# ACCORD SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

## 1. OBJET

Le présent Accord sur la protection des données 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 l'Abonné/Utilisateur 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 ").

## 2. DÉFINITIONS

Les définitions attachées au présent Accord sur la protection des données 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 unissant Doctolib et l'Abonné/Utilisateur.

## 4. STATUT DES PARTIES

Les Parties sont convenues que l'Utilisateur/Abonné est le Responsable de traitement et Doctolib est le Sous-Traitant concernant les Traitements des Données à caractère personnel et Données de santé, mentionnés en Annexe 1, qu'elles soient fournies directement ou indirectement à Doctolib par l'Utilisateur/Abonné ou par un Administrateur qui s'est vu accorder par l'Utilisateur/Abonné l'accès aux Services.

Doctolib est autorisée par l'Utilisateur/Abonné à traiter, pour le compte du Responsable de traitement, les Données à caractère personnel et Données de santé nécessaires à la fourniture des Services 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 la demande expresse de l'Utilisateur/Abonné et sous son contrôle et sa responsabilité, Doctolib pourra néanmoins l'assister dans l'importation des Données de base patient au sein de la Plateforme Doctolib.

Dès lors que le Responsable de traitement renseigne 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, il doit respecter les prescriptions légales sur l'information et/ou le consentement de ces tiers.

### 4.1. Obligations de l'Utilisateur/Abonné

L'Utilisateur et/ou l'Abonné, en sa qualité de Responsable de traitement, est 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 appartient également à ce dernier d'informer 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, l'Utilisateur et/ou l'Abonné est seul responsable de l'exactitude, de la fiabilité et de la pertinence des Données à caractère personnel et Données de santé. Il est notamment responsable de l'utilisation de la Plateforme Doctolib et des Documents qu'il dépose, stocke, consulte et sort de l'espace de stockage. Il lui incombe de faire toutes les déclarations nécessaires. L'Utilisateur et/ou l'Abonné s'engage 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.

L'Utilisateur et/ou l'Abonné s'engage 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 représenter le Responsable de traitement et le cas échéant un délégué à la protection des Données à caractère personnel 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. Obligations de Doctolib**

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 la seule instruction préalable du Responsable de traitement. En cas d'impossibilité ou de difficulté dans la réalisation de certaines instructions, Doctolib en informera le Responsable de traitement dans les meilleurs délais. Doctolib peut formuler une demande écrite de dérogation aux instructions. Doctolib devra recueillir l'autorisation écrite, préalable et spécifique du Responsable de traitement pour pouvoir procéder à cette dérogation ;

- Ne pas faire de copie des Données à caractère personnel et Données de santé sans autorisation ou instruction du Responsable de traitement, 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 qui lui sont confiées par le Responsable des traitements. 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 ;

- Notifier dans les meilleurs délais le Responsable de traitement 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 communiquées par le Responsable de traitement 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 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 Personnelles.

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.

Doctolib met en œuvre tous les moyens nécessaires pour aider le Responsable de traitement 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 la disposition du Responsable de traitement toutes les informations nécessaires concernant les Traitements des Données à caractère personnel et Données de santé afin de l'assister dans l'accomplissement de ses obligations légales et réglementaires en tant que Responsable de traitement conformément aux dispositions du RGPD (annexe 3.1).

En l'absence d'instruction particulière de la part du Responsable de traitement 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, le Responsable de traitement reconnait et accepte que celles ci seront traitées selon les modalités mentionnées dans les Annexes 1 et 2. En tant que Responsable de traitement, l'Utilisateur/Abonné peut demander à Doctolib lors de l'exécution du Contrat à ce que ces modalités soient modifiées.

## 5. VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

Doctolib notifie au Responsable de traitement 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 le Responsable de traitement.

Cette notification est accompagnée, sur demande du Responsable de traitement, de toute documentation utile afin de permettre à celui-ci, 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 le compte du Responsable de traitement conformément aux dispositions du RGPD.

