Conditions Générales d'Utilisation du site omnidoc.fr

Dernière mise à jour : 21 avril 2022.

1. Préambule

Les présentes Conditions Générales d'Utilisation (ci-après « CGU ») sont conclues entre « Omnidoc.fr», site dédié à la mise en relation et à la réalisation de télé-expertises, et entre les praticiens de santé inscrits sur le site (ci-après les « Utilisateurs ») qui utilisent le site accessible notamment à l'adresse www.app.omnidoc.fr (ci-après le « Site »).

Le Site est édité par la société Omnidoc, SAS au capital social de 1000 euros dont le siège social est situé 12 rue Anselme, 93400 Saint-Ouen-sur-Seine, Paris, et est immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 847 506 144.

Les données de santé à caractère personnel collectées et traitées dans le cadre de l'utilisation de la plateforme Omnidoc sont hébergées auprès d'un hébergeur agréé de santé, conformément aux dispositions de l'article L.1111-8 du Code de la santé publique. En particulier, les données de santé et les serveurs sont hébergés par : Claranet (ci-après "l'Hébergeur").

Société par actions simplifiée au capital de 10.069.020 euros
Siège social : 2 rue Kellermann, 59100 Roubaix
RCS Lille 424 761 419

Les serveurs sont administrés par Claranet, infogéreur certifié pour l'hébergement et l'infogérance des données de santé (ci-après "l'Infogéreur").
Siège social : 2 rue Bréguet 75011 Paris
RCS de Paris B 419 632 286

2. Fonctionnalités du site

Omnidoc.fr est une plateforme de collaboration entre Praticiens de santé. Le Site permet plus particulièrement la réalisation de téléexpertises médicales, telles que définies dans la loi Hôpital Patient Santé et Territoires (HPST) de juillet 2009, et selon les conditions précisées dans l'avenant 6 à la convention médicale de 2016.

En particulier, le site assure :

- L'identification des acteurs
- La sécurité des données
- La traçabilité des échanges

Les données sont hébergées et infogérées par un infogéreur certifié pour l'hébergement de données de santé

(Claranet).

Les données de santé collectées lors des téléexpertises ne sont accessibles qu'aux Praticiens de santé ayant participé à leur réalisation.

3. Accès au Site

L'accès au Site et son utilisation sont réservés aux Médecins inscrits à l'Ordre national des médecins et titulaire d'un numéro RPPS en cours de validité ainsi qu'aux Infirmiers titulaire d'un numéro RPPS. Cette validité est contrôlée par comparaison avec la base de données RPPS mise à disposition par l'ANS et mise à jour quotidiennement.

3.1. Conditions d'ouverture de compte sur le Site

L'ouverture d'un compte Utilisateur sur le Site est subordonnée à la transmission du formulaire d'inscription dûment complété. Pour pouvoir bénéficier de tous les services du site, en particulier pour pouvoir demander ou répondre à une téléexpertise, l'utilisateur doit valider son profil, ce qu'il peut faire en utilisant les outils d'authentification de l'ANS (CPS ou eCPS) ou en soumettant une copie d'un justificatif (carte CPS ou carte d'identité) sur le site. Dans le premier cas, la validation est instantanée, dans le second, elle intervient dans les deux heures suivant la soumission (du lundi au vendredi de 9h à 19h).
En cas d'incohérence entre le formulaire transmis et la pièce justificative adressée, Omnidoc se réserve la possibilité de solliciter des informations complémentaires. Si les personnes souhaitant bénéficier du Site ne communiquent pas l'ensemble des informations demandées, ou si elles communiquent des informations inexactes et/ou incomplètes, leur inscription au Site ne sera pas validée et elles ne pourront pas utiliser les services mis à leur disposition sur le Site.

3.2. Acceptation des CGU

Dans le cadre de leur inscription au Site, les Utilisateurs prennent connaissance des présentes CGU et les acceptent formellement en poursuivant leur inscription. Omnidoc est susceptible de modifier unilatéralement les présentes CGU, ce dont elle informera en temps utile les Utilisateurs par tout moyen, notamment lors de leur identification et/ou connexion ultérieure au Site ou par email. A défaut d'acceptation des CGU modifiées, l'Utilisateur pourra voir son accès au Site suspendu.

4. Confidentialité et déontologie

Les mots de passe et identifiant de l'Utilisateur sont strictement personnels. L'utilisateur s'interdit de les communiquer à un tiers.
Dans le cas contraire, il supporte toutes les conséquences qui découleraient d'une utilisation du Site non conforme aux CGU de ses identifiant et mot de passe par une tierce personne.
En cas de divulgation involontaire, ou de présomption de divulgation involontaire, l'Utilisateur s'engage à prendre toutes précautions utiles et notamment à modifier sans délai son mot de passe via la rubrique prévue à cet effet et accessible sur le Site.
L'Utilisateur est soumis, dans ses relations avec ses patients et dans ses relations avec les autres Utilisateur, aux dispositions du Code de déontologie médicale et du Code de la santé. En particulier, l'Utilisateur s'interdit toute manœuvre constitutive d'une captation ou d'un détournement de clientèle.

