ACCORD SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

CONDITIONS GENERALES

INTRODUCTION

La présente section vous permet de comprendre l'accord sur la protection des Données à caractère personnel (ci-après "l'Accord") ainsi que les conditions de modification du présent Accord et la version applicable, en fonction des Services que vous utilisez.

1. OBJET

Le présent Accord entre vous et Doctolib (ci-après les "Parties) a pour objet de définir les conditions dans lesquelles Doctolib s'engage à effectuer les opérations de traitement des Données à caractère personnel fournies par vous, en tant qu'Abonné/Utilisateur (ci-après "Vous"), pour l'exécution des Services.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter les dispositions de la loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et modifiée (ci-après « Loi Informatique et Libertés ») et du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après le "RGPD").

Afin d'éviter toute confusion, les Conditions générales de l'Accord concernent l'ensemble des Services de Doctolib alors que les Conditions spécifiques s'appliquent dans la mesure où vous utilisez certains Services qui impliquent certains traitements de données. Par conséquent, si vous ne souscrivez pas et/ou n'utilisez pas certains Services, Doctolib ne traitera pas les données mentionnées dans les Conditions spécifiques.

En fonction des Services auxquels vous avez souscrits ou que vous utilisez, les Conditions spécifiques ci-dessous, qui décrivent des traitements de Données à caractère personnel et Données de santé, et ce conformément à l'article 28(3) du RGPD, s'appliquent:

Conditions spécifiques pour les produits Doctolib :

- Conditions spécifiques au traitement "Paramétrage des comptes abonnés et utilisateurs",
- Conditions spécifiques au traitement "Gestion des rendez-vous et de l'agenda",
- Conditions spécifiques au traitement "Service de téléconsultation",
- Conditions spécifiques au traitement "Service de messagerie patients",
- Conditions spécifiques au traitement "Mise à disposition d'un logiciel de gestion de cabinet",
- Conditions spécifiques au traitement "Assistant de consultation",
- Conditions spécifiques au traitement "Dictée médicale",
- Conditions spécifiques au traitement "Gestionnaire de tâches intelligent",
- Conditions spécifiques au traitement "Mise à disposition du lecteur Doctolib",
- Conditions spécifiques au traitement "Mise à disposition d'un service de messagerie",
- Conditions spécifiques au traitement "Gestion des documents et des formulaires",
- Conditions spécifiques au traitement "Mise à disposition d'un service de transmission de prescriptions",
- Conditions spécifiques au traitement "Mise à disposition d'un service de pré-admission",
- Conditions spécifiques au traitement "Assistant téléphonique virtuel",
- Conditions spécifiques au traitement "Mise en place d'un Réseau de l'Organisation privé",
- Conditions spécifiques au traitement "Mise à disposition d'un service de messagerie".

En cas de conflit entre les Conditions générales et les Conditions spécifiques de l'Accord, les Conditions spécifiques prévalent.

En plus des Conditions générales et spécifiques, les mesures techniques et organisationnelles s'appliquent en fonction des Services auxquels vous avez souscrits ou que vous utilisez:

- les mesures techniques et organisationnelles standard applicables par défaut,

- les mesures techniques et organisationnelles applicables uniquement quand un Connecteur a été mis en place afin de permettre l'interopérabilité entre la Plateforme et les systèmes d'information tiers,
- les mesures techniques et organisationnelles appliquées par Doctolib dans le cadre du Service de Messagerie et Doctolib Connect Organisations.

L'Accord comprend également la liste des Sous-traitants ultérieurs utilisés afin de fournir les Services.

2. DEFINITIONS

Les définitions attachées au présent Accord sont disponibles ici.

3. ENTRÉE EN VIGUEUR ET DURÉE

Le présent Accord entre en vigueur à compter de la signature du Contrat auquel il est attaché et reste en vigueur durant toute la durée de la relation contractuelle vous unissant à Doctolib.

4. STATUT DES PARTIES

Les Parties sont convenues des définitions et obligations suivantes:

RESPONSABLE DE TRAITEMENT: Vous, en tant qu'Abonné et/ou Utilisateur.

SOUS-TRAITANT: Doctolib est le Sous-traitant en ce qui concerne le traitement des Données à caractère personnel et Données de santé mentionnées dans les Conditions spécifiques en fonction des Services auxquels vous avez souscrit ou que vous utilisez, qu'elles soient fournies directement ou indirectement à Doctolib par vous ou par un Administrateur qui s'est vu accorder par vous l'accès aux Services.

Vous autorisez Doctolib à traiter, pour votre compte, les Données à caractère personnel et Données de santé nécessaires à la fourniture des Services auxquels vous avez souscrit pour les finalités et dans le strict respect des conditions mentionnées ci-après.

Il est précisé que l'engagement de Doctolib se limite à l'installation, la fourniture des Services et l'hébergement de la Plateforme Doctolib, des Fiches Patients et du Portail Patient. A votre demande expresse et sous votre contrôle et votre responsabilité, Doctolib pourra néanmoins vous assister dans l'importation des Données de base patient au sein de la Plateforme Doctolib.

Dès lors que vous renseignez des Données à caractère personnel ou Données de santé de tiers dans la Plateforme Doctolib ou sur le Portail Patient, telles que des données de confrères ou de Patients, vous devez respecter les prescriptions légales sur l'information et/ou le consentement de ces tiers.

4.1. Vos obligations en tant qu'Utilisateur/Abonné agissant en qualité de Responsable de traitement

En votre qualité de Responsable de traitement, vous êtes seul responsable de la tenue du registre des traitements et le cas échéant de l'accomplissement des formalités préalables à la mise en œuvre du traitement de Données à caractère personnel et Données de santé auprès de la CNIL. Il vous appartient également d'informer les Personnes concernées notamment les confrères et les Patients de l'intégration de leur Données à caractère personnel et Données de santé dans la Plateforme Doctolib ainsi que des modalités d'exercice de leurs droits en mettant à disposition de ces derniers une fiche d'information.

En tant que Responsable de traitement, vous êtes seul responsable de l'exactitude, de la fiabilité et de la pertinence des Données à caractère personnel et Données de santé. Vous êtes notamment responsable de l'utilisation de la Plateforme Doctolib, des Services, des Documents et du Contenu Généré par l'Utilisateur que vous déposez, stockez, consultez et sortez de l'espace de stockage. Il vous incombe de faire toutes les déclarations nécessaires. Vous vous engagez à indemniser Doctolib, ses représentants, ses employés et ses Sous-traitants et à les décharger de toute responsabilité quant à l'ensemble des réclamations, responsabilités, dommages et frais (y compris les frais de justice, honoraires et frais) imposés à ou subis par Doctolib, ses représentants, employés, et Sous-traitants résultant du non-respect de cette obligation.

Les traitements mis en œuvre doivent répondre à un objectif précis et être justifiés au regard des missions et des activités des Acteurs de santé.

Vos activités comprennent des traitements permettant l'exercice des activités de prévention, de diagnostic et de soins des Patients ainsi que la gestion administrative de votre établissement de santé, centre de santé ou cabinet libéral.

Vous vous engagez à :

- respecter et faire respecter le secret médical ;
- mettre en place une politique d'habilitation, de gestion des droits d'accès et des rôles et privilèges, permettant de garantir la confidentialité des Données à caractère personnel et Données de santé et ce conformément à la volonté des Patients et de leurs Proches ;
- fournir à Doctolib les données nécessaires à la sous-traitance, incluant la liste des Données à caractère personnel et Données de santé à traiter, la base légale de traitement, les finalités de traitements ainsi que la durée de conservation des Données à caractère personnel et Données de santé ;
- documenter par écrit toute instruction concernant le/les traitement(s) de Données à caractère personnel et Données de santé effectué(s) par Doctolib ;
- veiller, au préalable et pendant toute la durée du traitement, au respect par Doctolib des obligations prévues par le RGPD ;
- superviser les traitements effectués par Doctolib en qualité de Sous- traitant ;
- désigner un interlocuteur privilégié chargé de vous représenter et le cas échéant un délégué à la protection des données conformément aux dispositions du RGPD ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD.

4.2. Les obligations de Doctolib en tant que Sous-traitant

4.2.1. Doctolib s'engage à :

- traiter les Données à caractère personnel et Données de santé suivant les finalités et le cadre défini au sein du présent Accord, et se conformer aux normes techniques et aux bonnes pratiques applicables en matière de Données à caractère personnel et Données de santé ;
- n'agir que sur votre seule instruction préalable. En cas d'impossibilité ou de difficulté dans la réalisation de certaines instructions, Doctolib vous en informera dans les meilleurs délais. Doctolib peut formuler une demande écrite de dérogation aux instructions. Doctolib devra recueillir votre autorisation écrite, préalable et spécifique pour pouvoir procéder à cette dérogation ;
- ne pas faire de copie des Données à caractère personnel et Données de santé sans votre autorisation ou instruction, ne pas les communiquer à des tiers et à ne pas les utiliser à des fins autres que celles spécifiées au Contrat ;
- ne pas exploiter ou traiter pour son propre compte et/ou pour le compte de tiers, à quelque fin que ce soit et de quelque manière que ce soit, les Données à caractère personnel et Données de santé que vous lui confiez, sauf autorisation de votre part. Est notamment interdite, toute utilisation de ces Données de santé à des fins marketings, publicitaires, commerciales ou statistiques ;
- mettre tous les moyens en sa possession au regard des stipulations contractuelles et des règles de l'art pour assurer la sécurité et la confidentialité des Données à caractère personnel et Données de santé qui lui sont confiées et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés et plus généralement, mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les Données à caractère personnel et Données de santé contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite ;
- vous notifier dans les meilleurs délais de toute survenance de faille de sécurité impactant directement ou indirectement les Données à caractère personnel, Données de santé ou traitements le concernant ;
- procéder à des sauvegardes régulières des Données à caractère personnel et Données de santé ;
- procéder régulièrement à des tests d'intrusion (ou Pentest) ;
- maintenir les matériels nécessaires au bon fonctionnement des Services ;
- s'assurer de la confidentialité des Données à caractère personnel et Données de santé traitées ;
- prendre en compte toute mise à jour, correction, suppression ou autres modifications que vous lui communiquez concernant les Données à caractère personnel et Données de santé ;
- respecter la période de conservation des Données à caractère personnel et Données de santé applicable aux finalités pour lesquelles elles ont été collectées ou fournies, selon les instructions du Responsable de traitement, et les supprimer/anonymiser dès lors que ces finalités n'existent plus, sous réserve des obligations légales ;
- désigner un délégué à la protection des Données.

4.2.2. Par ailleurs, Doctolib s'engage à veiller à ce que les personnes autorisées à traiter les Données à caractère personnel et Données de santé en vertu du présent Accord :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- reçoivent la formation nécessaire en matière de protection des Données à caractère personnel et des Données de santé ;
- considérer les principes de protection des données, y compris des données à caractère personnel et de santé, comme un standard dans le développement et le déploiement des outils, produits, applications ou services.

Doctolib vous aide, en prenant en compte la nature des traitements de données et les informations à sa disposition, dans la réalisation d'analyses d'impact relative à la protection des Données à caractère personnel et Données de santé ainsi que pour la réalisation de la consultation préalable de l'autorité de contrôle.

Doctolib met à votre disposition toutes les informations nécessaires concernant les traitements des Données à caractère personnel et Données de santé afin de vous assister dans l'accomplissement de vos obligations légales et réglementaires en tant que Responsable de traitement conformément aux dispositions du RGPD.

En l'absence d'instruction particulière de votre part sur la nature des Données à caractère personnel et Données de santé à traiter, les finalités, la base légale ainsi que la durée de conservation, vous reconnaissez et acceptez que celles-ci seront traitées selon les modalités mentionnées dans les Conditions spécifiques et conformément aux recommandations de la CNIL. En tant que Responsable de traitement, vous pouvez demander à Doctolib lors de l'exécution du Contrat à ce que ces modalités soient modifiées**.**

4.3 Réutilisation des données

(i) Réutilisation de données sans données de santé des Patients

Vous autorisez Doctolib à réutiliser, les Données à caractère personnel suivantes initialement traitées en tant que Sous-traitant dans le cadre des traitements décrits dans les Conditions spécifiques : vos données professionnelles (notamment motifs de consultation disponibles, particularités du lieu de consultation) ; les données d'usage et de connexion liées à votre usage des Services de Doctolib ; les données de rendez-vous sans la possibilité de pouvoir identifier les Patients (par exemple : date/heure et lieu du rendez-vous, statut du rendez-vous).

La finalité de cette réutilisation est d'améliorer les Services ; de produire des statistiques susceptibles d'être communiquées au public et à des tiers ; et d'anonymiser les Données à caractère personnel listées. Vous reconnaissez que ces finalités sont compatibles avec les finalités des traitements mentionnées dans les Conditions spécifiques de cet Accord.