## 7. INFORMATION ET DROITS DES PERSONNES CONCERNÉES

Il appartient au Responsable de traitement 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 d'assister le Responsable de traitement dans cette information, Doctolib publie sur le Portail Patient une Politique de protection des données à caractère personnel accessible à l'adresse https://www.doctolib.fr/terms/agreement

## 8. GESTION DES DROITS

Il appartient au Responsable de traitement 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 demande du Responsable de traitement, pourra assister le Responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des Personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage), droit d'organiser le sort de ses 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 le Responsable de traitement afin que ce dernier puisse donner suite à sa demande.
Doctolib, à la demande de celui-ci pourra assister ce dernier dans les suites à donner aux demandes mais ne pourra répondre directement aux demandes desdites Personnes concernées.

## 9. SÉCURITÉ ET CONFIDENTIALITÉ

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 des Données à caractère personnel de l'Utilisateur/Abonné, comme indiqué dans l'Annexe 2 (Mesures techniques et organisationnelle). 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.

Les obligations visées ci-dessus ne déchargent en aucun cas l'Utilisateur/Abonné 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 sur la protection des données pourra être mis à disposition de la CNIL ou tout autorité compétente en cas de contrôle.

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

**9.3 Détention des données** : Sauf Accord sur la protection des données exprès contraire, le Responsable de traitement demeure 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 publiées par le Responsable de traitement. Les statistiques anonymisées d'utilisation du Portail Patient sont la propriété de Doctolib.

## 10. PERSONNEL DE DOCTOLIB

Doctolib affecte à la réalisation des Services des équipes suffisantes et qualifiées disposant des compétences techniques et/ou fonctionnelles nécessaires à la fourniture des Services. Les personnes habilitées à traiter des Données à caractère personnel et/ou Données de santé pour le compte du Responsable de traitement sont formées à la réglementation en matière de protection des Données à caractère personnel.

## 11. SOUS TRAITANCE ULTÉRIEURE

L'Utilisateur/Abonné concède à Doctolib une autorisation écrite générale lui permettant de faire appel aux Sous-Traitants ultérieurs énumérés ici, quand cela est raisonnablement nécessaire pour fournir les Services. Conformément à cette autorisation générale, Doctolib s'engage à informer chaque Utilisateur/Abonné, 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, offrant ainsi à l'Utilisateur/Abonné la possibilité de soulever toute objection qu'il pourrait avoir à l'égard de ces changements. Si l'Utilisateur/Abonné a des raisons légitimes et raisonnables de s'opposer à la nomination d'un nouveau Sous-Traitant ultérieur, l'Utilisateur doit immédiatement motiver sa 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 l'Utilisateur/Abonné sera réputé avoir approuvé et accepté cette nomination.

Après discussions et en l'absence d'accord entre Doctolib et l'Utilisateur/Abonné, l'Utilisateur/Abonné pourra, 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 les Données à caractère personnel et Données de santé des Abonnés/Utilisateurs ainsi que 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 le Responsable de traitement de l'exécution par les Sous-Traitants ultérieurs de ses obligations conformément aux termes du Contrat.

## 12. CERTIFICATION HDS

12.1. Conformément à l'article L1111-8 du Code de la santé publique et du Décret n°2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel, l'hébergeur des Services Doctolib, Amazon Web Services SARL (AWS) dont le siège social est situé 38 avenue John F. Kennedy, L - 1885 Luxembourg, est certifié HDS (Hébergeur de Données de Santé).

AWS a obtenu le 28 janvier 2021 un certificat "hébergeur d'infrastructures physiques" et un certificat "hébergeur infogéreur". La date du prochain renouvellement de ces certificats est fixée au 13 janvier 2025.

Les Données à caractère personnel de santé sont hébergées par AWS à Francfort (Allemagne) et à Paris (France). En qualité d'Hébergeur de Données de Santé, Doctolib confie à AWS la sous-traitance des services suivants relatifs à l'hébergement de la Plateforme Doctolib : "mise à disposition et le maintien en condition opérationnelle de sites physiques destinés à accueillir l'infrastructure physique du système d'information utilisé pour le traitement des données de santé ; fourniture et maintien en condition opérationnelle de l'infrastructure physique du système d'information utilisé pour le traitement des données de santé ; mise à disposition et la maintenance de l'infrastructure virtuelle du système d'information servant au traitement des données de santé ; mise à disposition et la maintenance de la plateforme d'hébergement des applications du système d'information ; sauvegarde des données de santé".

