi, il est de votre responsabilité de vous assurer que vos prestataires (par exemple : éditeurs de logiciels métiers) garantissent un niveau de sécurité adapté au risque sur les données de santé. La certification Hébergeur de Données de Santé (certification HDS délivrée par la HAS) est le gage de conformité pour la partie hébergement.

### QUID DE LA SAUVEGARDE DE MES DONNÉES ?

Si vous hébergez tout ou partie de vos données en local, il est naturel de vouloir les sauvegarder afin de vous prémunir de vols ou autres évènements inattendus (incendie, panne…). La sauvegarde locale répond aux mêmes obligations que celles indiquées dans le paragraphe précédent.

### MES APPAREILS NOMADES SONT-ILS DE POTENTIELS LIEUX D'HÉBERGEMENT DE DONNÉES DE SANTÉ ?

Vous utilisez peut-être votre portable ou tablette pour prendre des photos de vos patients ou de leurs documents administratifs médicaux. Compte-tenu des risques de pertes et vols sur ce type d'appareil, il est déconseillé de stocker des données sensibles dans la mémoire de l'appareil pour une consultation ultérieure. Il est ainsi recommandé de transférer les données vers votre ordinateur de votre cabinet dès que possible, ou d'utiliser les applications mobiles compatibles de vos fournisseurs habituels pour les consulter à distance.

### EST-IL POSSIBLE DE TRANSMETTRE LES DONNÉES DE SANTÉ À TOUS LES PROFESSIONNELS DE SANTÉ ?

Vous devez limiter l'accès aux données de santé de vos patients : seules certaines personnes sont autorisées, au regard de leurs missions, à accéder à celles-ci, tels qu'une équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, une secrétaire médicale, des organismes d'assurance maladie pour le remboursement des actes et prestations et leur contrôle, etc. Ces personnes n'accèdent qu'aux données nécessaires à l'exercice de leur mission.

Trois exceptions existent toutefois au partage de données de santé entre confrères et pour lesquelles il conviendra de remettre les données au patient en prenant soin de bien l'éclairer sur les conséquences de cette transmission. Ainsi, il n'est pas possible de partager directement les données de santé d'un patient : au médecin d'une compagnie d'assurances, au médecin expert judiciaire et au médecin du travail.

### SOUS QUELLES CONDITIONS PUIS-JE PARTAGER MES DONNÉES DE SANTÉ AVEC DES CONFRÈRES OU SECRÉTAIRES DE MON CABINET ?

Si l'accès aux données de santé est justifié au regard de leur mission, il est possible de partager vos données de santé avec vos confrères et/ou secrétaires médicaux de façon régulière dans le cadre de leurs activités. Toutefois, vous devez vous assurer du respect des règles de sécurité pour protéger les données des patients contre des accès non autorisés ou illicites : le partage d'identifiants de connexion/d'accès aux données de santé entre utilisateurs est à proscrire. Chaque professionnel de santé accédant aux données de façon régulière doit disposer de ses propres identifiants d'accès permettant d'assurer une traçabilité des traitements réalisés sur celles-ci.

### COMMENT FAIRE POUR PARTAGER DES DONNÉES DE SANTÉ EN TOUTE LÉGALITÉ ?

Vous ne publieriez jamais les données de santé de vos patients sur les réseaux sociaux ? Et pourtant partager une photo ou un document médical par SMS ou via votre messagerie email habituelle relève de la même erreur en termes de sécurité. Les bonnes solutions sont d'utiliser un service de Messagerie Sécurisé de Santé (MSSanté) pour le partage entre confrères et/ou, plus généralement, de déposer les fichiers à partager sur un service hébergé sur un serveur HDS et de fournir un lien sécurisé à vos patients ou vos confrères pour y accéder.

### QUELS SONT LES RISQUES ENCOURUS EN CAS D'UTILISATION D'UNE SOLUTION NON AGRÉÉE PAR LA HAS ?

L'hébergement ou le traitement d'une base de données de santé à caractère personnel sans certification HDS selon le référentiel HAS (prévu par l'article L. 1111-8) est puni par la loi de trois ans d'emprisonnement et de 45 000 euros d'amende (article L1115-1 du Code de la Santé Publique). Les solutions de cloud publiques telles que Dropbox, iCloud ou Box ne sont pas certifiées HDS et ne sont donc pas conformes pour l'hébergement de données de santé en France.

Par ailleurs, le Cloud Act et le FISA (Foreign Intelligence Surveillance Act) permettent aux autorités américaines de contraindre les sociétés de droit américain, telles que celles citées précédemment, à fournir sans mandat les données stockées sur leurs datacenters, même lorsque ceux-ci sont situés en Europe, et sans même informer les personnes concernées. En 2021, la CNIL s'est ainsi clairement positionnée en qualifiant de « non adapté » l'hébergement de données de santé de citoyens européens par des sociétés de droits américains même si elles disposaient d'une certification HDS.

medical cloud

117 rue de Charenton 75012 Paris
01.84.25.16.25
contact@medicalcloud.fr
www.medicalcloud.fr