5. Responsabilité

5.1. Responsabilité du site

Omnidoc est tenu à une obligation de moyen pour la délivrance du service accessible via le Site.

En particulier, Omnidoc n'est pas responsable en cas :

- de survenance d'un événement de force majeure ayant un impact sur le service du Site ;
- de problèmes liés au réseau internet ;

- de pannes ou dommages résultant des équipements de l'Utilisateur ou encore de la contamination du système informatique de l'Utilisateur par des virus, attaques et malveillances de tiers ;
- d'indisponibilité ou dysfonctionnement du Site quelle qu'en soit la raison ;
- d'utilisation du Site par l'Utilisateur non conforme aux présentes CGU.L'indisponibilité du service ne donne droit à aucune indemnité et la responsabilité d'Omnidoc ne saurait être engagée en cas de d'indisponibilité ou de dysfonctionnement du Site.

5.2. Responsabilité de l'Utilisateur

L'Utilisateur est seul responsable de l'utilisation du Site conformément à son usage, dans le respect des lois et règlements en vigueur et des présentes CGU. Ainsi, l'Utilisateur est seul responsable du contenu des messages échangés au moyen du Site.
Toute utilisation du Site préjudiciable au patient est susceptible d'engager la responsabilité de l'Utilisateur.
Omnidoc ne contrôle pas le contenu des messages échangés entre les Utilisateurs. En conséquence, les Utilisateurs sont seuls responsables des messages échangés et du contenu des messages.

6. Télé-expertise médicales

Le Site permet de réaliser des télé-expertises médicales. Une télé-expertise est une demande d'avis à distance, entre confrères, au sujet d'un patient du requérant.
Les informations relatives aux patients ne peuvent pas être partagées avec d'autres professionnels de santé qui ne seraient pas Utilisateurs du Site. La consultation des télé-expertises médicales est réservée à l'Utilisateur qui requiert une télé-expertise, et à celui qui y répond. Par conséquent, le patient ne peut maîtriser le contenu où les accès à son dossier en dehors des cas prévus à l'article suivant.

7. Données à caractère personnel et secret médical

7.1. Définitions

Au titre de la présente clause, les termes « **Autorité de Contrôle** » « **Données à Caractère Personnel** », « **Responsable du Traitement** » « **Sous-traitant** » « **Traitement** » « **Personnes Concernées** » « **Violation de Données à Caractère Personnel** » ont la signification donnée à ces termes à l'article 4 du Règlement Européen 2016/679 du 27 avril 2016 RGPD (ci-après « **RGPD** »).

« **Règlementation Applicable en matière de Protection des Données** » signifie le RGPD et la loi française n° 78-17 du 6 janvier 1978, dite loi informatique et libertés, ainsi que toute loi nationale applicable transposant la directive européenne 2002/058/CE du 12 juillet 2002, dite directive e-Privacy, telle que régulièrement mise à jour, modifiée et/ou remplacée.

7.2. Description des différents Traitements mis en œuvre

Dans le cadre de la fourniture des services de téléexpertise via la plateforme Omnidoc au titre des présentes Conditions Générales d'Utilisation et, en fonction des modalités d'exercice du Praticien de santé, au titre du Contrat liant l'établissement de santé ou l'organisation libérale et Omnidoc, les Parties reconnaissent et acceptent que plusieurs types de Traitements de Données à Caractère Personnel sont mis en œuvre pour lesquels les rôles, obligations et responsabilités des Parties sont différents :

- **des Traitements relatifs à la gestion des réseaux de téléexpertise**, dans le cadre desquels l'établissement de santé et/ou l'organisation libérale agissent en qualité de Responsable du Traitement et Omnidoc agit en qualité de Sous-Traitant. **Pour ces Traitements, les obligations respectives des Parties sont définies au sein de l'article 4 de l'Accord sur le traitement des données à caractère personnel signé entre Omnidoc et l'établissement de santé ou l'organisation libérale**.

- **des Traitements relatifs à l'initiation d'un acte de téléexpertise par l'Utilisateur requérant,** dans le cadre duquel l'Utilisateur requérant agit en qualité de Responsable du Traitement et Omnidoc agit en

qualité de Sous-traitant. Pour ces Traitements, **les obligations respectives des Parties sont définies au sein de l'article 7 des présentes Conditions Générales d'Utilisation** ;

- **des Traitements relatifs à la gestion des actes de téléexpertise, à l'hébergement de la Plateforme Omnidoc, ainsi qu'à la fourniture des services associés**, dans le cadre desquels :
    - **lorsque le Praticien de santé, Utilisateur, exerce au sein d'un établissement de santé**, ledit établissement de santé agit en qualité de Responsable du Traitement et Omnidoc agit en qualité de Sous-Traitant. Pour ces Traitements, **les obligations respectives des Parties sont définies au sein de l'article 4 de l'Accord sur le traitement des données à caractère personnel signé entre Omnidoc et l'établissement de santé** ;
    - **lorsque le Praticien de santé, Utilisateur, exerce à titre individuel ou au sein d'une organisation libérale**, le Praticien de santé, Utilisateur, agit en qualité de Responsable du Traitement et Omnidoc agit en qualité de Sous-traitant. Pour ces Traitements, **les obligations respectives des Parties sont définies au sein de l'article 7 des présentes Conditions Générales d'Utilisation** ;

- **des Traitements relatifs à la fourniture de comptes utilisateurs uniques aux Praticiens de santé** dans le cadre desquels Omnidoc agit en qualité de Responsable du Traitement et les Praticiens de santé, Utilisateurs, sont des Personnes Concernées par le Traitement. Pour ces Traitements, les informations relatives à la nature et aux caractéristiques du Traitement figurent au sein de la Politique de Confidentialité d'Omnidoc accessible via le lien hypertexte suivant : https://omnidoc.fr/donnees-personnelles.