12.2 Conformément à l'article L1111-8 du Code de la santé publique et en tant qu'Hébergeur de Données de Santé certifié, AWS :

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

(ii) met à disposition de Doctolib des fonctionnalités lui permettant (a) d'assurer le droit à la portabilité des Utilisateurs 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 à caractère personnel 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.

12.3. Doctolib est également titulaire d'un certificat "hébergeur infogéreur" depuis le 14 octobre 2021 pour le périmètre "fourniture de services informatiques Infogérés incluant des données personnelles d'identification, des données de santé (y compris des données médicales), couvrant les activités ANS n°5 et n°6 du Référentiel HDS version 1.1 (2018)", conformément à la déclaration d'applicabilité (DdA) version 1.2 datée du 14 septembre 2021. La date de renouvellement de ce certificat est fixée au 14 octobre 2024.

12.4 Les Données à caractère personnel de santé sont hébergées par Doctolib à Francfort (Allemagne) et Paris (France). Doctolib s'engage à ne pas utiliser les Données à caractère personnel de santé à d'autres fins que l'exécution de l'activité d'hébergement de données de santé, sauf instruction documentée contraire provenant du Responsable de traitement.

12.5 Doctolib notifie au Responsable de traitement toute violation de Données à caractère personnel de santé dans les conditions de l'article 5 du présent Accord.

12.6 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 des Données à caractère personnel de santé de l'Utilisateur/Abonné, comme indiqué dans l'Annexe 2 (Mesures techniques et organisationnelle). A ce titre, les Données à caractère personnel 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.

12.7 A la fin du Contrat ou sur demande de l'Abonné en cas de retrait de la certification HDS de Doctolib, l'Abonné et l'Utilisateur pourront récupérer les Données à caractère personnel de santé hébergées par Doctolib dans les conditions mentionnées par l'article 14 du présent Accord.

12.8 Le Responsable de traitement, quant à lui, s'engage à respecter la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S).

## 13. AUDIT

13.1 Afin de mesurer la sécurité des Services, le Responsable de traitement pourra faire réaliser à ses 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 étant facturé au Responsable de traitement.

13.2 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 de Services, systèmes, réseaux, logiciels et/ou matériels informatiques autres que ceux alloués à l'usage exclusif de l'Utilisateur/Abonné; (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 et l'application 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. Sur demande du Responsable de traitement, Doctolib communiquera à celui-ci les rapports d'audit de certification délivrés par l'organisme de certification destinés à une telle communication.

13.3 Le Responsable de traitement devra 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.

13.4 Les informations obtenues au cours de l'audit sont des Informations Confidentielles et devront être traitées comme telles par le Responsable de traitement. 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 le Responsable de traitement souhaite faire appel à un auditeur externe, le Responsable de traitement devra 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.

Le Responsable de traitement s'engage 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.

## 14. RÉCUPÉRATION DES DONNÉES

L'Abonné et l'Utilisateur pourront récupérer les Données de base patient ainsi que l'historique de leurs rendez-vous à la fin du Contrat, sauf dans le cas où ces données auraient été collectées de façon illicite par l'Abonné et/ou l'Utilisateur. Ces données seront mises à disposition de l'Utilisateur/Abonné 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 disposition de l'Utilisateur/Abonné, 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 l'accès de l'Utilisateur/Abonné aux Services Doctolib, quelle qu'en soit la cause, Doctolib met l'Utilisateur en mesure de récupérer, par tout moyen et sur tout support, la dernière copie de ses Données de base patient ainsi que de son historique de rendez-vous (sauf dans le cas où ces données auraient été collectées de façon illicite par l'Utilisateur).

A la fin du Contrat et sur demande formelle du Responsable de traitement, Doctolib s'engage également à détruire les Données à caractère personnel de santé sans en garder de copie, sous réserve d'obligations de conservation légales auxquelles Doctolib

serait soumise. La politique de destruction des Données à caractère personnel de santé peut être communiquée sur demande du Responsable de traitement.

### 15. TRANSFERTS DE DONNEES A CARACTERE PERSONNEL

Les Données à caractère personnel peuvent faire l'objet, pour les finalités listées dans le présent Accord sur la protection des données personnelles, d'un transfert à destination des sociétés du groupe de 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 informe l'Utilisateur/Abonné 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 ici.