Doctolib s'engage à permettre aux Personnes concernées d'exercer leur droit d'opposition. Si vous ne souhaitez pas autoriser cette réutilisation, vous pouvez modifier les réglages administrateurs dans votre centre de confidentialité.

(ii) Réutilisation de données incluant des données de santé des Patients

Sous réserve de votre autorisation spécifique, Doctolib peut réutiliser les catégories de données suivantes : vos données professionnelles ; les données de support et de retours d'expérience ; les données d'usage et de connexion liées à votre utilisation des Services (notamment les logs) ; vos enregistrements vocaux, notamment la dictée vocale ; les Données à caractère personnel des Patients listées dans les Conditions spécifiques, incluant notamment les Données de santé, les données de Messagerie, ainsi que les données issues d'appareils et d'applications tierces. Aucune donnée directement identifiante ne sera réutilisée.

La finalité de cette réutilisation est de réaliser des recherches et des études ; améliorer et développer les Services ; anonymiser les Données à caractère personnel listées. Vous reconnaissez que ces finalités sont compatibles avec les finalités des traitements mentionnées dans les Conditions spécifiques de cet Accord.

Aucune autorisation n'est présumée par défaut. Vous êtes libre d'accepter ou de refuser, et de modifier votre choix à tout moment via les réglages administrateurs dans votre centre de confidentialité. Doctolib s'engage à permettre aux Personnes concernées d'exercer leur droit au retrait du consentement.

Les Données de santé des Patients ne seront traitées qu'après la collecte du consentement des Patients concernés ou l'obtention des autorisations administratives requises. Les Patients conservent la décision finale

sur l'usage de leurs Données de santé : seuls ceux ayant accepté, via leur compte Doctolib, de participer à la recherche et au développement de produits innovants seront concernés.

5. VIOLATION DE DONNEES A CARACTERE PERSONNEL

Doctolib vous notifie toute violation de Données à caractère personnel et/ou Données de santé dans les meilleurs délais après en avoir pris connaissance, par message électronique ou tout autre moyen de communication mis à sa disposition par vous.

Cette notification est accompagnée, sur demande de votre part, de toute documentation utile afin de vous permettre, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et le cas échéant aux Personnes concernées.

Le référent à contacter pour le traitement des incidents ayant un impact sur les Données de santé hébergées est contact.dataprivacy@doctolib.fr.

6. TENUE DU REGISTRE DES ACTIVITÉS DE TRAITEMENT

Doctolib déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour votre compte conformément aux dispositions du RGPD.

7. INFORMATION DES PERSONNES CONCERNÉES

Il vous appartient d'informer les Personnes concernées (i) des traitements mis en œuvre dans le cadre des Services et de recueillir leur(s) consentement(s) dès lors que cela s'avère nécessaire en vertu de la loi applicable; (ii) des bases légales des traitements mis en oeuvre, des finalités des traitements ainsi que de la liste des sous-traitants susceptibles de traiter leurs Données à caractère personnel.

Afin de vous assister dans cette information, Doctolib publie sur le Portail Patient une Politique de protection des Données à caractère personnel accessible ici.

8. GESTION DES DEMANDES DE DROITS

Il vous appartient de donner suite aux demandes de droit des Personnes concernées sur leurs Données à caractère personnel.

Dans la mesure du possible, Doctolib, en sa qualité de Sous-traitant et sur votre demande, pourra vous assister à vous acquitter de votre 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), droit d'organiser le sort des Données à caractère personnel notamment après la mort.

Si une Personne concernée contacte directement Doctolib pour exercer l'un de ses droits relatifs à ses Données à caractère personnel traitées par Doctolib en qualité de Sous-traitant, Doctolib s'engage à renvoyer la Personne concernée vers vous afin que vous puissiez donner suite à sa demande.

Si vous en faites la demande, Doctolib pourra vous assister dans les suites à donner aux demandes mais ne pourra répondre directement aux demandes desdites Personnes concernées.

9. SECURITE ET CONFIDENTIALITE

9.1. Pour ce qui concerne les Services, Doctolib met en œuvre les mesures techniques et organisationnelles appropriées liées à la sécurité conformément aux dispositions prévues par la Loi Informatique et Libertés et le RGPD, et visant à garantir un niveau de sécurité approprié face aux risques présentés par le Traitement de vos Données à caractère personnel, comme indiqué dans les mesures techniques et organisationnelles applicables, en fonction des Services auxquels vous avez souscrit ou que vous utilisez. Pour évaluer le niveau de sécurité approprié, Doctolib tiendra compte des risques pouvant résulter d'une destruction accidentelle ou illicite, d'une corruption, d'une perte, d'une modification, d'une divulgation non autorisée ou de l'accès à des Données à caractère personnel susceptibles d'être transmises, stockées ou autrement traitées, conformément aux dispositions de l'article 32 du RGPD.

Ainsi, tous les employés disposent d'un badge avec leur photographie qui leur permet d'accéder aux locaux selon leur accréditation au sein de l'entreprise. L'accréditation est définie, soit en fonction du rôle de l'employé, soit en fonction de la demande de son responsable, qui doit être validée par le service compétent. Le port d'un badge est obligatoire pour chaque employé. En cas d'oubli, l'employé doit présenter une carte d'identité à la sécurité. Celle-ci vérifie son identité et, si la vérification est concluante, lui remet un badge temporaire qui doit être restitué le soir même. Cette mesure assure donc la confidentialité des données personnelles que vous nous confiez.

Les obligations visées ci-dessus ne vous déchargent en aucun cas de mettre en place l'ensemble des moyens de sécurité nécessaires à la confidentialité des Documents et des Données Abonné, Données base patient, Données Utilisateurs, Données à caractère personnel et Données de santé présentes sur la Plateforme Doctolib.

Il est convenu entre les Parties que le Contrat dont fait partie le présent Accord pourra être mis à disposition de la CNIL ou toute autorité compétente en cas de contrôle.

9.2. Personnes autorisées : Doctolib affecte à l'exécution des Services des équipes suffisantes et qualifiées disposant des compétences techniques et/ou fonctionnelles nécessaires à la fourniture des Services. Les personnes autorisées à traiter des Données Personnelles et/ou des Données de Santé pour votre compte sont formées à la réglementation relative à la protection des Données Personnelles.

9.3. Secret Professionnel : Doctolib reconnaît et accepte que les Données à caractère personnel et Données de santé traitées par vous lors de l'utilisation des Services sont strictement couvertes par le secret professionnel (article 226-13 du Code pénal).

Le Responsable du traitement informe Doctolib que les personnes impliquées dans les activités professionnelles d'un détenteur de secrets professionnels qui divulguent illégalement le secret d'un tiers, dont elles ont eu connaissance au cours de l'exercice ou à l'occasion de leur activité, sont passibles de poursuites en vertu de l'article 226-13 du Code Pénal.

Doctolib s'assure que tous les employés et autres personnes travaillant pour Doctolib (par exemple, les Sous-traitants) impliqués dans le Traitement de données soumises au secret professionnel du Responsable du traitement sont obligés par écrit de ne pas divulguer sans autorisation les secrets professionnels dont ils ont eu connaissance au cours de l'exercice ou à l'occasion de leur activité et qu'ils ont été informés de la responsabilité pénale potentielle.

9.4. Détention des données : sauf accord sur la protection des données exprès contraire, vous demeurez seul détenteur des Données Abonné/Utilisateur publiées sur le Portail Patient ainsi que sur la Fiche Profil Utilisateur et la Plateforme Doctolib. Doctolib ne pourra revendiquer aucun droit sur les données que vous publiez. Les statistiques anonymisées d'utilisation du Portail Patient sont la propriété de Doctolib.

10. SOUS-TRAITANCE ULTÉRIEURE

Vous concédez à Doctolib une autorisation écrite générale lui permettant de faire appel aux Sous-traitants ultérieurs énumérés dans la "Liste des Sous-traitants" à la fin de l'Accord, quand cela est raisonnablement nécessaire pour fournir les Services. Conformément à cette autorisation générale, Doctolib s'engage à vous informer, par le biais d'un préavis écrit de trente (30) jours, de tout changement envisagé concernant l'ajout ou le remplacement de Sous-traitants ultérieurs, vous offrant ainsi la possibilité de soulever toute objection que vous pourriez avoir à l'égard de ces changements. Si vous avez des raisons légitimes et raisonnables de vous s'opposer à la nomination d'un nouveau Sous-traitant ultérieur, vous devez immédiatement motiver votre réclamation à Doctolib en adressant un avis écrit à Doctolib à contact.dataprivacy@doctolib.com, dans les trente (30) jours ouvrables suivant l'avis émis par Doctolib, à défaut de quoi vous serez réputé avoir approuvé et accepté cette nomination.

Après discussions et en l'absence d'accord entre vous et Doctolib, vous pourrez, dans les trente (30) jours suivant la notification, résilier la partie du Contrat affectée par la mise à jour en question.

Concernant chaque Sous-traitant ultérieur, Doctolib : (i) fera preuve d'une diligence raisonnable sur le plan commercial dans l'évaluation, la nomination et la surveillance des activités de traitement des Sous-traitants ultérieurs; (ii) inclura dans le contrat entre Doctolib et chaque Sous-traitant ultérieur des clauses offrant un niveau de protection équivalent pour vos Données à caractère personnel et Données de santé, des Abonnés/Utilisateurs ainsi que celles des Patients et de leurs Proches, telles que celles prévues dans le présent Accord.

Si les Sous-traitants ultérieurs ne remplissent pas leurs obligations en matière de protection des Données à caractère personnel, Doctolib demeure responsable devant vous de l'exécution par les Sous-traitants ultérieurs de leurs obligations conformément aux termes du Contrat.

11. CERTIFICATION HDS

11.1. Amazon Web Services EMEA (AWS), dont le siège social est situé 38 avenue John F. Kennedy, L - 1885 Luxembourg, en tant que prestataire d'hébergement certifié HDS (Hébergeur de Données de Santé), agit en qualité de sous-traitant de Doctolib concernant l'hébergement de données de santé à caractère personnel collectées dans le cadre d'activités de prévention, de diagnostic, de traitement ou de suivi social et médico-social conformément à l'article L. 1111-8 du Code de la santé publique. Les activités sur lesquelles AWS est certifié sont l'Activité 1 (mise à disposition et maintien en condition opérationnelle des sites physiques hébergeant l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé), l'Activité 2 (mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé), l'Activité 3 (mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé), l'Activité 4 (mise à disposition et maintien en condition opérationnelle de la plateforme d'hébergement des applications du système d'information), l'Activité 5 (administration et exploitation du système d'information contenant les données de santé) et l'Activité 6 (sauvegarde des données de santé). AWS ne détient pas de qualification SecNumCloud 3.2.

Les données à caractère personnel traitées par AWS sont stockées au sein de l'Espace économique européen (EEE), sans aucun accès depuis l'extérieur de l'EEE dans le cadre du service. La société mère ultime d'AWS est établie aux États-Unis. Dans des cas spécifiques, AWS peut donc être tenu de se conformer à la loi ou à une ordonnance valide et contraignante d'un organisme gouvernemental (USA Patriot Act, FISA Section 702, Cloud Act, EO 12333), auquel cas les données à caractère personnel peuvent faire l'objet d'un accès depuis l'extérieur de l'EEE, notamment depuis les États-Unis, comme décrit ici. AWS Inc. est certifié au EU-U.S. Data Privacy Framework (DPF), qui a été reconnu en juillet 2023 par la Commission européenne comme offrant un niveau adéquat de protection des données à caractère personnel.

Dans le cadre de la prestation d'hébergement, aucun risque résiduel de transfert hors EEE n'est identifié

11.2. Conformément au Code de la santé publique et en tant qu'Hébergeur de Données de Santé certifié, AWS :

(i) ne traite les Données de santé que sur instructions documentées de Doctolib et met en place des mesures de sécurité pour encadrer l'accès à ces Données de santé ;

(ii) met à disposition de Doctolib des fonctionnalités lui permettant (a) d'assurer votre droit à la portabilité et (b) de couvrir toute défaillance éventuelle de la part d'AWS et (c) d'obtenir en fin de contrat la restitution et/ou suppression des Données de santé hébergées par AWS ;

(iii) notifie Doctolib dans les meilleurs délais en cas d'incident de sécurité et met en œuvre toutes les mesures raisonnables pour atténuer les dommages résultant d'un tel incident et permet à Doctolib de renseigner un référent contractuel à contacter pour traiter les éventuels incidents ayant un impact sur les Données à caractère personnel hébergées ;

(iv) s'engage à ce que que ses éventuels Sous-traitants assurent un niveau de protection équivalent à celui que garantit AWS à l'égard de Doctolib ;

(v) autorise Doctolib à conduire des audits afin de s'assurer du respect des obligations qui lui incombent au titre de son contrat conclu avec Doctolib ; les mesures techniques et organisationnelles de sécurité peuvent faire l'objet d'audits documentaires sur demande de Doctolib tandis que la conformité au standard ISO 27001 (incluant la sécurité des data centers) peut être vérifiée par Doctolib sur communication du rapport d'audit annuel effectué par un tiers indépendant expert en sécurité ;

(vi) met à disposition de Doctolib via ce lien les indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci ;

(vii) se conforme à toutes les lois, règles, réglementations et ordonnances applicables à son activité d'Hébergeur de Données de santé.