Les stipulations suivantes ont donc uniquement vocation à s'appliquer aux Traitements mis en œuvre dans le cadre de la gestion de l'initiation d'un acte de téléexpertise par l'Utilisateur requérant, la gestion des actes de téléexpertises des Praticiens de santé, Utilisateurs requis, au titre de leur exercice individuel et/ou dans le cadre d'une organisation libérale.

7.3. Obligation d'Omnidoc vis-à-vis de l'Utilisateur

Dans le cadre de la fourniture de la plateforme Omnidoc et des services associés aux Utilisateurs, Omnidoc est informé qu'il est susceptible d'avoir accès à ou plus généralement de traiter des Données à Caractère Personnel appartenant à l'Utilisateur, Praticien de santé et à ses patients et ainsi à mettre en œuvre des traitements de Données à Caractère Personnel, en qualité de Sous-Traitant dont les modalités sont précisées en Annexe 1 des présentes.

A ce titre, Omnidoc s'engage à traiter les données qui lui sont confiées par l'Utilisateur, requérant ou requis, dans le strict respect des présentes stipulations contractuelles et de la Règlementation Applicable en matière de Protection des Données.

Dans le cadre des prestations fournies à l'Utilisateur, Omnidoc mettra en œuvre toutes les mesures techniques et organisationnelles adaptées à l'état des connaissances, au contexte, aux finalités du Traitement et aux risques afin de protéger les Données à Caractère Personnel et prendra toutes les précautions nécessaires pour préserver la sécurité, la disponibilité, la confidentialité et l'intégrité de ces Données à Caractère Personnel, notamment contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé.

A la date de signature des présentes, les mesures de sécurité mises en place sont listées en Annexe 2. L'Utilisateur reconnaît et accepte que les mesures de sécurité sont sujettes à des progrès et développements techniques. Dans ce contexte, Omnidoc contrôlera régulièrement l'adéquation des mesures de sécurité prises et pourra les mettre à jour ou les modifier pendant l'exécution des présentes Conditions Générales d'Utilisateur, sous réserve que ces mises à jour et ces modifications ne dégradent pas ou ne diminuent pas la sécurité globale des services fournis aux Utilisateurs.

Par ailleurs, Omnidoc s'engage notamment à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) énoncée(s) en Annexe 1 et conformément aux instructions de l'Utilisateur. Si Omnidoc considère qu'une instruction constitue une violation de la Règlementation Applicable en matière de Protection des Données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement l'Utilisateur,
- Informer l'Utilisateur s'il est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis,
- Prendre toutes précautions utiles pour garantir la confidentialité des Données à Caractère Personnel traitées dans le cadre des présentes Conditions Générales d'Utilisation,
- Veiller à ce que les personnes autorisées à traiter les Données à Caractère Personnel en vertu des présentes Conditions Générales d'Utilisation s'engagent à respecter elles-mêmes la confidentialité et reçoivent la formation nécessaire en matière de protection des Données à Caractère Personnel,
- Aider l'Utilisateur pour la réalisation d'analyses d'impact relatives à la protection des données et pour la réalisation éventuelle de la consultation préalable de l'Autorité de Contrôle,
- Indiquer à l'Utilisateur si le Traitement fait l'objet d'un transfert de données hors de l'Union Européenne, le cas échéant apporter les éléments de preuve exigés par le RGPD, notamment la signature des clauses contractuelles types de la commission européenne concernant un transfert de données dans un pays n'étant pas considéré par la Commission Européenne comme offrant une protection adéquate. Il est à cet égard précisé que les transferts de données hors de l'Union Européenne existant au jour de la signature des présentes sont listés en Annexe 1.

7.4. Sous-traitance

Omnidoc peut faire appel à un Sous-Traitant pour mener des activités de Traitement spécifiques. Il est à cet égard précisé qu'au jour de la signature des présentes, la liste des sous-traitants ultérieurs autorisés à intervenir figure en Annexe 1. Dans le cas où Omnidoc souhaiterait apporter une modification à la liste des sous-traitants ultérieurs autorisés, il informe préalablement et par écrit l'Utilisateur de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants ultérieurs. Cette information, adressée au point de contact mentionné au sein de l'article 7.10, doit indiquer clairement les activités de Traitement sous-traitées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance. L'Utilisateur dispose d'un délai de trente (30) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si l'Utilisateur n'a pas émis d'objection pendant le délai susvisé.