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 au nom et pour le compte du Responsable de Traitement afin de respecter ses obligations légales. Dans ce cas, et sauf disposition légale contraire, Doctolib s'engage à notifier le Responsable de Traitement de cette communication.

### 16. CONTACT

En cas de questions sur le Traitement des Données à caractère personnel et Données de santé effectué par Doctolib conformément aux stipulations contractuelles, l'Utilisateur/l'Abonné peut contacter le DPO 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.

### 17. LOI APPLICABLE

L'Accord est régi et interprété conformément à la législation nationale applicable au Responsable du traitement.

### 18. 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 l'Utilisateur/Abonné et Doctolib.

# ANNEXE 1 : DÉTAILS SUR LE TRAITEMENT DES DONNÉES PERSONNELLES

Cette Annexe 1 contient certains détails relatifs au Traitement des Données à caractère personnel et Données de santé, conformément à l'article 28(3) du RGPD.

**RESPONSABLE DE TRAITEMENT :** l'Abonné ayant souscrit un Abonnement Doctolib et/ou l'Utilisateur ayant un Compte Utilisateur Doctolib.

Les activités du Responsable de traitement comprennent des Traitements permettant l'exercice des activités de prévention, de diagnostic et de soins ainsi que la gestion administrative de son établissement de santé, centre de santé ou cabinet libéral.

Les Traitements permettent notamment, pour les besoins de la prise en charge des patients (i) la gestion des rendez-vous ; (ii) la gestion des dossiers médicaux nécessaires au suivi du patient ; (iii) le recours aux pratiques de soins à distance requérant des technologies de l'information et de la communication, telles que la télémédecine et le télésoin ; (iv) les communications entre professionnels identifiés et structures de soins participant à la prise en charge de la Personne concernée et à la coordination de celle-ci ; (v) l'établissement et la télétransmission des documents destinés à la prise en charge des frais de santé par l'assurance maladie (feuilles de soins, arrêt de travail, protocole de soins électroniques, etc.) ; (vi) la tenue de la comptabilité.

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.

**SOUS-TRAITANT(S) :** Doctolib SAS

Les activités effectuées par le Sous-traitant pour le compte des Responsables de traitement sont décrites ci-dessous.

---

## TRAITEMENT N°1 : PARAMÉTRAGE DES COMPTES ABONNÉS ET UTILISATEURS

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**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 ;

**BASE LÉGALE DU TRAITEMENT** :

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.
Afin d'aider le Responsable de traitement, la CNIL a mis à disposition un référentiel qui propose, à titre indicatif, l'intérêt légitime comme base légale. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

**PERSONNES CONCERNÉES :**

Abonné et Utilisateur tels que définis dans le Contrat.

**TYPES DE DONNEES A CARACTERE PERSONNEL** :

Dans un souci de minimisation des Données à caractère personnel traitées, le Responsable de traitement doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle.

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

a) **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, identifiant compte Stripe.
b) **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.
c) Les **logs d'utilisation et de connexion** qui rendent compte des "actions métiers" des Utilisateurs au sein de la Plateforme Doctolib ainsi que les **logs techniques** qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur/Abonné afin que Doctolib puisse assurer le fonctionnement et l'accès aux fonctionnalités demandées.

Sauf instruction particulière de la part du Responsable de traitement, Doctolib traite toutes les Données à caractère personnel mentionnées ci-dessus afin de fournir le Service, objet du Contrat.

**DESTINATAIRES ET SOUS TRAITANTS ULTÉRIEURS:**

Se référer à la liste mentionnée à l'article 11 du présent Accord.

**DURÉE DE CONSERVATION:**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée à Doctolib.
A défaut d'une telle instruction de la part du Responsable de traitement, Doctolib appliquera les durées de conservations telles que recommandées par la CNIL ou la législation applicable.

## TRAITEMENT N°2 : LA GESTION DES RENDEZ VOUS & DE L'AGENDA

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel et Données de santé listées ci-dessous.