11.3. Doctolib est certifié Hébergeur de Données de Santé (HDS) depuis le 14 octobre 2021. Le certificat a été renouvelé le 4 mars 2026, sur sa version 2.0. Cette certification englobe l'ensemble des activités réglementées (activités 1 à 6) telles que définies à l'article R1111-9 du Code de la santé publique. Les informations détaillées concernant la notification, notamment sa date de délivrance, son renouvellement et le périmètre des activités certifiées sont disponibles sur le site officiel de l'Agence du Numérique en Santé (ANS).

11.4. Doctolib s'engage à ne pas utiliser les Données de santé à d'autres fins que l'exécution de l'activité d'hébergement de Données de santé, sauf instruction documentée contraire de votre part.

11.5 Doctolib vous notifie toute violation de Données de santé dans les conditions de l'article 5 du présent Accord.

11.6. Doctolib met en œuvre les mesures techniques et organisationnelles appropriées liées à la sécurité et visant à garantir un niveau de sécurité approprié face aux risques présentés par l'hébergement de vos Données à caractère personnel, comme indiqué dans les mesures techniques et organisationnelles applicables. A ce titre, les Données de santé ne transitent que par des réseaux de communication sécurisés.

En cas d'évolution technique introduite par Doctolib dans ces mesures techniques et organisationnelles, Doctolib s'engage à conserver un niveau de sécurité équivalent à celui assuré par le présent Accord, à moins que l'évolution technique en question soit imposée par une obligation légale ou réglementaire.

11.7. A la fin du Contrat ou si vous en faîtes la demande, en cas de retrait de la certification HDS de Doctolib, vous pourrez récupérer les Données de santé hébergées par Doctolib dans les conditions mentionnées par l'article 14 du présent Accord.

11.8. Vous vous engagez quant à vous à respecter la Politique générale de sécurité des systèmes d'information de santé.

11.9. A votre demande, et sous réserve que Doctolib et vous aient mis en place un accord de confidentialité, Doctolib vous fournira une copie des Contrôles du Système et de l'Organisation de Doctolib, du rapport de type ou de tout autre rapport ou certification substantiellement équivalents, tel que raisonnablement déterminé par Doctolib. Doctolib mettra cette documentation à votre disposition par courrier électronique et cette documentation sera traitée comme une Information Confidentielle de Doctolib, conformément à l'accord de confidentialité. En outre, Doctolib vous permet de consulter les traces d'accès aux données de santé à caractère personnel par le personnel sous son contrôle.

11.10. Doctolib s'engage à publier et à mettre à jour régulièrement une cartographie complète des transferts de Données de Santé à Caractère Personnel vers tout pays situé en dehors de l'Espace Économique Européen, y compris tout accès à distance potentiel à ces données. Cette cartographie sera mise à la disposition du public et des autorités compétentes dans un format accessible, permettant d'identifier clairement la destination, la finalité et les garanties juridiques de chaque transfert.

12. AUDIT

12.1. Afin de mesurer la sécurité des Services, vous pourrez faire réaliser à vos frais des audits de sécurité, dans le respect des conditions prévues au présent article et dans la limite d'un (1) audit par an et de cinq (5) jours ouvrés maximum, le temps passé par le personnel de Doctolib vous étant facturé.

12.2. L'audit se limitera à la vérification des processus, de l'organisation et des outils directement et exclusivement liés à la mise en œuvre des dispositions du RGPD pour les Services concernés.

L'audit ne doit en aucun cas avoir pour but de surveiller ou d'exiger l'accès (i) à toute Donnée à caractère personnel ou Donnée de santé non spécifique, qu'elle soit confidentielle ou non, ou à toute information dont la divulgation pourrait, à la discrétion de Doctolib, nuire à la sécurité des Services ou d'un autre de ses Utilisateurs ; (ii) aux données financières de Doctolib ; ou (iii) aux Données à caractère personnel relatives aux employés de Doctolib ou de ses Sous-traitants.

Il est convenu que toutes les activités entreprises dans le cadre d'un audit ne doivent, ni concurremment ni par ailleurs : (i) être de nature à entraver, modifier ou affecter de quelque manière que ce soit le fonctionnement des Services, systèmes, réseaux, logiciels et/ou matériels informatiques autres que ceux alloués à votre usage exclusif ; (ii) endommager l'infrastructure hébergeant les Services ; (iii) endommager, supprimer, modifier tout type de données ; (iv) permettre un accès non autorisé ou la maintenance des données précitées.

Aucun test d'intrusion ou de pénétration visant la Plateforme Doctolib n'est autorisé pour quelque motif que ce soit et est exclu des audits sans l'accord écrit et préalable de Doctolib.

Tous les documents et informations nécessaires à la réalisation de l'audit seront mis à la disposition des auditeurs par Doctolib exclusivement dans les locaux de celui-ci, sans qu'il n'y ait de possibilité de retrait ou de copie, à quelque fin que ce soit. Cette interdiction s'appliquera également aux documents et informations mis à disposition par les Sous-traitants de Doctolib. Si vous en faîtes la demande, Doctolib communiquera à celui-ci les rapports d'audit de certification délivrés par l'organisme de certification destinés à une telle communication.

12.3. Vous devrez faire parvenir à Doctolib au minimum trente (30) jours avant la réalisation de l'audit une convention d'audit détaillant son périmètre exact, les dates et horaires prévus, les conditions y afférent. L'auditeur devra également préciser, les éventuels comptes et profils utilisés pour les tests (adresse IP sources, user agent etc), la méthodologie employée, ainsi que les acteurs qui seront audités.

Le contenu de la convention d'audit doit être accepté préalablement par Doctolib avant tout début d'audit.

12.4. Les informations obtenues au cours de l'audit sont des informations confidentielles que vous devrez traiter comme telles. Ces informations pourront uniquement être communiquées aux personnes soumises à des exigences fortes en matière de confidentialité et ayant un intérêt direct et majeur à les connaître et ne devront en aucune manière être divulguées au public ou en interne.

Si vous souhaitez faire appel à un auditeur externe, vous devez obtenir l'accord préalable écrit de Doctolib, étant entendu que Doctolib ne pourra refuser ledit auditeur qu'en faisant valoir des arguments objectifs et fondés.

L'auditeur externe ne pourra en aucun cas être un concurrent de Doctolib et devra s'engager par écrit au respect des conditions fixées au présent article.

Vous engagez à communiquer gratuitement le rapport d'audit à Doctolib qui pourra présenter ses observations.

Doctolib disposera d'un délai raisonnable à compter de la réception du rapport pour corriger les manquements et/ou non-conformités constatés.

13. RÉCUPÉRATION DES DONNÉES DE BASE PATIENT

Vous pourrez récupérer les Données de base patient (excepté pour le Service de Messagerie où les Conditions spécifiques prévalent) ainsi que l'historique de leurs rendez-vous à la fin du Contrat, sauf dans le cas où vous auriez collecté ces données de façon illicite en tant qu'Utilisateur et/ou Abonné. Ces données seront mises à votre disposition dans un format garantissant leur interopérabilité. La demande d'export doit être faite par email à l'adresse suivante: contact@doctolib.com.

Doctolib s'engage à tenir à votre disposition, pendant toute la durée du Contrat et pendant toute la durée du processus de récupération des données, une copie de celles-ci. En cas de suspension de vos accès aux Services Doctolib, quelle qu'en soit la cause, Doctolib vous met en mesure de récupérer, par tout moyen et sur tout support, la dernière copie de vos Données de base patient ainsi que de votre historique de rendez-vous (sauf dans le cas où vous auriez collecté ces données de façon illicite).

A la fin du Contrat et sur demande formelle de votre part, Doctolib s'engage également à détruire les Données de santé sans en garder de copie, sous réserve d'obligations de conservation légales auxquelles Doctolib serait soumise. La preuve de la destruction des Données peut vous être communiquée sur demande.

14. TRANSFERTS DE DONNÉES

Les Données à caractère personnel peuvent faire l'objet, pour les finalités listées dans le présent Accord, d'un transfert à destination des entités du Groupe Doctolib, leurs Sous-traitants ou prestataires établis dans des pays bénéficiant d'un niveau de protection adéquat ou offrant des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes, et ce conformément à la législation applicable.

Doctolib vous informe que les Données à caractère personnel peuvent aussi être transférées par Doctolib vers des pays tiers à des Sous-traitants ultérieurs, uniquement lorsqu'un tel transfert est requis pour l'exécution des Services commandés. La "Liste des Sous-traitants ultérieurs" est disponible à la fin de l'Accord.

Si le transfert a lieu vers un pays tiers dans lequel la législation n'a pas été reconnue comme offrant un niveau de protection adéquat des Données à caractère personnel, Doctolib veille à ce que les mesures adéquates soient mises en place conformément à la Loi Informatique et Libertés et au RGPD, et notamment, lorsque nécessaire à

ce que des Clauses Contractuelles Types ou des clauses ad hoc équivalentes soient intégrées dans le contrat conclu entre Doctolib et le Sous-traitant ultérieur.

En sa qualité de Sous-traitant, Doctolib s'engage à héberger ou faire héberger les Données à caractère personnel sur le territoire de l'Union Européenne et, le cas échéant, à reporter, sur le prestataire hébergeant les Données à caractère personnel, l'ensemble des obligations stipulées au sein du présent Accord.

Par ailleurs, à la demande d'autorités administratives et judiciaires habilitées, Doctolib est susceptible de communiquer des Données à caractère personnel qu'elle traite pour votre compte afin de respecter ses obligations légales. Dans ce cas, et sauf disposition légale contraire, Doctolib s'engage à vous informer de cette communication.

15. CONTACT

En cas de questions sur le Traitement des Données à caractère personnel et Données de santé effectué par Doctolib conformément aux stipulations contractuelles et afin de communiquer à Doctolib des instructions spécifiques concernant le traitement des données à caractère personnel, vous pouvez contacter le délégué à la protection des données de Doctolib à l'adresse mentionnée ci-dessous.

Doctolib SAS (France) est l'établissement principal du Groupe Doctolib au sens de l'article 4.16 du RGPD. L'autorité cheffe de file pour les traitements transfrontaliers au sens de l'article 56 du RGPD pour le Groupe Doctolib est la CNIL (https://www.cnil.fr). Le délégué à la protection des données de Doctolib SAS peut être contacté à l'adresse suivante : DOCTOLIB – DPO, 54 quai Charles Pasqua, 92300 Levallois-Perret ou contact.dataprivacy@doctolib.com.

16. LOI APPLICABLE

L'Accord est régi et interprété conformément à la législation nationale qui vous est applicable.

17. INTÉGRALITÉ DE L'ACCORD

Le présent Accord constitue l'intégralité de l'accord entre les Parties en ce qui concerne son objet et remplace tous les accords antérieurs ou contemporains entre les Parties ayant le même objet, y compris toute version antérieure d'accord sur la protection des Données à caractère personnel qui aurait été signée entre vous et Doctolib.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “PARAMÉTRAGE DES COMPTES ABONNÉS ET UTILISATEURS”

FINALITÉS DU TRAITEMENT:

- Gestion des comptes : paramétrer le Compte Utilisateur et les habilitations des Utilisateurs ;
- Support technique et assistance : assurer le support technique, la maintenance et le traitement des demandes des Utilisateurs, le conseil, le stockage, l’hébergement et les autres services fournis aux Utilisateurs ;
- Support Données à caractère personnel : assistance dans la gestion des violations de Données à caractère personnel et Données de santé, assistance dans la construction de PIA, accompagnement pour répondre aux demandes d’exercice de droits des Personnes concernées ;
- Adressage de Patients vers un Acteur de santé ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.
Afin d’aider les Responsables de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l’intérêt légitime comme base légale. Vous êtes libre de mentionner à Doctolib une autre base légale.

PERSONNES CONCERNÉES:

- Abonné et Utilisateur.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Dans un souci de minimisation des Données à caractère personnel traitées, vous devez veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de vos besoins de traitement de gestion médicale et administrative de votre patientèle, et prendre également en compte toute Donnée de santé liée à la prise de rendez-vous.

Sont en principe considérées comme pertinentes, pour les finalités mentionnées ci-dessus, les données suivantes :

- L’identité et coordonnées de l’Acteur de santé : genre, nom, prénom, numéro de téléphone et email, adresse postale, photographie, signature, carte d’identité ou passeport, carte CPx, numéro ADELI ou RPPS, numéro FINESS de l'établissement d'exercice, identifiant compte Stripe ou Adyen ;
- Données professionnelles : photographie, spécialité, détail de la prise en charge, parcours de l’Acteur de santé, motifs de consultation disponibles, heure d’ouverture et de fermeture, particularités liées au lieu de consultation ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs) ;
- Données fournies au Chatbot mis à disposition par Doctolib.