Il appartient à Omnidoc de s'assurer que le sous-traitant ultérieur présente les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences de la Règlementation Applicable en matière de Protection des Données. Omnidoc s'engage à reporter sur le sous-traitant ultérieur, dans le cadre d'un contrat écrit, l'ensemble des obligations mises à sa charge par les présentes. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, Omnidoc demeure pleinement responsable devant le Utilisateur.

7.5. Exercice des droits des personnes

Dans la mesure du possible, Omnidoc aidera le Utilisateur à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des Personnes Concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Si les Personnes Concernées venaient à exercer auprès d'Omnidoc des demandes d'exercice de leurs droits, ce dernier doit adresser ces demandes, dans les meilleurs délais et au plus tard dans les huit (8) jours ouvrés, par courrier électronique à l'adresse du responsable de la protection des données de l'Utilisateur.

7.6. Notification des Violations de Données à Caractère Personnel

Omnidoc notifie à l'Utilisateur toute violation de données à caractère personnel dans les meilleurs délais et en tout état de cause dans un délai de (48) heures après en avoir pris connaissance par email à l'adresse du responsable de la protection des données de l'Utilisateur. Cette notification, adressée au point de contact mentionné au sein de l'Article 7.10., est accompagnée de la description de la violation, les données concernées, la cause et toute documentation utile afin de permettre à l'Utilisateur, si nécessaire, de notifier cette violation à l'Autorité de Contrôle compétente.

7.7. Sort des données

A l'expiration de la relation contractuelle entre les Parties, pour quelque cause que ce soit, Omnidoc devra sans délai et en fonction de la demande de l'Utilisateur, soit détruire les données et toute copie quel qu'en soit le support, soit restituer les données et détruire les copies existantes quel qu'en soit le support, sauf à ce qu'il soit tenu de conserver les données en application de la Réglementation Applicable en matière de Protection des Données, ce dont il s'engage à informer l'Utilisateur.

Il appartiendra à Omnidoc de s'assurer que toutes données ou copies de données qui auraient pu être transmises à un tiers soient également détruites.

En tout état de cause, Omnidoc devra apporter la preuve de ces destructions à première demande de l'Utilisateur.

7.8 Audit

L'Utilisateur pourra faire procéder, une fois par an, par un cabinet d'audit tenu au secret professionnel et agréé par les deux Parties, à l'examen de tout élément permettant de s'assurer de la bonne exécution des stipulations définies au sein de l'article 7 des présentes Conditions Générales d'Utillisation. Cet audit aura lieu aux heures d'ouverture des bureaux d'Omnidoc et sous réserve d'en avoir informé Omnidoc au moins trente (30) jours avant sa mise en œuvre, par lettre recommandée avec accusé de réception. Les frais d'audit seront à la charge de l'Utilisateur sauf dans le cas où l'audit révèlerait un manquement grave dans le cadre des obligations d'Omnidoc.

Cet audit pourra être effectué par un cabinet extérieur, pour autant que celui-ci n'exerce pas lui-même une activité concurrente de celle d'Omnidoc.

Un exemplaire du rapport d'audit sera remis à Omnidoc.

Si le rapport d'audit fait apparaître un non-respect des obligations d'Omnidoc, ce dernier s'engage, dans le cadre d'un plan d'action, à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai à convenir entre les Parties en fonction de la nature du manquement et de sa gravité.

Les Parties conviennent qu'en tout état de cause, la procédure d'audit ou son absence de mise en œuvre n'exonèrent d'aucune manière Omnidoc du respect de ses obligations contractuelles et ne peuvent être interprétées comme valant acceptation de la qualité des Prestations effectuées.

7.9 Obligations de l'Utilisateur vis-à-vis d'Omnidoc

L'Utilisateur s'engage à :

- Fournir à Omnidoc les données nécessaires à la fourniture des services prévus au sein des présentes Conditions Générales d'Utilisation,
- Documenter par écrit toute instruction concernant le Traitement des Données à Caractère Personnel par Omnidoc,
- Veiller, au préalable et pendant toute la durée de la relation contractuelle, au respect des obligations prévues par la Règlementation Applicable en matière de Protection des Données et les dispositions du Code de la Santé Publique, notamment
    - o à l'information des Personnes Concernées par le Traitement, en l'occurrence les patients e
    - o à l'information des patients concernant l'hébergement de leurs Données à Caractère Personnel de santé auprès d'un hébergeur bénéficiant de la certification Hébergement Données de Santé et à leur droit d'opposition à cet égard,
- Obtenir, lorsque cela s'avère nécessaire en raison des dispositions légales applicables, le consentement des Personnes Concernées, au partage de leurs données avec d'autres praticiens de santé

L'Utilisateur reconnaît et accepte qu'il est le seul responsable de l'exactitude des Données à Caractère Personnel fournies au Prestataire sur la plateforme Omnidoc ainsi que de la conformité et de la légalité du Traitement mis en œuvre via la plateforme Omnidoc.

Les Parties reconnaissent et acceptent que la téléexpertise représente un enjeu clé pour l'amélioration de l'organisation du système de santé et l'accès aux soins pour tous les assurés sur tout le territoire, que son développement et déploiement très récent nécessite que des analyses et études soient faites afin d'améliorer le service fourni.