**FINALITÉS DU TRAITEMENT :**

- Accompagnement dans la récupération des données attachées aux Agendas ;
- Respecter les règles relatives à l'identito vigilance ;
- Permettre au Responsable de traitement de gérer son Agenda ;
- Permettre au Responsable de traitement de gérer le parcours de soin des Patients et de leurs Proches ;
- Permettre au Responsable de traitement de gérer son Agenda, d'organiser la prise en charge des Patients au sein de son établissement de santé ou de son cabinet en cas de crise sanitaire ;
- Permettre la prise de rendez-vous en ligne par les Patients 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 ;
- 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 le référencement des Données à caractère personnel et de santé des Patients avec l'identité INS véhiculées par le Responsable de traitement ou le responsable de référencement sélectionné par le Responsable de traitement 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.

**BASE LÉGALE DU TRAITEMENT :**

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.
Afin d'aider le Responsable 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. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

**PERSONNES CONCERNÉES :**

Les Patients et leurs Proches, confrères des Acteurs de santé.

**TYPES DE DONNEES A CARACTERE PERSONNEL :**

Dans un souci de minimisation des Données à caractère personnel et Données de santé traitées, le Responsable de traitement doit veiller à ne collecter et utiliser que les Données à caractère personnel et Données de santé pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle.

Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :
a) **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.
b) **la situation professionnelle du Patient ou du Proche** : la profession.
c) **Santé** : statut d'assuré, identité et coordonnées du médecin traitant, identité et coordonnées du médecin adressant, date/heure et lieu du rendez-vous, spécialité du médecin et nature de la consultation, statut du rendez-vous, documents médicaux du Patient, notes complétées par l'Acteur de santé, 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) ;
d) Les **logs d'utilisation et de connexion** qui rendent compte des "actions métiers" des Utilisateurs au sein de la Plateforme Doctolib ainsi que les **logs techniques** qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur afin que Doctolib puisse assurer le bon fonctionnement et l'accès aux fonctionnalités demandées.

Sauf instruction particulière de la part du Responsable de traitement, Doctolib traite toutes les Données à caractère personnel et Données de santé mentionnées ci-dessus afin de fournir le Service, objet du Contrat.

**DESTINATAIRES ET SOUS TRAITANTS ULTÉRIEURS:**

- les Acteurs de santé ;
- les personnes en charge du secrétariat, dans le respect des dispositions sur le secret professionnel ;
- les personnes habilitées au sein de Doctolib ;
- les Sous-traitants ultérieurs : Se référer à la liste mentionnée à l'article 11 du présent Accord.

**DURÉE DE CONSERVATION:**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée à Doctolib.
Par défaut et sauf instruction contraire de la part du Responsable de traitement, cette dernière sera fixée à 5 ans pour l'historique de rendez-vous.
Le Responsable de traitement est libre de communiquer à Doctolib une durée de conservation différente comprise entre 1 an et 20 ans.
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.

### TRAITEMENT N°3 : SERVICE DE TÉLÉCONSULTATION

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS DU TRAITEMENT :**

- Permettre au Responsable de traitement de disposer d'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
- 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 aux Patients des Utilisateurs et/ou Abonnés pour les informer de l'ouverture du Service de Téléconsultation de leurs praticiens.

**BASE LÉGALE DU TRAITEMENT :**

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.
Afin d'aider le Responsable 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. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

**PERSONNES CONCERNÉES :**

Les Patients et leurs Proches

**TYPES DE DONNEES A CARACTERE PERSONNEL :**

Dans un souci de minimisation des Données à caractère personnel traitées, le Responsable de traitement doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle.

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

a) **l'identité et coordonnées du Patient ou du Proche** : Genre, nom, prénom
b) **Le flux vidéo** permettant la vidéo transmission entre le Patient et l'Acteur de santé lors de la Téléconsultation
c) Information de session de Téléconsultation : Erreur & bug, heure de début et de fin de la Téléconsultation, débit vidéo et sonore, information concernant l'état des Équipements utilisés pour la Téléconsultation (niveau de batterie, accès caméra et micro), retour d'information sur la Téléconsultation

d) **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)
e) Les **logs d'utilisation et de connexion** qui rendent compte des "actions métiers" des Utilisateurs au sein des services Doctolib ainsi que les **logs techniques** qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur afin que Doctolib puisse assurer le fonctionnement et l'accès par l'Utilisateur aux fonctionnalités désirées.

Sauf instruction particulière de la part du Responsable de traitement, Doctolib traite toutes les Données à caractère personnel mentionnées ci-dessus afin de fournir le Service, objet du Contrat.