DUREE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.
A défaut d’une telle instruction de votre part, Doctolib appliquera les durées de conservation telles que recommandées par la CNIL ou la législation applicable.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “GESTION DES RENDEZ-VOUS ET DE L’AGENDA”

FINALITÉS DU TRAITEMENT:

- Accompagnement dans la gestion du téléchargement et extraction du contenu des Agendas, rendez-vous, et si nécessaire, de la Base de Données Patients de l’Acteur de santé sur la Plateforme Doctolib ;
- Respecter les règles relatives à l’identito vigilance ;
- Vous permettre de gérer votre Agenda ainsi que les données liées ;
- Permettre la prise de rendez-vous successifs pour les Patients réguliers (exemple, même motif de visite, même localisation, même format de rendez-vous - en personne ou par visio) ;
- Faciliter la prise de rendez-vous par les Patients et leurs Proches par le Profil “Google Business” de l’Acteur de santé ;
- Permettre la prise de rendez-vous en ligne par les Patients pour eux-mêmes et leurs Proches ;
- Permettre aux Patients d'afficher, de façon complète, dans leur compte leur historique des rendez-vous ainsi que l'historique de leurs échanges avec vous, pour eux-mêmes et leurs Proches ;
- Permettre la prise de rendez-vous en ligne dans le cadre du service public d’accès aux soins ;
- Permettre la gestion d’un rendez-vous en présentiel ou en vidéo consultation ;
- Permettre la communication entre l’Acteur de santé et le Patient et fournir des informations aux Patients et à leurs Proches relatives au profil Utilisateur et à leur parcours de soin ;
- Permettre à l’Acteur de santé d’envoyer et recevoir des documents de Patients ou de Proches ;
- Envoyer des SMS, emails et notifications push (i) de confirmation, d’annulation ou de rappel de rendez-vous ; (ii) d’information sur l’envoi de Documents ; (iii) d’information de rappels et (iv) d’informations liées à la prise en charge du Patient ou liées à l'organisation de son activité ;
- Permettre à l'Acteur de santé d'envoyer à ses Patients des communications groupées à caractère informatif ou préventif, notamment par l'utilisation de filtres spécifiques et/ou par le téléchargement par l'Acteur de santé de listes de destinataires ;
- Permettre la suppression de données erronées après signalement d’erreurs par le détenteur légitime des données et vérification par Doctolib ;
- Permettre le référencement des Données à caractère personnel et de santé des Patients avec l’identité INS que vous véhiculez ou le responsable de référencement sélectionné par vos soins et envoyée à Doctolib ;
- Permettre dans le cadre de la prise de rendez-vous en ligne, la bonne gestion de l’identité Patient dans les Services en permettant notamment d’éviter la création de Fiches Patients en doublons ;
- Permettre une limitation du nombre de rendez-vous pouvant être pris par Utilisateur, pour certaines spécialités, sur une période de 7 jours afin d’éviter les surréservations ;
- Reporting, debug statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.

Afin d’aider les Responsables de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l’intérêt légitime comme base légale. Vous êtes libre de mentionner à Doctolib une autre base légale.

PERSONNES CONCERNÉES:

- Patients et leurs Proches ;
- Confrères des Acteurs de santé ;
- Abonné et Utilisateur.

TYPES DE DONNEES A CARACTERE PERSONNEL:

Dans un souci de minimisation des Données à caractère personnel et Données de santé traitées, vous devez veiller à ne collecter et utiliser que les Données à caractère personnel et Données de santé pertinentes et nécessaires au regard de vos besoins de traitement de gestion médicale et administrative de votre patientèle.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- L’identité et coordonnées du Patient ou du Proche : genre, nom, prénom, date de naissance, lieu de naissance, adresse postale et digicode, email et numéro de téléphone ;

- La situation professionnelle du Patient ou du Proche : la profession ;
- Vos données professionnelles (incluant la spécialité, les motifs de consultation disponibles, les spécificités du lieu de consultation et les coordonnées) ;
- Santé : statut d'assuré, identité et coordonnées de l'Acteur de santé, identité et coordonnées de l'Acteur de Santé adressant, date/heure et lieu du rendez-vous, spécialité de l'Acteur de santé et motif de consultation, statut du rendez-vous, documents médicaux du Patient, champs remplis, l'identité INS (de la personne prise en charge) : à savoir le matricule INS (NIR ou NIA) et les traits d'identités INS (sexe, nom, les prénoms, date de naissance, lieu de naissance) ;
- Vos Données d'utilisation et de connexion (telles que les logs) liées à votre usage des Services Doctolib.

DESTINATAIRES :

- Les Acteurs de santé ;
- L'Assistant, dans le respect des règles de secret professionnel ;
- Les personnes habilitées au sein de Doctolib.

DUREE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

A défaut d'une telle instruction de votre part, cette dernière sera fixée à 5 ans pour l'historique de rendez-vous.

Vous êtes libre de communiquer à Doctolib une durée de conservation différente comprise entre 1 an et 20 ans.

Concernant les informations partagées (données professionnelles) avec Google, la durée de conservation est de 24 heures.

Au regard des finalités de gestion de l'établissement de santé et du cabinet médical ou paramédical, les données enregistrées dans la Plateforme Doctolib peuvent être conservées pendant une durée maximale de vingt ans à compter de la date de la dernière prise en charge du Patient.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “SERVICE DE TÉLÉCONSULTATION”

FINALITÉS DU TRAITEMENT:

- Mettre à la disposition de l’Acteur de santé un outil de Téléconsultation incluant la vidéotransmission ;
- Permettre la transmission de Documents aux Patients via le profil de l’Acteur de santé (ordonnance, compte rendu médical, note d’honoraire…) et la réception de ceux-ci pour le suivi Patient ;
- Permettre à l’Acteur de santé de prendre des notes pendant la Téléconsultation ;
- Permettre le paiement de la Téléconsultation ;
- Détecter la fraude ;
- Support et assistance techniques : assurer le support technique, la maintenance, l'administration et le traitement des demandes des Utilisateurs, des Abonnés et des Patients relatives à la Téléconsultation et au paiement en ligne ;
- Permettre la prise de captures d’écrans de la Téléconsultation pour le dossier médical du Patient par l’Acteur de santé ;
- Permettre la communication entre l’Acteur de santé et le Patient via un chat video ;
- Permettre la facturation et prise en charge financière des dépenses de santé ;
- Reporting, debug et statistiques ;
- Campagne de communication par email et/ou SMS à vos Patients pour les informer de l’ouverture du Service de Téléconsultation de leurs praticiens ;
- Amélioration des Services ;
- Production de statistiques ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.
Afin d’aider les Responsables de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l’intérêt légitime comme base légale pour la gestion des rendez-vous et des agendas. Vous êtes libre de mentionner à Doctolib une autre base légale.

PERSONNES CONCERNÉES:

- Utilisateur ;
- Les Patients et leurs Proches autorisés.

TYPES DE DONNEES A CARACTERE PERSONNEL:

Dans un souci de minimisation des Données à caractère personnel traitées, vous devez veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de vos besoins de traitement de gestion médicale et administrative de votre patientèle.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- L’identité et les coordonnées du Patient ou du Proche : Genre, nom, prénom, adresse e-mail, numéro d'identification du Patient, numéro d'identification de la transaction, code postal, date de création du compte Utilisateur ;
- Données de paiement : genre, nom, prénom, adresse e-mail, numéro d’identification du Patient, numéro de transaction, code postal, date de création du compte, coordonnées bancaires, date et heure de la transaction, montant facturé, mode de paiement utilisé ;
- Santé : Documents médicaux du Patient, notes complétées par l’Acteur de santé, capture d’écran effectuées par l’Acteur de santé pour le suivi médical du Patient, le NIR (à des fins de facturation et de remboursement des soins) ;
- Les données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DUREE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

Au regard des finalités de gestion de l’établissement ou du cabinet médical ou paramédical, les données enregistrées dans la Plateforme Doctolib peuvent être conservées pendant une durée maximale de vingt ans à compter de la date de la dernière prise en charge du Patient.

Les données de paiement sont conservées pendant 10 ans, conformément à l’article L. 123-22 du Code de Commerce.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “SERVICE DE MESSAGERIE PATIENTS”

FINALITÉ DU TRAITEMENT:

- Permettre à l'Abonné et/ou aux personnes autorisées à le faire au sein de l'organisation d'envoyer un message à un Patient ;
- Permettre à l'Utilisateur de décider d'accepter ou non les messages des Patients ou, dans certains cas, des non-Patients ;
- Permettre à un Patient d'envoyer un message à l’Utilisateur et à l'Utilisateur d'y répondre ;
- Permettre la gestion de la demande par l'Utilisateur;
- Permettre à l'Utilisateur d'envoyer des documents au Patient et de recevoir des documents du Patient ;
- Permettre à l'Utilisateur de communiquer au Patient des informations sur les soins qui lui sont prodigués.
- Reporting, debug statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base juridique avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Les Patients ;
- Utilisateurs.

TYPES DE DONNÉES À CARACTÈRE PERSONNELS:

Dans un souci de minimisation des Données à caractère personnel traitées, vous devez veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de vos besoins de Traitement de gestion médicale et administrative de votre patientèle, en prenant également en compte les Données de santé liées à la demande soumise par le biais du service.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données des Utilisateurs ;
- Identité et coordonnées du Patient : sexe, prénom, nom, date de naissance, adresse électronique ;
- Santé : médecin traitant et référent, prescriptions médicales, analyses cliniques, rapports, toutes informations contenues dans le champ d'informations complémentaires et que le Patient juge nécessaire et pertinent de partager avec l'Acteur de santé pour la gestion du Service demandé, contenu des Documents pouvant inclure des Données de santé, informations que l'Acteur de santé inclut dans le champ d'informations complémentaires pouvant inclure des Données de santé ;
- Les données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

Il vous est rappelé que vous êtes tenu de respecter le principe de proportionnalité, ou minimisation des données, et ainsi de ne demander que les informations strictement nécessaires à la prise en charge du Patient dans le cadre de ce Service.

Toute intégration de données non liées à la gestion des demandes de Patients ou qui n’est pas essentielle à la prise en charge doit être exclue.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “MISE À DISPOSITION D’UN LOGICIEL DE GESTION DE CABINET”

FINALITÉS:

- Mise à disposition d’un Service de logiciel de gestion de cabinet permettant notamment :
  - d’exercer votre activité de prévention, de diagnostic, de soin et de gestion de votre cabinet en vous permettant de créer et gérer des dossiers médicaux contenant notamment : les consultations, l’historique des rendez-vous, les antécédents, les éventuelles allergies, les vaccins, les Prescriptions et examens médicaux, des Documents, les rappels et alertes prévention du Patient et de ses Proches, les traitements et les bilans ;
  - de gérer le remboursement des frais relatifs à la prise en charge du Patient et de ses Proches : établissement et télétransmission des feuilles de soins, gestion des tiers payants et les règlements ;
  - de permettre le paiement de la consultation pour les Abonnés éligibles à ce Service ;
  - de gérer le suivi médical des Patients et de leurs Proches : édition d’ordonnances médicales et paramédicales, édition de certificats, gestion des résultats d’analyse des laboratoires, édition de demandes d’examens, envoi de courriers aux confrères etc ;
  - de qualifier l’identité INS en appelant le Téléservice INSi et de référencer les Données à caractère personnel et de santé avec l’identité INS qualifiée ;
  - suppression de données erronées après signalement d’erreurs par le détenteur légitime des données et vérification par Doctolib ;
- Support technique et assistance : assurer le support technique, la maintenance, l’administration et le traitement de vos demandes, le conseil, le stockage, l’hébergement du Service de logiciel de gestion de cabinet ;
- Mises à jour et amélioration du Service de logiciel de gestion de cabinet à votre demande ;
- Accompagnement dans la gestion des imports et des exports des Données base patient pour votre compte et sous votre responsabilité ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.

Afin d’aider les Responsables de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l’obligation légale comme base légale pour la tenue du dossier médical. Vous êtes libre de mentionner à Doctolib une autre base légale.