En dépit des stipulations figurant au sein de l'article 7.2. ci-dessus, l'Utilisateur reconnaît avoir été informé par Omnidoc de son intention de réutiliser certaines des Données à Caractère Personnel traitées dans le cadre de la gestion de l'initiation d'une téléexpertise et la gestion des actes de téléexpertise à des fins d'amélioration de sa solution par Omnidoc et d'élaboration et d'exploitation de statistiques relatives au parcours de soins. A toutes fins utiles, il est précisé qu'Omnidoc ne traitera dans ce contexte aucune donnée de santé, que ce soit des données relatives à l'identité du patient ou des données médicales. Omnidoc utilisera uniquement les données d'identification des Utilisateurs, requérants et des requis, leur appartenance ou non à un réseau, leur profession et spécialité, les logs d'accès à la Plateforme, ainsi que les métadonnées liées à l'acte de téléexpertise, à savoir date et heure d'initiation de la téléexpertise, statut de la téléexpertise (en cours, terminée), date de fin de la téléexpertise, code d'acte**.**

Dans ce contexte, l'Utilisateur :

- reconnaît et accepte que les finalités de Traitement envisagées par Omnidoc lui semblent compatibles avec le Traitement initial mis en œuvre au moyen des Données à Caractère Personnel mentionnées au sein de l'Annexe 1.

- donne ainsi à Omnidoc l'autorisation de réutiliser certaines Données à Caractère Personnel mentionnées au sein de l'Annexe 1 (à savoir de manière exhaustive, les données d'identification des requérants et des requis, leur appartenance ou non à un réseau, leur profession et spécialité, les logs d'accès à la Plateforme, ainsi que les métadonnées liées à l'acte de téléexpertise, à savoir date et heure d'initiation de la téléexpertise, statut de la téléexpertise (en cours, terminée), date de fin de la téléexpertise, code d'acte), à des fins d'amélioration de sa solution de téléexpertise et d'élaboration et l'exploitation de statistiques relatives au parcours de soin.
- S'engage à informer les Personnes Concernées de la transmission de leurs données à Omnidoc à des fins d'amélioration de sa solution et d'élaboration et exploitation de statistiques relatives au parcours de soin.

7.10 Coordonnées du/des Délégués à la Protection des Données et des points de contact

- Coordonnées du point de contact d'Omnidoc

Omnidoc a procédé à la désignation d'un Délégué à la Protection des Données auprès de la CNIL qui peut être contacté à l'adresse suivante :

Omnidoc – 12 rue Anselme, 93400 Saint-Ouen ou contact_rgpd@omnidoc.fr

Pour toute question relative à la protection des Données à Caractère Personnel, l'Utilisateur est invité en priorité à contacter le Délégué à la Protection des Données d'Omnidoc qui agit en tant que point de contact pour Omnidoc.

- Coordonnées du point de contact de l'Utilisateur

Pour toute question relative à la protection des Données à Caractère Personnel, Omnidoc contactera l'Utilisateur au moyen de l'adresse email renseignée lors de la création de son compte sur la Plateforme.

Ces coordonnées seront également utilisées par Omnidoc pour procéder aux différentes notifications et/ou informations mentionnées au sein de cet Article 7.

ANNEXE 1 – DÉTAILS SUR LE TRAITEMENT MIS EN ŒUVRE

I. DÉTAIL SUR LE TRAITEMENT MIS EN ŒUVRE PAR OMNIDOC POUR LE COMPTE DE L'UTILISATEUR

Finalités et Objet du Traitement

Les Données à Caractère Personnel sont traitées par Omnidoc, en qualité de Sous-Traitant, afin de permettre aux Utilisateurs de mettre en œuvre des Traitements de :

- Gestion de l'initiation d'un acte de téléexpertise, hébergement des avis demandés et émis dans le cadre de la téléexpertise et transmission des conclusions de la téléexpertise aux patients, par l'Utilisateur requérant agissant ainsi en qualité de Responsable du Traitement ;

- Gestion et réalisation des actes téléexpertises : réalisation de l'acte de téléexpertise ; échanges de communications entre praticiens de santé ; hébergement des avis demandés et émis dans le cadre de la téléexpertise, par l'Utilisateur requis agissant ainsi en qualité de Responsable du Traitement.

Les Données à Caractère Personnel sont traitées par Omnidoc, Sous-Traitant, dans le cadre de la mise à disposition de la plateforme de téléexpertise et de la fourniture des services décrits dans les Conditions Générales d'Utilisation.

Nature du Traitement

Les Données à Caractère Personnel seront soumises aux activités de Traitement de base suivantes :

Collecte ; Organisation ; Structuration ; Conservation ; Extraction ; Consultation ; Communication par transmission ; Diffusion ; Comparaison ; Hébergement ; Saisie ; Enregistrement ; Modification et Effacement.

Maintenance et support informatique de la solution Omnidoc.

Durée du Traitement

Les Données à Caractère Personnel seront traitées conformément à la durée paramétrée par les Utilisateurs requis et/ou aux instructions de l'Utilisateur requis.

Ces durées de conservation sont notamment transmises à Omnidoc au moyen du paramétrage des durées de conservation sur la solution Omnidoc ou par tout autre moyen (email).