**DESTINATAIRES ET SOUS TRAITANTS ULTÉRIEURS:**

Se référer à la liste mentionnée à l'article 11 du présent Accord.

**DURÉE DE CONSERVATION:**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée 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.

### TRAITEMENT N°4 : MISE À DISPOSITION D'UN LOGICIEL DE GESTION DE CABINET

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS :**

1/ Mise à disposition des Responsables de traitement d'un Service de logiciel de gestion de cabinet leur permettant notamment :

- d'exercer leur activité de prévention, de diagnostic, de soin et de gestion de leur cabinet en leur 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 personnelles et de santé avec l'identité INS qualifiée.

2/ Support technique et assistance : Assurer le support technique, la maintenance, l'administration et le traitement des demandes des Utilisateurs et Abonnés, le conseil, le stockage, l'hébergement du Service de logiciel de gestion de cabinet.

3/ Mises à jour et amélioration du Service de logiciel de gestion de cabinet à la demande du Responsable de traitement.

4/ Accompagnement dans la gestion des imports et des exports des Données base patient pour le compte et sous la responsabilité du Responsable de traitement.

5/ Reporting, debug et statistiques.

**BASE LÉGALE DU TRAITEMENT** :

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.
Afin d'aider le Responsable 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. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

**PERSONNES CONCERNÉES :**

Les Patients ainsi que leurs Proches suivis par les Utilisateurs et les éventuels confrères de ces derniers.

**TYPES DE DONNÉES CONCERNÉES :**

Il est rappelé qu'il appartient aux Responsables de traitement 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 appartient aux Abonnées/Utilisateurs d'obtenir l'accord préalable du Patient et de ses Proches.

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 l' Abonné /Utilisateur ;
- Informations relatives aux habitudes de vie : si collectées avec l'accord du Patient et lorsque nécessaire de ses Proches et dans la stricte mesure où elles sont nécessaires au diagnostic et aux soins.

Doctolib, en tant que sous traitant, et l'Utilisateur/ Abonné 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 ET SOUS-TRAITANTS ULTÉRIEURS DES DONNÉES :**

- les Acteurs de santé et les professionnels 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 ;
- les Sous-traitants ultérieurs : Se référer à la liste mentionnée à l'article 11 du présent Accord.

Les Documents, Données de santé et Données à caractère personnel contenus sur la Plateforme Doctolib et le Service de logiciel de gestion de cabinet sont strictement confidentiels et restent à l'usage unique de l'Abonné/Utilisateur. Néanmoins, à titre exceptionnel et afin de donner suite à une requête émise par un tribunal ou par toute autorité administrative et/ou judiciaire compétente, Doctolib pourrait être amenée, exceptionnellement, à lever la confidentialité des Documents, Données de santé et Données à caractère personnel sauvegardés.

**DURÉE DE CONSERVATION :**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée 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.

### TRAITEMENT N°5 : MISE À DISPOSITION DU LECTEUR DOCTOLIB

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS :**

1/ Permettre l'envoi du Lecteur Doctolib à l'adresse indiquée par l'Abonné lors de l'Abonnement ;
2/ Permettre au Responsables de traitement d'accéder aux services de la CNAM ;
3/ Permettre la sécurisation des FSE ;
4/ Permettre la création, la gestion et la signature des factures lors de visites médicales au domicile des Patients.
5/ Reporting, debug et statistiques.

**PERSONNES CONCERNÉES :**

1/Patients et bénéficiaires inscrits sur la carte vitale.
2/Abonnés/Utilisateurs du Lecteur Doctolib.

**DONNÉES CONCERNÉES :**

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

- les données de contact de l'Abonné/Utilisateur : 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 ;

**DESTINATAIRES DES DONNÉES :**

- 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 :**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée 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.

### TRAITEMENT N°6 : MISE À DISPOSITION D'UN SERVICE DE MESSAGERIE

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS :**

1/ Faciliter la communication entre Acteurs de santé en proposant un canal d'échange sécurisé par messagerie instantanée ;
2/ Permettre l'échange de Documents et de données pouvant inclure des Données à caractère personnel relatives aux Patients ;
3/ Permettre aux Utilisateurs du Service de Messagerie de bloquer ou débloquer un autre Utilisateur ;
4/ Réaliser des actes de télé-expertise ;
5/Reporting, debug et statistiques.