PERSONNES CONCERNÉES:

- Patients et Proches ;
- Utilisateurs et Abonnés.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Il est rappelé qu’il vous appartient de ne renseigner dans le Service de logiciel de gestion de cabinet mis à disposition par Doctolib que les Données de santé et Données à caractère personnel nécessaires au suivi du Patient et de ses Proches.
Toute intégration d’informations sans lien avec l’objet de la consultation du Patient et de ses Proches ou non indispensables au diagnostic et à la délivrance des soins doit être exclue.
Avant toute intégration de Données de santé ou Données à caractère personnel relatives au Patient et/ou à leurs Proches, il vous appartient d’obtenir l’accord préalable du Patient et de ses Proches, si nécessaire.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Les données d’identification et de contact : nom, prénom, date de naissance, lieu de naissance, adresse, numéro de téléphone ;
- Le numéro de sécurité sociale (de l’ouvrant droit) : uniquement pour l’édition des feuilles de soins et la télétransmission aux caisses d’assurance maladie ;
- L’identité INS (de la personne prise en charge) : à savoir le matricule INS (NIR ou NIA) et les traits d’identités de référence (sexe, nom, les prénoms, date de naissance, lieu de naissance) ;
- Selon les contextes, informations relatives à la situation familiale : situation matrimoniale, nombre d’enfants ;
- Selon les contextes, informations relatives à la vie professionnelle : profession, conditions de travail ;

- Données de santé : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du Patient et/ou de ses Proches et considéré comme pertinent par vous ;
- Informations relatives aux habitudes de vie : dans la stricte mesure où elles sont nécessaires au diagnostic et aux soins ;
- Données d'utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs) ;
- Données de paiement : genre, nom, prénom, adresse e-mail, numéro d'identification du Patient, numéro de transaction, code postal, date de création du compte, coordonnées bancaires, date et heure de la transaction, montant facturé, mode de paiement utilisé.

Doctolib, en tant que Sous-traitant, et vous en tant que Responsable de traitement, s'engagent à respecter les dispositions du référentiel INS mis à disposition par l'Agence française du numérique en santé.

DESTINATAIRES :

- Les Acteurs de santé concourant à la prévention et aux soins afin d'assurer la continuité des soins ;
- Les personnels des organismes d'assurance maladie et d'assurance maladie complémentaires ;
- Les personnes habilitées au sein de Doctolib ;

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

Au regard des finalités de gestion de l'établissement ou du cabinet médical ou paramédical, les données enregistrées dans la Plateforme Doctolib peuvent être conservées pendant une durée maximale de vingt ans à compter de la date de la dernière prise en charge du Patient.

Les données de paiement sont conservées pendant 10 ans, conformément à l'article L. 123-22 du Code du Commerce.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT " ASSISTANT DE CONSULTATION"

FINALITÉS:

- Mise à disposition d'un Service Assistant de consultation permettant notamment :
  - de transcrire l'enregistrement de la consultation entre un Acteur de santé et son Patient ;
  - d'en générer des suggestions de prise de notes ;
  - et, après validation de ces dernières par l'Acteur de santé, d'alimenter le dossier médical du Patient avec des éléments structurés issus des suggestions ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base juridique avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Patients et/ou Proches ;
- Accompagnants éventuels du Patient ;
- Acteurs de santé.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Afin de minimiser les Données à caractère personnel et les Données de santé traitées, vous devez vous assurer que vous ne collectez et traitez que les données nécessaires à la réalisation de ce traitement.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Voix et données contenues dans l'enregistrement audio ;
- Transcription de l'enregistrement audio ;
- Données du dossier médical du Patient (données déjà renseignées dans le dossier médical du Patient, complétées par la prise de notes par l'Assistant de consultation, après votre validation/modification) ;
- Données d'utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs) ;
- Enregistrements vocaux.

DESTINATAIRES:

- L'Acteur de santé;
- L'Assistant, dans le respect des règles de secret professionnel.

DUREE DE CONSERVATION:

Les suggestions de prise de notes et transcriptions sont conservées pendant 48h à la suite de la consultation, afin que vous puissiez valider les suggestions ou les modifier le cas échéant.

Une fois les informations issues des suggestions restituées dans le dossier médical du Patient, les données seront conservées conformément à la durée de conservation définie pour le Service de logiciel de gestion de cabinet.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “DICTÉE MÉDICALE”

FINALITÉS:

- Mise à disposition d’un Service Dictée médicale permettant notamment de :
  - transcrire le texte dicté par un Acteur de Santé dans certains champs du Service de logiciel de gestion de cabinet.
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base juridique avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Patients et/ou Proches ;
- Accompagnants éventuels du Patient ;
- Acteur de santé.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Afin de minimiser les Données à caractère personnel et les Données de santé traitées, vous devez vous assurer que vous ne collectez et traitez que les données nécessaires à la réalisation de ce traitement.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Voix et données contenues dans l’enregistrement audio ;
- Transcription de l’enregistrement audio ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs) ;
- Données du dossier médical du Patient (données transcrites par la Dictée médicale, après votre validation/modification le cas échéant).

DESTINATAIRES:

- L’acteur de santé ;
- Les Assistants, dans le respect des règles de secret professionnel.

DUREE DE CONSERVATION:

Les transcriptions sont conservées jusqu’à leur insertion dans un champ de texte.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT "GESTIONNAIRE DE TÂCHES INTELLIGENT"

FINALITÉS:

- Mise à disposition d'un Service de gestionnaire de tâches intelligent facilitant la communication et la gestion des tâches au sein de l'organisation de l'Abonné, notamment en :
  - créant des tâches pour le suivi des patients ;
  - la planification des rendez-vous ;
  - la gestion des tâches administratives ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base juridique avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Patients et/ou Proches,
- Acteurs de santé et/ou Assistants disposant d'un Compte.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Afin de minimiser les Données à caractère personnel et les Données de santé traitées, vous devez vous assurer que vous ne collectez et traitez que les données nécessaires à la réalisation de ce traitement.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Identité et données de contact de l'Acteur de santé et des Assistants ;
- Le statut professionnel de l'Acteur de santé et des Assistants ;
- Les données d'identification du Patient ou du Proche : genre, nom, prénom, date de naissance, lieu de naissance, adresse postale, digicode, adresse email et numéro de téléphone ;
- Le statut professionnel du Patient ou du Proche ;
- Données de santé : des informations sur le régime d'assurance maladie et l'organisme auquel le Patient et les bénéficiaires sont rattachés ; détails relatifs au médecin traitant, identité et contact de l'Acteur de santé référent, date, heure et lieu du rendez-vous, spécialité de l'Acteur de santé, motif du rendez-vous, champs complétés par l'Acteur de santé, statut du rendez-vous, Documents médicaux du Patient, l'identité INS de la personne : le numéro de sécurité sociale, les caractéristiques d'identifiant NIS (genre, noms de famille, prénom, lieu de naissance, date de naissance) ;
- Données d'utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DESTINATAIRES:

- L'Acteur de santé ;
- Les Assistants dans le respect des règles de secret professionnel.

DURÉE DE CONSERVATION:

Les tâches sont conservées jusqu'à leur clôture. Après leur clôture, les tâches sont conservées un an avant suppression.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “MISE À DISPOSITION DU LECTEUR DOCTOLIB”

FINALITÉS:

- Permettre l’envoi du Lecteur Doctolib à l’adresse indiquée par l’Abonné lors de l’Abonnement ;
- Vous permettre d’accéder aux services de la CNAM ;
- Permettre la création, la gestion et la signature des factures lors de visites médicales au domicile des Patients ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base juridique avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Les Patients et bénéficiaires inscrits sur la carte vitale;
- Les Utilisateurs et Abonnés du lecteur Doctolib.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Vos données de contact : nom, prénom, adresse postale, numéro de téléphone ;
- Les données d’identification du Patient et des bénéficiaires inscrits sur la carte vitale : nom, prénom, date de naissance, lieu de naissance, genre ;
- Le numéro de sécurité sociale : uniquement pour l’édition des feuilles de soins et la télétransmission aux caisses d’assurance maladie ;
- Des informations sur le régime d’assurance maladie et l’organisme auquel le Patient et les bénéficiaires sont rattachés ;
- Éventuellement des informations sur les droits à la complémentaire santé solidaire (CSS) ;
- Éventuellement des informations sur les droits à l’exonération du ticket modérateur ;
- Données de santé : historique médical, historique des soins, traitements prescrits et tout élément de nature à caractériser la santé du Patient et/ou de ses Proches ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DESTINATAIRES:

- Les Professionnels de santé et les professionnels concourant à la prévention et aux soins afin d’assurer la continuité des soins dans le respect des dispositions des articles L. 1110-4 et L.1110-12 du Code de la santé publique ;
- Les personnels des organismes d’assurance maladie et d’assurance maladie complémentaires ;
- Le transporteur chargé de la livraison du Lecteur Doctolib.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

Au regard des finalités de gestion de l’établissement ou du cabinet médical ou paramédical, les données enregistrées dans la Plateforme Doctolib peuvent être conservées pendant une durée maximale de vingt ans à compter de la date de la dernière prise en charge du Patient.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “GESTION DES DOCUMENTS ET FORMULAIRES”

FINALITÉS:

- Permettre la création et le formatage de Documents ;
- Permettre (i) l’envoi de Document par le Patient, par un Proche autorisé, ou par l’Acteur de santé et (ii) la réception de Document par le Patient, par un Proche autorisé, l’Acteur de santé et/ou tout autre destinataire choisi par l’Acteur de santé ;
- Vous permettre (i) de demander au Patient ou à un Proche autorisé, en amont et pour faciliter la préparation du rendez-vous, d'envoyer un ou plusieurs documents, ou de répondre à certaines questions concernant le Patient, (ii) l'édition de ces documents ou formulaires, (iii) la réception et le stockage de ces documents et formulaires ;
- Permettre la Signature Électronique Simple des Documents ;
- Reporting, debug et statistiques;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement. Afin d’aider les Responsables de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l’intérêt légitime comme base légale pour la gestion des rendez-vous et des agendas. Vous êtes libre de mentionner à Doctolib une autre base légale.

PERSONNES CONCERNÉES:

- Patients et/ou Proches ;
- Acteurs de santé ayant ou non un Compte Utilisateur Doctolib.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données d’identification ;
- Carte Vitale et/ou Numéro de Sécurité Sociale (NIR) à des fins de facturation et de remboursement des soins, informations relatives à la complémentaire santé ;
- Données de contact ;
- Données relatives aux habitudes de vie, e.g. exercice physique, régime et comportement alimentaire, etc. ;
- Antécédents médicaux, familiaux et allergies ;
- Données de consultation ;
- Données de prescription ;
- Données de biométrie et biologie ;
- Données relatives à l’équipe soignante ;
- Imagerie médicale ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

En ce qui concerne les Documents et informations demandés au Patient ou à un Proche autorisé en préparation d'un rendez-vous, il vous est rappelé que vous êtes tenu de respecter le principe de proportionnalité, ou minimisation des données, et ainsi de ne demander que les documents ou informations strictement nécessaires à la prise en charge du Patient.

DESTINATAIRES DES DONNÉES:

- Les Acteurs de santé ;
- Les Patients et Proches autorisés.

Lorsque l'Acteur de santé partage un Document ou une information dans le cadre de la préparation ou des suites d'un rendez-vous pris pour le Patient par un Proche, l'Acteur de santé s'assure sous sa propre responsabilité du respect du secret médical dans le cadre de ce partage. Ainsi, l'Acteur de santé s'assure (i) que le Proche est régulièrement autorisé, légalement ou par contrat, à représenter le Patient et accéder à ses Données de santé, et/ou (ii) d'obtenir le consentement du Patient au partage de ses Données de santé avec le Proche ayant pris un rendez-vous pour son compte.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

Sauf instruction particulière de votre part, les Documents conservés par l'Utilisateur dans la Plateforme Doctolib sont stockés selon les conditions attachées à chaque Service ou jusqu'à suppression par l'Utilisateur.

Par dérogation, et sous réserve de l'obtention par Doctolib du consentement exprès du Patient ou du Proche autorisé, vous autorisez expressément Doctolib en qualité de Responsable de traitement, à stocker dans la section "Mes Documents" ou dans la fiche rendez-vous les Documents ou formulaires envoyés par le Patient ou par vous, aux fins de permettre (i) au Patient de consulter les Documents et formulaires envoyés ou reçus sur son compte Doctolib à tout moment, (ii) au Patient de réutiliser ces Documents et informations dans le cadre de la préparation de futurs rendez-vous sur Doctolib. Les Documents seront conservés jusqu'à suppression par le Patient du Document ou suppression par le Patient de son Compte ou retrait par le Patient de son consentement au stockage des Documents dans la section "Mes Documents".