A noter que pour les Utilisateurs requis utilisant la solution Omnidoc dans le cadre de leur activité au sein d'un établissement de santé, la durée de conservation des actes de téléexpertise est fixée par l'établissement de santé.

A cet égard, il est précisé que la Solution Omnidoc est une solution de téléexpertise et qu'elle n'a pas vocation à se substituer aux dossiers médicaux des patients constitués et tenus par les Utilisateurs requérants et requis. Les Utilisateurs requérants et requis doivent télécharger le rapport de téléexpertise produit grâce à la solution Omnidoc à l'issue de la téléexpertise et l'intégrer aux dossiers médicaux de leurs patients afin que les informations qui y sont intégrées soient conservées au sein de ceux-ci pendant la durée nécessaire au suivi du patient et aux responsabilités médicales associées aux actes médicaux.

Dans la mesure où les durées de conservation des actes de téléexpertise sont déterminées par les Utilisateurs requis, les Utilisateurs requérants, à l'origine de l'initiation de l'acte de téléexpertise seront informés de la suppression imminente des données liées à l'acte de téléexpertise (conformément aux paramétrages des durées de conservation définis par les Utilisateurs requis) afin de leur permettre, les cas échéant, de télécharger tout rapport manquant et les intégrer aux dossiers médicaux de leurs patients.

Catégories de Personnes Concernées

Les Données à Caractère Personnel traitées concernent les catégories suivantes de Personnes Concernées suivantes :

- les Utilisateurs, praticiens de santé habilités, qui requièrent un avis (« requérant ») dans le cadre d'une procédure de téléexpertise ;
- les Utilisateurs, praticiens de santé habilités, qui reçoivent une demande d'avis (« requis ») dans le cadre d'une procédure de téléexpertise ;
- les patients faisant l'objet de la demande d'avis dans le cadre d'une téléexpertise.

Catégories de Données à Caractère Personnel concernées

Les Données à Caractère Personnel traitées concernent les catégories suivantes de données (y compris éventuellement les catégories particulières de données) :

- Concernant les Utilisateurs :
    - Concernant les requis : données d'identification (et notamment les noms, prénoms) ; numéro de téléphone et email professionnel; profession et lieu d'exercice ; numéro RPPS et AM ; liste des téléexpertises réalisées ; date de la demande de téléexpertise et de finalisation de la téléexpertise ; avis délivrés, comprenant donc des données de santé relatives à la fois aux pathologies des patients pour lesquels un avis est émis ainsi que les données relatives au diagnostic émis ; voix et image ; signature ; statut de la téléexpertise ; code d'acte ; statut de facturation.

    - Concernant les requérants : données d'identification (et notamment les noms, prénoms) numéro de téléphone et email professionnels; profession ; lieu d'exercice ; numéro RPPS et AM ; liste des téléexpertises demandées ; date de la demande de téléexpertise et de finalisation de la téléexpertise ; avis demandés pouvant comprendre des données de santé relatives aux pathologies des patients pour lesquels un avis est demandé ; voix et image ; signature ; statut de la téléexpertise ; code d'acte.

- Concernant les patients : données d'identification (et notamment les noms, prénoms, dates et lieu de naissance, genre), numéro de sécurité sociale ; régime de l'assuré ; numéro de téléphone ; adresse ; code caisse, code centre ; pathologie et éventuels antécédents médicaux ; tout élément communiqué par le requérant de manière spontanée et/ou demandé par le requis dans le cadre de l'acte de téléexpertise ; avis délivré concernant la requête de téléexpertise ; éventuellement images.

II. LISTE DES SOUS-TRAITANTS ULTÉRIEURS AUTORISÉS ET TRANSFERTS HORS UNION-EUROPÉENNE AUTORISÉS

La liste à jour des sous-traitants ultérieurs du Omnidoc autorisés à intervenir dans le cadre de la fourniture des prestations impliquant un Traitement de Données à Caractère Personnel est la suivante :

Identification du Sous-Traitant Ultérieur	**Nature et finalités des opérations de Traitement réalisées**	**Localisation des équipes impliquées** **En cas de transferts de données hors UE, garanties mises en œuvre**
Claranet	Hébergement et infogérance des serveurs hébergeant la plateforme et les bases de données. Il s'agit d'un Omnidoc bénéficiant de la certification Hébergeur de Données de Santé : https://www.claranet.fr/certification-hds.	Union Européenne
OVH	Envoi de SMS transmettant un code d'accès unique permettant de sécuriser l'accès à la plateforme. Envoi de SMS de rappel si une demande reste 5 jours sans réponse. Pas de traitement de données de santé.	Union Européenne
Twilio	Envoi de SMS transmettant un code d'accès unique permettant de sécuriser l'accès à la plateforme. Pas de traitement de données de santé.	Etats-Unis : transferts basés sur les Clauses Contractuelles types
Mailgun	Envoi d'emails transactionnels relatifs à l'activité réalisés sur la plateforme (réception d'une requête de la part d'un requérant ; réception d'un avis de la part d'un requis). Envoi de SMS de rappel si une demande reste 5 jours sans réponse. Pas de traitement de données de santé.	Etats-Unis : transferts basés sur les Clauses Contractuelles types
Google	Mise à disposition de tableaux de bord via Google Data Studio Pas de traitement de données de santé	Etats-Unis : transferts basés sur les Clauses Contractuelles types

ANNEXE 2 – MESURES DE SÉCURITÉ MISES EN ŒUVRE

Dans le cadre de l'exécution des prestations, Omnidoc met en œuvre les mesures de sécurité suivantes :

Authentification Forte

L'accès à la plateforme est réservé aux Utilisateurs, praticiens de santé enregistrés dans le répertoire RPPS. A l'inscription, leur identité est vérifiée automatiquement via les moyens d'authentification fournis par l'Agence du Numérique en Santé (Pro Santé Connect, CPS et eCPS) ou manuellement via la soumission d'un scan de carte d'identité ou de carte CPS.

Pour les connexions ultérieures, l'Utilisateur, praticien de santé, peut utiliser de nouveau sa carte CPS / eCPS ou une authentification deux facteurs via email / mot de passe et un code à usage unique envoyé par email ou par SMS. Lorsqu'il se connecte, l'Utilisateur peut décider de cocher la case "Se souvenir de l'appareil" qui permet à l'appareil de jouer le rôle de deuxième facteur lors des connexions ultérieurs (ie. l'email et le mot de passe suffisent si l'Utilisateur se connecte depuis le même appareil et qu'il a coché cette case lors de la précédente connexion).

Les établissements de santé clients de la solution ont également la possibilité d'avoir des comptes administrateurs pour faciliter l'intégration des données à leurs systèmes. Ces comptes sont créés, sur demande du client, par Omnidoc et sont également protégés par une authentification forte.

Certification HDS

Toutes les données hébergées et stockées sur la plateforme Omnidoc le sont sur les bases de données HDS info-gérées par Claranet (infogéreur certifié HDS : https://www.claranet.fr/certification-hds) mettant en place des mesures de sécurité fortes auditées dans le cadre de la certification HDS.

Chiffrement des Connexions Réseau

Toutes les connexions entre les Utilisateurs autorisés, ainsi que les requérants tiers (navigateur Web) et les serveurs Omnidoc se font via des appels chiffrés (HTTPS).

Chiffrement des Données à Caractère Personnel de Santé

Une téléexpertise contient des Données à Caractère Personnel de santé, à savoir des données d'identification du patient (nom, prénom et autres données administratives) et des données de santé (la description et les pièces jointes, ainsi que les avis et diagnostics émis). Toutes les données textuelles de santé sont chiffrées en base. Un accès frauduleux à la base de données ne permettrait donc pas d'obtenir de données de santé ni de les associer à un patient.

Omnidoc utilise une bibliothèque de cryptographie (cryptography.io) pour chiffrer les données avant de les stocker.

Secret Médical

Pour pouvoir déchiffrer ces données, il faut être l'auteur ou le destinataire de la demande. A noter que lorsque la demande est adressée à un groupe, par exemple à un service hospitalier, le destinataire est compris comme l'ensemble des médecins et assistants du groupe. Aucun autre Utilisateur et aucun employé d'Omnidoc (ni aucun employé du sous-traitant Claranet) n'a accès aux données de santé sous une forme non chiffrée.

Traçabilité des Actions

Toute opération de lecture et d'écriture en base est enregistrée dans les journaux systèmes et sauvegardée pour une durée de 6 mois.

Toutes les connexions aux serveurs sont également enregistrées.

Cookie Tiers

Aucun cookie non strictement nécessaire à la fourniture du service n'est déposé lorsque les Utilisateurs accèdent à la plateforme Omnidoc.

Système de permissions pour l'accès aux données

Un Utilisateur non connecté ou non validé n'a accès à aucune donnée sensible. Les Utilisateurs validés n'ont accès qu'aux téléexpertises dont ils sont l'auteur ou le destinataire.

A noter que lorsque la demande est adressée à un groupe, par exemple à un service hospitalier, le destinataire est compris comme l'ensemble des médecins et assistants du groupe.

Moyens permettant de garantir la disponibilité et la résilience constante des systèmes

CLARANET opère une plateforme de sauvegarde sur disques, basés sur la solution AVAMAR, et permettant d'assurer une sauvegarde et une restauration rapide des données. Afin d'assurer une conservation sécurisée des données de santé, les disques de sauvegarde sont chiffrés. Pour garantir un meilleur niveau de protection en cas d'incident majeur :

- sur le site d'hébergement : la plateforme de sauvegarde est physiquement située dans un datacenter différent de celui des serveurs de production. Cette plateforme de sauvegarde est physiquement hébergée au sein du Datacenter TELEHOUSE, distant de plus de 20 kilomètres des Datacenters hébergeant les données de santé
- sur le site de sauvegarde : les baies de sauvegarde sont répliquées sur le site EQUINIX PA2. Cette plateforme de sauvegarde est supervisée et administrée en 24x7 par les équipes techniques de CLARANET, pour identifier, isoler et résoudre tout incident ou perte de performance.