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “MISE À DISPOSITION D’UN SERVICE DE TRANSMISSION DE PRESCRIPTIONS”

FINALITÉS:

- Permettre la transmission sécurisée de Prescriptions pouvant inclure des Données à caractère personnel relatives aux Patients et des Données de santé par les Patients vers les Professionnels de Santé relevant du monopole des pharmaciens au sens du Code de la santé publique, sur la Plateforme Doctolib ;
- Permettre aux Utilisateurs du Service de Transmission de Prescriptions de renseigner et être renseignés sur le statut de délivrance des Prescriptions ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE DU TRAITEMENT:

Il vous appartient de déterminer cette base légale avant toute opération de traitement. A titre indicatif, l’intérêt légitime pourrait constituer la base légale. Vous êtes libre de mentionner à Doctolib une autre base légale**.**

PERSONNES CONCERNÉES:

- Patients consultant les Acteurs de santé utilisant le Service de Transmission de Prescriptions ;
- Acteurs de santé ayant ou non un Compte Utilisateur.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données d’identification ;
- Antécédents médicaux, familiaux et allergies ;
- Données de consultation ;
- Données de prescription ;
- Historique de délivrance des Prescriptions ;
- Données de biométrie et biologie ;
- Données relatives à l’équipe soignante ;
- Carte Vitale et/ou Numéro de Sécurité Sociale (NIR) à des fins de facturation et de remboursement des soins, informations relatives à la complémentaire santé ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DESTINATAIRES DES DONNÉES:

- Les Professionnels de Santé relevant du monopole des pharmaciens au sens du Code de la santé publique ayant un Compte Utilisateur.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib

En l’absence d’instruction contraire de la part de votre part pour une conservation particulière, les Prescriptions sont conservées par défaut 13 mois à compter de la date de leur transmission sur le Service de Transmission de Prescriptions**.**

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “SERVICE DE PRÉ-ADMISSION”

FINALITÉS:

- Permettre à l’Acteur de santé de gérer les dossiers de Pré-admission des Patients et des Proches ;
- Permettre la réalisation de la Pré-admission en ligne par le Patient ou l’utilisateur du système de Pré-admission (pour lui-même et ses Proches) ;
- Permettre à l’Acteur de santé de communiquer au Patient ou à l’utilisateur du système de Pré-admission et à ses Proches des informations relatives à leur venue dans l’établissement et la préparation de leur dossier de Pré-admission ;
- Envoyer des SMS, emails et notifications push (i) de confirmation, d’annulation ou de rappel de rendez-vous ; (ii) d’information sur l’envoi de Documents et de questionnaires de Pré-admission ; (iii) d’information et de rappels concernant les Documents et questionnaires de Pré-admission non complétés (iv) d’informations liées à la prise en charge du Patient et/ou des Proches ou liées à l'organisation de la consultation ou de l'hospitalisation ou à la réalisation de son dossier d’admission ;
- Permettre l’envoi par le Patient, ou l’utilisateur du système de Pré-admission à l’Acteur de santé des Documents et questionnaires jugés nécessaires à la préparation de sa Pré-admission médicale ou administrative ou de celle de ses Proches, et demandés par l’Acteur de santé ;
- Amélioration des Services ;
- Reporting, debug et statistiques ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Patients et leurs Proches ;
- Assistants.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données d’identification et de contact ;
- Antécédents médicaux, familiaux et allergies ;
- Données de consultation ;
- Données de prescription ;
- Historique de délivrance des prescriptions ;
- Données de biométrie et biologie ;
- Données relatives à l’équipe soignante ;
- Données contenue dans les documents transmis ;
- Données d’utilisation et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DESTINATAIRES DES DONNÉES:

- Les Acteurs de santé ;
- Les Assistants ;
- Les personnes autorisées au sein de Doctolib.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “ASSISTANT TÉLÉPHONIQUE VIRTUEL”

FINALITÉS:

Fourniture d’un assistant téléphonique virtuel qui permet notamment de :

- Conserver, transcrire et enregistrer des conditions téléphoniques entre Patients d’Acteurs de santé et autres appelants et l'assistant téléphonique virtuel ;
- Afficher des messages générés à partir des transcriptions dans le Service de Messagerie Patients, et générer des rendez-vous correspondants aux demandes ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LÉGALE:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

PERSONNES CONCERNÉES:

- Patients et leurs Proches ;
- Appelants.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Enregistrement audio de l'appelant ;
- Données contenues dans les enregistrements audio (nom, date de naissance, raison de l’appel, ordonnances, informations relatives à la famille, informations médicales, allergies, données biométriques et biologiques, et/ou autres Données à caractère personnel communiquées volontairement par l'appelant) ;
- Numéro de téléphone ;
- Transcription de l'enregistrement audio ;
- Données d’usage et de connexion liées à votre usage des Services Doctolib (telles que les logs).

DESTINATAIRES DES DONNÉES:

- Les Acteurs de santé ;
- Les Assistants.

DURÉE DE CONSERVATION:

Sauf dans le cas où vous instruisez Doctolib autrement par écrit, Doctolib conservera les enregistrements audio 60 jours après la conversation avec l’assistant téléphonique virtuel afin que l’Utilisateur puisse confirmer, ou si nécessaire, modifier la transcription.

Les messages résultant des transcriptions visibles dans le Service de Messagerie Patient seront conservés conformément aux durées de conservation définis pour ce Service.

A l’expiration de ces durées de conservation, les données seront supprimées.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “RÉSEAU DE L’ORGANISATION PRIVÉ”

(DOCTOLIB CONNECT ORGANISATIONS)

FINALITÉS:

Avec le Service Doctolib Connect Organisation, les employés/membres de l'organisation peuvent facilement se trouver et se contacter les uns les autres et partager des informations par le Réseau de l'Organisation. À travers l'Outil d'Administration Doctolib Connect Connect, vous pouvez configurer et personnaliser le Réseau d'Organisation, diffuser des messages, inviter des personnes à rejoindre le Réseau d'Organisation, et pré-créer des conversations pour les Utilisateurs. Doctolib peut également effectuer des rapports, du débogage et des statistiques pour votre Compte et à des fins d’amélioration des Services.

BASE LÉGALE:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.

PERSONNES CONCERNÉES:

- Patients et leurs Proches ;
- Acteurs de santé ou leurs Assistants disposant d’un Compte Utilisateur

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données d’identification, données professionnelles et de contact des Acteurs de santé faisant partie de l’organisation ;
- Antécédents médicaux, familiaux et allergies ;
- Données de consultation ;
- Données de prescription ;
- Historique de délivrance des Prescriptions ;
- Données de biométrie et biologie ;
- Imagerie médicale ;
- Photographie ;
- Flux de vidéos et d’appels vocaux ;
- Données d’utilisation et de connexion liées à votre usage du Service (telles que les logs).

DESTINATAIRES DES DONNÉES:

- Les Acteurs de santé ou leurs Assistants disposant d’un Compte Utilisateur.

DURÉE DE CONSERVATION:

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

DESTRUCTION DES DONNÉES:

A la fin du Contrat et à votre demande, Doctolib s’engage à détruire le Contenu Généré par l’Utilisateur sans en conserver de copie, sous réserve des obligations légales de conservation auxquelles Doctolib serait soumise.

CONDITIONS SPÉCIFIQUES AU TRAITEMENT “MISE À DISPOSITION D’UN SERVICE DE MESSAGERIE”

FINALITÉS:

Le service de messagerie est développé afin de permettre une meilleure coordination des soins, permettant aux Utilisateurs de communiquer et d’envoyer des messages textes, vidéo, photos ou des notes vocales ou d’autres médias. Cela permet les conversations entre deux Utilisateurs ou en groupe.

- Faciliter la communication entre Acteurs de santé et/ou Assistants en proposant un canal d’échange sécurisé par messagerie instantanée ;
- Permettre l’échange de Documents et de données pouvant inclure des Données à caractère personnel relatives aux Patients ;
- Permettre aux Utilisateurs du Service de Messagerie de bloquer ou débloquer un autre Utilisateur ;
- Permettre aux Utilisateurs du Service de Messagerie d’inviter de nouveaux utilisateurs ;
- Reporting, debug et statistiques ;
- Amélioration des Services ;
- Production de statistiques pour votre compte ;
- Anonymisation des données.

BASE LEGALE:

Il vous appartient de déterminer cette base légale avant toute opération de traitement.

A titre indicatif, l’intérêt légitime pourrait constituer la base légale. Vous êtes libre de mentionner à Doctolib une autre base légale.

Dans le cas où vous communiquez les Données de base patient à un Acteur de santé qui ne fait pas partie de l’équipe de soin du Patient donné, vous devez au préalable requérir le consentement de ce Patient.

PERSONNES CONCERNÉES:

- Patients ;
- Acteurs de santé ou Assistants ayant ou non un Compte Utilisateur Doctolib ;
- Utilisateurs de Réseau de l’Organisation qui peuvent être expéditeur ou destinataires des messages.

TYPES DE DONNÉES À CARACTÈRE PERSONNEL:

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

- Données d’identification ;
- Données de contact ;
- Antécédents médicaux, familiaux et allergies ;
- Données de consultation ;
- Données de prescription ;
- Données de biométrie et biologie ;
- Données relatives à l’équipe soignante ;
- Imagerie médicale ;
- Photos, videos ;
- Notes vocales ;
- Pour les appels vidéos et vocaux : le flux de données permettant la transmission entre les Acteurs de santé ou Assistants ;
- Données d’utilisation et de connexion liées à votre usage du Service de Messagerie (telles que les logs).

DESTINATAIRES:

- Les Acteurs de santé ou Assistants ayant un Compte Utilisateur ;
- Les Acteurs de santé ou Assistants sans Compte Utilisateur invités par les Utilisateurs à utiliser le Service de Messagerie.

DURÉE DE CONSERVATION :

Vous devez fixer une durée de conservation précise des données et la communiquer à Doctolib.

A moins que vous n'ayez activé l'option "Conserver la conversation" dans les réglages spécifiques de chaque conversation, tous les messages seront effacés après une durée de trente (30) jours.

Dans l'hypothèse où vous auriez activé cette option, tout le Contenu Généré par l'Utilisateur relatif à la conversation sera conservé jusqu'à ce que votre Compte Utilisateur soit supprimé ou jusqu'à ce que cette option de conservation soit désactivée.

Lors de la rupture du Contrat et/ou sur demande écrite, Doctolib s'engage à supprimer le contenu créé par l'Utilisateur sans conserver de copie, sauf dans le cas où Doctolib y serait contraint par des dispositions légales ou réglementaires.

TERMES SPÉCIFIQUES À L'EXPORT DES DONNÉES POUR LE TRAITEMENT DE MESSAGE:

Le cas échéant, vous pourrez exporter le Contenu Généré par l'Utilisateur qui est encore conservé sur les Services jusqu'à la fin de la durée totale du Contrat, en exportant directement la publication (partagée sur les canaux) ou la conversation via la fonctionnalité d'exportation disponible sur l'Application.

DESTRUCTION DES DONNÉES:

À la fin du contrat et sur votre demande formelle, Doctolib s'engage également à détruire le Contenu Généré par l'Utilisateur sans en conserver de copie, sous réserve des obligations légales de conservation auxquelles Doctolib pourrait être soumis.

MESURES TECHNIQUES ET ORGANISATIONNELLES STANDARD APPLICABLES PAR DÉFAUT

Note: ces mesures sont applicables par défaut (hors cas où un Connecteur entre la Plateforme et les systèmes d'informations tiers est mis en place). Pour plus de précisions sur les mesures applicables, se référer au Contrat d'Abonnement.

CERTIFICATIONS DE SÉCURITÉ

Voici la liste des certifications obtenues par Doctolib :

- Hébergement de Données de Santé ;
- ISO/IEC 27001:2022 ;
- ISO/IEC 27701:2019 ;
- BSI C5 ;
- TÜV (téléconsultation).

SÉCURITÉ DU PRODUIT

- **Vérification :** après création du compte Utilisateur, l'accès aux services requiert une vérification de l'identité de l'Utilisateur de l'une des deux manières suivantes:
    1. via le processus Pro Santé Connect. Si la machine de l'Utilisateur est inconnue du service d'authentification, il devra insérer sa carte CPS dans le lecteur et son code pour être identifié, ou
    2. via le processus OnFido permettant de vérifier la possession d'un document d'identité valide et une preuve de droit d'exercice de professionnel de santé (exemple : un diplôme).

- **Authentification en deux étapes :** à chaque connexion sur un nouveau matériel, l'Utilisateur doit fournir son mot de passe et un code à usage unique (2FA) obtenu via email ou sms ou via une application à usage unique (exemple : l'application Authenticator).

- **Politique de mot de passe :** composés d'au minimum 8 caractères parmi les chiffres, symboles, lettres et majuscules, les mots de passe les plus classiques sont interdits (par exemple identifiant, nom, simples suites de chiffres). Le mot de passe doit valider un test de complexité calculé dynamiquement analysant la difficulté de le casser.
  L'Utilisateur doit utiliser son identifiant de connexion et son mot de passe pour accéder aux Services.

- **Protection de la session Utilisateur :**
  Les sessions ouvertes peuvent être déverrouillées de deux manières :
    1. Par mot de passe (la session expire alors automatiquement).
    2. Par code PIN :
        a. Les codes PIN simples sont interdits.
        b. La session se verrouille automatiquement avec le code PIN après 1h d'inactivité.
        c. La session expire automatiquement toutes les nuits.