La bonne exécution des sauvegardes est supervisée par l'équipe en charge de la solution. Dans le cas où les sauvegardes échouent à cause d'une application spécifique d'Omnidoc ou de l'Utilisateur ou d'un composant

non managé par CLARANET (application client ou tiers), il sera demandé à l'Utilisateur ou à Omnidoc d'intervenir avec les ingénieurs CLARANET pour identifier et corriger la source du problème. Si l'Utilisateur et/ou Omnidoc ne peuvent ou ne veulent pas intervenir pour corriger ce type de problème, CLARANET ne pourra pas rétablir le service, et donc sera dans l'incapacité de restaurer les données en cas de besoin.

CLARANET travaillera en collaboration avec l'Utilisateur et Omnidoc pour résoudre tout problème lié aux opérations de sauvegarde.

CLARANET procèdera à une restauration de données chaque fois que cela sera nécessaire, ou sur requête spécifique d'Omnidoc et de l'Utilisateur, à condition que le ou les serveurs concernés soient pleinement opérationnels. Dans le cas où le serveur n'est plus opérationnel, il faudra dans un premier temps reconstruire ou reconfigurer le serveur avant de pouvoir procéder à la restauration de données. Si aucune restauration n'a été réalisée dans l'année, un test est proposé à Omnidoc par CLARANET. Un ou plusieurs éléments à restaurer sont sélectionnés par Omnidoc. CLARANET les restaure dans un dossier ou environnement ne perturbant pas le fonctionnement de l'application Omnidoc. Après validation de la correcte restauration, un PV est émis par CLARANET.

Audits réguliers de l'efficacité des Mesures Techniques et Organisationnelles

Le service de supervision de CLARANET a pour objectif de tester de façon automatique et régulière les équipements et services d'Omnidoc afin de générer une alerte lorsqu'un dysfonctionnement est identifié (service non accessible, seuil d'alerte atteint, etc).

L'outil de supervision Nagios/Centreon. Il s'appuie sur le protocole SNMP et des agents NRPE pour collecter les informations sur l'utilisation des ressources. Le protocole SNMP doit être actif sur chaque serveur, et les flux SNMP doivent être ouverts sur le LAN. CLARANET traite en 24x7 l'ensemble des alertes qui surviennent depuis les plateformes de supervision. Dans le cas d'un incident impactant le service (incident majeur), Omnidoc est notifié dans le respect des SLAs correspondant à la criticité de la plateforme. Le centre de supervision reçoit les indicateurs des différents dispositifs sur une console centralisée. En cas d'anomalie (dépassement de seuil, dispositif injoignable, …), un pré-diagnostic est effectué.

Détection des Violations de Données

Toutes les actions réalisées sur les serveurs font l'objet d'une journalisation. Les journaux sont conservés 6 mois comme indiqué ci-dessus.

Les types de logs remontés sont fonctions des éléments :

- Serveurs : Pour les serveurs, les événements sont automatiquement remontés par le système d'exploitation et enregistrés dans les journaux systèmes. Sont notamment enregistrés :
    - Les tentatives d'ouverture de session et leur résultat (réussite ou échec) o Les redémarrages des services ou du serveur o Certaines erreurs applicatives

  De plus, toute intervention (changement, incident, demande) sur les serveurs de production est enregistrée dans l'outil de ticketing par l'équipe d'administration Claranet e-santé.e.

- Composants de sécurité : Sur les composants de sécurité sont inclus dans le journal :
    - Les ouvertures et fermetures de session VPN, aussi bien pour le client VPN que pour les VPNs site-à-site.

- Les accès à l'interface d'administration. o les flux réseau qui sont bloquées par les règles en place.

De plus, toute intervention (changement, incident, demande) sur les serveurs de production est enregistrée dans l'outil de ticketing par l'équipe d'administration Claranet e-santé.

- Bases de données : Les interventions des administrateurs eSanté sur les bases de données se limitent à agir sur le moteur ou à mettre en place des scripts techniques et sauvegarder les traces conformément à la demande du Utilisateur (formulée via le prérequis administration).

- Applications : Toutes les traces applicatives sont enregistrées dans les journaux systèmes et sauvegardées pour une durée de 6 mois.

Les journaux des équipements de sécurité sont centralisés sur le serveur "syslog" Claranet e-santé. Cette centralisation assure notamment que si un équipement de sécurité venait à être compromis, les événements ayant mené à cette compromission seront quand même disponibles.

Claranet a mis en place la solution Wallix AdminBastion pour assurer la traçabilité. Cette solution permet de tracer les connexions et les actions menées par les équipes sur les équipements administrés.

Une console Web permet de suivre les connexions Windows en temps réel et d'en consulter le journal. Les actions déclenchées sur les plates-formes d'hébergement sont enregistrées en continu, ce qui permet une visualisation ultérieure.

L'enregistrement de ces sessions permet de connaître exactement les actions effectuées par les administrateurs facilitant ainsi la compréhension de tout événement anormal :

- Les actions réalisées lors de sessions Linux sont enregistrées sous format texte.
- Les sessions Windows sont visualisables via une interface web

Ces informations sont stockées dans la base de données interne de Wallix AdminBastion et sont conservées 12 mois sur bande dans l'armoire, sur le site de secours, uniquement accessible par des personnes habilitées.