- **Processus de récupération :** Les comptes peuvent être récupérés de deux manières :
    1. Reset de mot de passe par email
    2. Reset de mot de passe par SMS avec le support Doctolib sur vérifications des informations du Compte avant de permettre sa récupération.

  Le succès d'une de ces manières aboutit à l'invalidation automatique de toutes les sessions actives.

- **Contrôle d'accès granulaire :** les Administrateurs peuvent donner des droits spécifiques à chaque Utilisateur au sein de leur organisation.

- **Traçabilité des actions :** Les actions des différents Utilisateurs d'une organisation sont consignées et journalisées. Les actions sensibles (modification des accès aux agendas, création de comptes Administrateurs) font l'objet de notifications de sécurité.

- **Protection contre le vol de compte :** les connexions réussies depuis un nouvel appareil sont notifiées à l'Utilisateur par email.

SÉCURITÉ DE LA PLATEFORME

- Les charges applicatives et les données sont stockées en toute sécurité en Europe ;

- Les systèmes d'exploitation sont **mis à jour** régulièrement pour Linux (immédiatement pour les correctifs de haute sévérité) ainsi que les mises à jour de sécurité des logiciels middleware ;
- Doctolib utilise des systèmes d'exploitation Linux avec des noyaux **renforcés** minimaux et une configuration sécurisée ;
- Doctolib applique une **segmentation** réseau rigoureuse entre les environnements de production et de non-production, en isolant chaque environnement ;
- Le trafic entrant au niveau applicatif est protégé par notre **pare-feu d'application Web** (Cloudflare) et contrôlé via des équilibres de charge d'entrée. Le trafic sortant au niveau applicatif est sécurisé par un proxy HTTP sortant, qui restreint le trafic à l'aide de whitelists ;
- Doctolib utilise Cloudflare pour atténuer les **protections contre les attaques DDOS** volumétriques.
- **Veille en sécurité :** nous surveillons en continu les menaces, vulnérabilités ou vecteurs d'attaques, qu'ils soient connus ou nouveaux.
- **Traçabilité :** nous enregistrons toute action, surveillons et alertons pour tout événement de sécurité.
- **Centres de données certifiés :** HDS, ISO 27001, BSI C5 Type 2.

DISPONIBILITÉ

- L'architecture de service de Doctolib est conçue avec la haute disponibilité et la résilience comme principes fondamentaux. Doctolib exploite deux stockages de données : un cluster principal situé dans la région AWS de Francfort et un cluster secondaire dans la région AWS de Paris ;
- Les systèmes critiques sont équipés de redondance, souvent répartis sur plusieurs zones de disponibilité pour assurer un fonctionnement continu ;
- En cas de catastrophe régionale, notre Plan de Reprise après Sinistre définit des mesures détaillées pour restaurer la fonctionnalité complète en moins de 30 minutes (RTO : Recovery Time Objective), minimisant les temps d'arrêt et les perturbations ;
- Pour garantir la préparation, notre équipe mène des tests complets de continuité d'activité et de reprise après sinistre au moins deux fois par an ;
- En cas de panne majeure dans la région principale, Doctolib peut basculer de manière transparente vers le cluster de base de données secondaire en moins de 10 minutes, assurant une perturbation minimale de nos services et maintenant la continuité des activités.

CHIFFREMENT DES DONNÉES

Chiffrement des communications :
- Toutes les données en transit sur les réseaux publics sont chiffrées. Nous utilisons le protocole TLS 1.2 standard de l'industrie, associé à un certificat SSL robuste de 4096 bits émis par l'autorité de certification renommée ;
- Le service de consultation vidéo de Doctolib est conçu pour répondre aux normes de sécurité les plus élevées, appliquant un chiffrement de bout en bout pour les communications vidéo et audio (en transit uniquement). Les flux de consultation vidéo ne sont jamais transmis via les serveurs de Doctolib ni stockés à aucun moment, garantissant que les interactions sensibles Patient-Acteur de santé restent privées.

Stockage des données :
- Pour assurer le plus haut niveau de protection des données au repos, nous employons un modèle de chiffrement à deux couches qui équilibre des normes cryptographiques robustes avec les exigences de performance et d'entreprise ;
- **Chiffrement de base pour toutes les données au repos :** la première couche de chiffrement est universellement appliquée à toutes les données stockées par Doctolib, garantissant que toutes les données, qu'elles soient liées à la santé ou non, sont chiffrées au niveau du stockage physique. Cette couche fondamentale est fournie par notre infrastructure cloud, utilisant **AES-256**. Le processus de chiffrement est effectué directement sur les supports physiques, garantissant que toutes les données sont protégées contre les accès non autorisés au niveau matériel. La gestion des clés pour cette couche est gérée séparément, les clés maîtres étant stockées en toute sécurité dans un Module de Sécurité Matériel (HSM) hébergé par Evidian ;
- **Deuxième couche de chiffrement pour les Données de santé :** cette seconde couche applique un chiffrement AES-256 côté serveur (soit au niveau des colonnes de base de données, soit au niveau des fichiers). Cette approche garantit que même si la base de données est compromise, les colonnes chiffrées restent inaccessibles sans les clés de déchiffrement appropriées. Les clés de chiffrement sont stockées en toute sécurité dans un Module de Sécurité Matériel (HSM) virtuel. Cela garantit que l'accès aux clés est strictement contrôlé, auditable et isolé de l'environnement d'application, minimisant le risque d'exposition non autorisée des clés.

CONTRÔLE D'ACCÈS

- Doctolib emploie un cadre de sécurité à confiance zéro pour fournir une protection rigoureuse pour toutes les applications de back-office utilisées par les employés et les contractants. L'accès à ces applications est sécurisé par des comptes individuels gérés via Single Sign-On (SSO) et renforcé par une authentification à deux facteurs (2FA) obligatoire ;
- Pour s'aligner sur le Principe du Moindre Privilège, l'accès à la base de données est soigneusement géré, fournissant plusieurs comptes avec différents niveaux d'autorisations basés sur les besoins spécifiques de dépannage de notre

équipe d'infrastructure. Pour ces comptes privilégiés, les actions doivent être validées par un collègue ou l'équipe de sécurité (également connu sous le nom de principe des "quatre yeux") avant de procéder ;
- De plus, nous veillons activement à ce que les droits d'accès soient rapidement ajustés si les responsabilités professionnelles d'un Utilisateur changent, renforçant notre engagement envers le modèle du moindre privilège ;
- L'accès aux Données à caractère personnel à des fins de support est strictement réglementé. Tout accès nécessite une demande de support traçable, et une alerte automatique est générée pour l'équipe de sécurité. Ce processus est facilité par un outil interne appelé Patient Privacy Patrol.

SÉCURITÉ DES APPLICATIONS

Sécurité et confidentialité *by Design* : Doctolib intègre la sécurité et la confidentialité dès le début du développement grâce à une stratégie de "shift-left", incorporant ces considérations dans les flux de travail d'ingénierie et de gestion de produit dès le départ.
Directives de développement sécurisé et formation : les directives de développement sécurisé de Doctolib sont alignées sur les normes OWASP et adaptées aux langages, frameworks et architecture spécifiques de l'entreprise.

Revue de code et gestion des changements : chaque modification du code source de l'application est suivie par notre outil de gestion de code source (i.e. Github). Le processus de gestion des changements repose techniquement sur des modifications documentées pour approbation par revue en binôme.

Tests de non-régression : le pipeline CI/CD de Doctolib intègre environ 50 000 tests unitaires et tests de bout en bout, des interrupteurs de fonctionnalités, avec une capacité de retour en arrière rapide.

Gestion des dépendances tierces : toutes les bibliothèques externes intégrées dans le code source de Doctolib font l'objet d'une surveillance et d'une gestion rigoureuses, avec un accent sur l'atténuation des risques liés aux vulnérabilités de la chaîne d'approvisionnement et au code malveillant.

Tests statiques de sécurité des applications (SAST) : Doctolib intègre une suite complète d'outils de tests statiques de sécurité des applications (SAST) dans son pipeline d'Intégration Continue (CI).

Protection contre les bots et les abus : Doctolib utilise la notation de réputation IP, CAPTCHA et la limitation de débit pour détecter et restreindre les activités malveillantes.

Tests de pénétration : Doctolib mène des tests de pénétration approfondis au moins une fois par an en partenariat avec une entreprise externe spécialisée. Ces évaluations suivent les directives OWASP pour assurer une évaluation approfondie de ses systèmes de sécurité, aidant à identifier et à atténuer les vulnérabilités potentielles.

Bug Bounty Public : Doctolib exploite un programme continu de Bug Bounty Public visant à tirer parti de l'expertise de la communauté des hackers white hat pour renforcer continuellement sa posture de sécurité.

ACCÈS PHYSIQUE À L'ÉTABLISSEMENT DE DOCTOLIB

Les bureaux de Doctolib sont sécurisés par alarme et équipés de systèmes de sécurité et de contrôle d'accès les plus modernes, que ce soit à l'entrée, dans les ascenseurs ou au niveau des étages hébergeant des zones d'activité dites sensibles.
Tous les accès autorisés aux locaux sont enregistrés.
Les visiteurs ne peuvent entrer dans les lieux qu'après inscription, et sont accompagnés d'un employé de Doctolib. Lors de visites, le visiteur ne sera jamais laissé sans surveillance ou seul.
Tous les systèmes sont exploités dans des centres de données agréés. Ceux-ci disposent de la vidéosurveillance, de systèmes de sécurité et d'un service de sécurité. Seul un petit groupe de spécialistes de Doctolib spécialement formés ont l'autorisation d'accès. Chacun de ces accès est enregistré.

Accès des employés de l'Établissement :
Les employés disposent tous d'un badge avec leur photo leur permettant d'accéder aux locaux en fonction de leur accréditation au sein de l'entreprise. L'accréditation est définie, soit en fonction du rôle de l'employé, soit en fonction de la demande de son manager qui doit être validée par le service compétent. Le port du badge est obligatoire pour chaque employé. En cas d'oubli, l'employé se rend à l'accueil et doit présenter une carte d'identité ou un passeport à l'agent de l'accueil. Ce dernier vérifie son identité auprès du référentiel RH et si la vérification est concluante, lui remet un badge temporaire (à rendre le soir même au plus tard auprès de l'accueil).

Lien avec le SI de l'Établissement :
Le lien avec le SI de l'Établissement peut s'effectuer de plusieurs façons:
- Connecteur API entre l'agenda Doctolib et l'agenda du SI ;
- Connecteur local, l'agenda Doctolib permet de remonter la fiche Patient du SI ;
- VPN IPSec entre le serveur et Doctolib (afin de confirmer la disponibilité)

MESURES TECHNIQUES ET ORGANISATIONNELLES APPLICABLES UNIQUEMENT QUAND UN CONNECTEUR A ÉTÉ MIS EN PLACE AFIN DE PERMETTRE L'INTEROPÉRABILITÉ ENTRE LA PLATEFORME ET LES SYSTÈMES D'INFORMATION TIERS

Note: Pour plus de précisions sur les mesures applicables, se référer au Contrat d'Abonnement.

Interopérabilité entre systèmes

- S'il existe un Connecteur entre les systèmes d'information de l'Abonné et les systèmes d'information de Doctolib, afin de garantir l'interopérabilité des systèmes, les flux et Documents transmis via les API font l'objet d'un déchiffrement par l'application Doctolib avant transmission ;
- L'Abonné reçoit une clé secrète de Doctolib afin de permettre à son système d'information de s'authentifier auprès du système Doctolib. L'Abonné est responsable de la confidentialité de cette clé secrète et de garantir sa protection selon les meilleures pratiques, notamment son chiffrement au repos des clés et le contrôle d'accès ;
- L'Abonné doit s'assurer que son système d'information est capable de s'authentifier et de mettre en œuvre un mécanisme de nouvelle tentative ;
- En cas de suspicion de compromission de la clé secrète, l'Abonné doit en informer Doctolib sans délai, afin d'initier une procédure de renouvellement de clé ;
- L'Abonné se verra proposer par Doctolib de restreindre l'utilisation de la clé secrète à un ensemble d'adresses IP fixes de son système d'information. Si l'Abonné choisit de ne pas restreindre l'utilisation de la clé secrète à ses adresses IP fixes, il est convenu que l'Abonné comprend qu'en cas de compromission de la clé, Doctolib ne peut être tenu responsable de l'utilisation frauduleuse de ladite clé par une personne ou un système non autorisé ;
- L'API utilise un Code d'Authentification de Message basé sur le Hachage (HMAC) pour garantir l'authentification et l'intégrité de tous les messages échangés. Cela garantit que les données restent sécurisées et inviolables pendant la transmission.

MESURES TECHNIQUES ET ORGANISATIONNELLES APPLIQUÉES PAR DOCTOLIB DANS LE CADRE DES TRAITEMENTS DE DONNÉES LIÉES AUX SERVICES DE MESSAGERIE ET DOCTOLIB CONNECT ORGANISATIONS

Politiques et contrôles organisationnels et administratifs

Doctolib a mis en place un système de gestion de la sécurité de l'information (SMSI) et est certifiée selon ISO27001 et NEN7510 (norme néerlandaise pour la gestion de la sécurité de l'information dans le secteur de la santé).

Données de message – données en transit

Pour comprendre les solutions permettant d'atténuer les risques pour les données en transit, veuillez lire le livre blanc sur la sécurité (https://www.siilo.com/resources/security-white-paper) de Doctolib, qui décrit en détail l'approche de sécurité dès la conception, le modèle de menace et les protocoles cryptographiques.

En bref, Doctolib utilise un chiffrement de bout en bout implémenté avec LibSodium, un fork de la bibliothèque cryptographique NaCl https://nacl.cr.yp.to/. ;

Cela signifie que chaque message entre l'expéditeur et le destinataire est protégé par une paire de clés publique/privée. Seuls l'expéditeur et le destinataire sont capables de déchiffrer et de lire les messages qu'ils échangent, et l'authenticité de tout message peut être vérifiée empiriquement. Les tiers, y compris Doctolib et ses employés, ne sont jamais en mesure de les lire.

Doctolib utilise l'épinglage de certificat pour empêcher les attaques dites « de l'homme du milieu », un processus par lequel les attaquants accèdent au trafic entre les téléphones et tentent de s'introduire et d'exploiter les lignes de communication pour lire les messages. Les communications TLS v1.2 standard nécessitent un certificat SSL valide émis par une autorité de certification approuvée, reconnue par l'appareil. L'épinglage de certificats va plus loin et exige que ces certificats ne soient émis qu'à partir d'une chaîne de confiance enracinée dans un émetteur spécifié. Cela met fin à une litanie de vulnérabilités découlant des problèmes de distribution des clés associés à l'infrastructure des autorités de certification d'Internet.

Données de message – données au repos sur l'appareil de l'utilisateur

Pour les données au repos sur l'appareil (iPhone, iPad, Android), les mesures de protection suivantes sont en place :

- Tous les « éléments clés », également connus sous le nom de codes utilisés par le cryptographe, sont stockés dans le Trousseau iOS ou le Magasin de clés Android, selon le cas ;
- Tout le « matériel de clé » est crypté par une « clé maîtresse » dérivée du code PIN choisi par l'utilisateur ;
- L'ensemble de la base de données est chiffré à l'aide de SQLiteCipher. Tous les messages, les métadonnées des messages et les informations de contact sont stockés de cette manière ;
- Tous les médias reçus sont stockés cryptés par la clé de cryptage symétrique à usage unique. Cette clé est accessible via la base de données mentionnée ci-dessus ;
- Un mécanisme de code PIN au niveau de l'application empêche l'accès par les personnes qui ont un accès physique à l'appareil. Cela concerne la plupart des formes d'ingénierie sociale en personne, telles que demander d'emprunter le téléphone pour un appel rapide, etc. ;
- Toutes les informations échangées dans le Service de Messagerie sont automatiquement supprimées après 30 jours. Les Utilisateurs peuvent décider eux-mêmes de supprimer des messages individuels au cas par cas s'ils jugent que cette période de 30 jours est trop longue. Doctolib a sciemment omis d'inclure des comptes à rebours et des durées de vie des messages telles que les secondes/heures, car cela pourrait créer un sentiment d'urgence entraînant des captures d'écran et d'autres comportements indésirables du côté du destinataire ;
- Lorsqu'un Utilisateur sait que son appareil est perdu, volé ou compromis d'une autre manière, il peut alerter son organisation (il s'agit d'une fonctionnalité de Doctolib Connect Organisations) et un Administrateur peut effacer à distance les données Doctolib de l'appareil.

Données de message – données au repos sur les serveurs Doctolib

Pour les données au repos sur les serveurs Doctolib, les mesures de protection suivantes sont en place :

- Tous les médias (envoyés via l'application et donc considérés comme sensibles) sont stockés et chiffrés par la clé de chiffrement symétrique à usage unique. Cette clé n'est stockée sur aucun serveur Doctolib. Les clés pour déchiffrer ces

données ne sont disponibles que sur les appareils de l'expéditeur et du destinataire. Stockage des Données à caractère personnel sur les serveurs Doctolib ;

- Les données des messages sont stockées sur des serveurs à Francfort (Allemagne) et à des fins de sauvegarde, des "instantanés" automatiques quotidiens sont pris et conservés pendant 7 jours maximum. Ces instantanés sont chiffrés au repos.

Données de l'utilisateur

Les données utilisateur sont stockées sur des serveurs à Dublin (Irlande) et sont sauvegardées quotidiennement et conservées pendant 30 jours maximum dans un compartiment préconfiguré qui est chiffré au repos.

Correspondance des numéros de téléphone sur le service de messagerie

Doctolib permet éventuellement à l'Utilisateur de découvrir d'autres contacts Doctolib Connect en les croisant avec le carnet d'adresses du téléphone. Si l'Utilisateur choisit de le faire, les numéros de téléphone sont hachés et téléchargés via une connexion TLS chiffrée vers le serveur (les 64 premiers bits du hachage SHA1 de la forme normalisée E.164 de chaque numéro de téléphone trouvé dans le carnet d'adresses du téléphone).

Seuls les numéros de téléphone sont hachés et recoupés. Doctolib n'intervient pas sur les noms, adresses e-mail et autres informations contenues dans le carnet d'adresses du téléphone. Le serveur Doctolib compare ensuite la liste des hachages de l'Utilisateur avec les hachages téléphoniques connus des Utilisateurs actuels de Doctolib Connect. Le serveur ne correspondra qu'aux Utilisateurs actuels de Doctolib Connect, et après avoir renvoyé les correspondances au client mobile, le serveur rejette immédiatement les hachages soumis.

LISTE DES SOUS-TRAITANTS ULTÉRIEURS

Dans le cadre de la fourniture de ses services, Doctolib fait appel à des prestataires qui agissent comme Sous-traitants ultérieurs. Ces derniers peuvent avoir accès aux Données à caractère personnel collectées par Doctolib uniquement dans le cadre et pour les besoins des opérations de traitement mentionnées ci-dessous. Doctolib veille à ce que chacun de ces Sous-traitants ultérieurs mette en place des mesures techniques et organisationnelles appropriées pour garantir la sécurité et la confidentialité des données traitées.

En cas de transfert en dehors de l'EEE - Espace économique européen (lorsque le serveur se trouve en dehors de l'EEE) ou en cas de risque d'un tel transfert (lorsque le serveur se trouve dans l'EEE mais que le pays d'origine du prestataire de services se trouve en dehors de l'EEE), Doctolib recourt aux services du Sous-traitant sur la base d'un instrument de transfert conforme au RGPD et met en place des mesures supplémentaires pour garantir un niveau de protection des données substantiellement équivalent à celui du RGPD.

Conformément au RGPD et dans un souci de transparence, Doctolib communique ci-dessous la liste de ses Sous-traitants.

Liste des Sous-traitants utilisés dans la cadre des services Doctolib présentés par catégories d'activités.

Hébergement:

Sous-traitant	Pays d'origine	Localisation des serveurs	Type de tâche effectuée
Atos	France	France	Hébergement de la clé de chiffrement de Doctolib
AWS EMEA	Maison mère : Etats-Unis Entité contractante : Luxembourg	UE	Hébergement des données de Services Doctolib
Cloudinary	Etats-Unis	Etats-Unis	Hébergement des photographies des Acteurs de santé
S3NS	France	Pays-Bas	Hébergement des données de Services Doctolib

Support:

Sous-traitant	Pays d'origine	Localisation des serveurs	Type de tâche effectuée
TeamViewer	Allemagne	UE	Offrir un service d'assistance à distance sous supervision de l'Utilisateur/ Abonné
Microsoft	Etats-Unis	UE	Stockage des enregistrements effectués dans le cadre d'opérations de support Utilisateurs / Abonnés
Walkme	Israël	UE	Surveiller, gérer et afficher dans l'application du contenu à destination des Utilisateurs / Abonnés
Salesforce	Maison mère : Etats-Unis Entité contractante : France	France	Gérer la relation client

Webhelp	France	France	Gérer les demandes de support des Utilisateurs/Abonnés
Calendly	Etats-Unis	UE	Faciliter la prise en charge et les rendez-vous avec les Utilisateurs / Abonnés
Atlassian	Maison mère : Australie Entité contractante : France	UE	Gérer les demandes de support des Utilisateurs/Abonnés
Datadog	Etats-Unis	UE	Surveiller et investiguer les alertes et bugs

Télécoms:

Sous-traitant	Pays d'origine	Localisation des serveurs	Type de tâche effectuée
Iagility	France	UE	Envoi des rappels de rendez-vous à destination des Patients (sms)
Sinch	Suède	UE	Envoi des rappels de rendez-vous à destination des Patients (sms)
SMSMODE (Calade technologie)	France	UE	Envoi des rappels de rendez-vous à destination des Patients (sms)
Sendinblue	France	UE	Envoi des rappels de rendez-vous à destination des Patients (emails)
Flowmailer	Pays-Bas	UE	Envoi des rappels de rendez-vous à destination des Patients (emails)
Braze	Etats-Unis	UE	Permet à Doctolib de gérer ses campagnes de communication avec les Utilisateurs/ Abonnés et d'évaluer l'impact de ses campagnes afin d'améliorer le contenu de ces dernières

Marketing:

Sous-traitant	Pays d'origine	Localisation des serveurs	Type de tâche effectuée
Guideflow	UE	UE	Aide Doctolib à faire des démonstrations de ses Services

Sécurité informatique:

Sous-traitant	Pays d'origine	Localisation des serveurs	Type de tâche effectuée
Cloudflare	Etats-Unis	UE	Aide Doctolib à se prémunir contre les attaques

			du type CDS et DDos

Autres :

Sous-traitant	Pays d'origine	Localisation des serveurs	Catégorie de service concerné	Type de tâche effectuée
Zapier	Etats-Unis	Etats-Unis	Logiciel d'automatisation de flux entre applications web	Permet à Doctolib d'automatiser la transmission de flux de données entre différentes applications web
Microsoft Azure	Etats-Unis	UE	Recherche et développement des Services	Aide Doctolib à traiter et analyser les données
Google Ireland	Ireland	Etats-Unis	Google My Business	Faciliter la prise de rendez-vous par les patients et leurs proches via vos profils Google Business
Adyen	Pays-Bas	UE	Paiements	Gérer les paiements en ligne pour les téléconsultations
Anthropic	Etats-Unis	UE	Fourniture du modèle de LLM	Analyse et création de contenu à des fins d'automatisation de tâches
Google Ireland (Gemini)	Etats-Unis	UE - Etats-Unis	Fourniture du modèle de LLM	Analyse et création de contenu à des fins d'automatisation de tâches

Liste des Sous-traitants utilisés dans le cadre du Service de Messagerie et du Service Doctolib Connect Organisations présentés par catégories d'activités :

Sous-traitant	Pays d'origine	Localisation des serveurs	Catégorie de service concerné	Type de tâche effectuée
AWS EMEA	Maison mère : Etats-Unis Entité contractante : Luxembourg	UE	Hébergement	Hébergement des données de Services Doctolib
Twilio	Etats-Unis	Irlande	Appel VOIP	Aide Doctolib à fournir les fonctionnalités de VOIP dans l'Application

				(appel depuis internet) et d'appel vidéo
CM.com	Pays-Bas	Pays-Bas	Télécoms	Envoi de SMS aux utilisateurs avec un code pour confirmer qu'ils ont accès au matériel connecté à un numéro spécifique
Firebase	Etats-Unis	UE	Analytique et rapport d'incidents	Aide Doctolib à faire des analyses et des rapports d'incidents dans l'Application IOS et Android. Cela lui permet aussi d'envoyer des notifications pour l'application Android et de créer des liens dynamiques pour les non-utilisateurs
Sentry	Etats-Unis	Etats-Unis	Analytique et rapport d'incidents	Aide Doctolib à contrôler et suivre les erreurs dans l'Application
ZenDesk	Etats-Unis	UE	Système de ticketing	Les Utilisateurs peuvent donner des avis depuis l'Application. En raison d'un grand nombre d'interactions, Doctolib utilise un système de ticketing afin de gérer les échanges entre son personnel et les Utilisateurs
Looker	Etats-Unis	Etats-Unis mais aucune Donnée à caractère personnel n'est stockée dans la base de données de Looker	Création de tableau de bord	Doctolib utilise Looker comme plateforme de création de tableau de bord et de BI qui se connecte à la base de données Amazon Redshift. Bien qu'aucune donnée ne soit stockée de manière permanente chez Looker, ce dernier (pour traiter et visualiser les données) a besoin

				d’une connexion et d’un cache temporaire de la base de données Redshift afin de pouvoir le faire