**BASE LÉGALE**

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.

A titre indicatif, l'intérêt légitime pourrait constituer la base légale. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

Dans le cas où le Responsable de traitement communique les Données de base patient à un Acteur de santé qui ne fait pas partie de l'équipe de soin du Patient donné, il doit au préalable requérir le consentement de ce Patient. Par ailleurs, dans le cadre de la réalisation d'actes de télé-expertise, le Responsable de Traitement est tenu d'informer le Patient sur les conditions de réalisation de la télé-expertise, et de recueillir un consentement exprès et éclairé sur la base de ces informations.

**PERSONNES CONCERNÉES :**

1/ Patients appartenant à la base patient des Acteurs de santé utilisant le Service de Messagerie Doctolib.
2/ Acteurs de santé ou Assistants ayant ou non un Compte Utilisateur Doctolib.

**DONNÉES CONCERNÉES :**

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 ;
- Numéro de sécurité sociale pour les besoins de la prise en charge des actes de télé-expertise, et matricule INS lorsque celui-ci est disponible et qualifié ;
- Les logs d'utilisation et de connexion qui rendent compte des "actions métiers" des Utilisateurs au sein de la Plateforme Doctolib ainsi que les logs techniques qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur/Abonné afin que Doctolib puisse assurer le fonctionnement et l'accès aux fonctionnalités demandées.

**DESTINATAIRES DES DONNÉES :**

- 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 :**

Sauf instruction particulière de la part du Responsable de traitement, Doctolib appliquera les durées de conservations telles que recommandées par la CNIL ou la législation applicable.

En l'absence d'instruction contraire de la part du Responsable de traitement pour une conversation particulière, l'historique des conversations, incluant les Documents, est conservé 6 mois à compter de la date de leur envoi, et l'historique des demandes de télé-expertise est conservé 2 ans à compter de la date de leur envoi.

## TRAITEMENT N°7 : GESTION DES DOCUMENTS ET DES FORMULAIRES

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS**

1/ Permettre la création et le formatage de Documents ;
2/ Permettre (i) l'envoi de Document par le Patient, par un Proche autorisé, ou par le Responsable de traitement et (ii) la réception de Document par le Patient, par un Proche autorisé, le Responsable de traitement et/ou tout autre destinataire choisi par le Responsable de traitement ;3/ Permettre (i) au Responsable de traitement 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 par le Responsable de traitement ;
4/ Permettre la Signature Électronique Simple des Documents ;
5/ Reporting, debug et statistiques.

**BASE LÉGALE DU TRAITEMENT**

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement. Afin d'aider le Responsable 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. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

En ce qui concerne les documents et informations demandés au Patient ou à un Proche autorisé en préparation d'un rendez-vous, il est rappelé au Responsable de Traitement qu'il est 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.

**PERSONNES CONCERNÉES**

1/ Patients ;
2/ Acteurs de santé ayant ou non un Compte Utilisateur Doctolib.

**DONNÉES CONCERNÉES**

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 ;
- Les logs d'utilisation et de connexion qui rendent compte des "actions métiers" des Utilisateurs au sein de la Plateforme Doctolib ainsi que les logs techniques qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur/Abonné afin que Doctolib puisse assurer le fonctionnement et l'accès aux fonctionnalités demandées.

**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**

Sauf instruction particulière du Responsable de traitement, 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, le Responsable de traitement autorise 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 le Responsable de traitement, 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".

## TRAITEMENT N°8 : MISE À DISPOSITION D'UN SERVICE DE TRANSMISSION DE PRESCRIPTIONS

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS :**

1/ 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 ;

2/ Permettre aux Utilisateurs du Service de Transmission de Prescriptions de renseigner et être renseignés sur le statut de délivrance des Prescriptions ;

3/Reporting, debug et statistiques.

**BASE LÉGALE**

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.

A titre indicatif, l'intérêt légitime pourrait constituer la base légale. Le Responsable de Traitement est libre de mentionner à Doctolib une autre base légale.

**PERSONNES CONCERNÉES :**

1/ Patients consultant les Acteurs de santé utilisant le Service de Transmission de Prescriptions Doctolib ;

2/ Acteurs de santé ayant ou non un Compte Utilisateur Doctolib.

**DONNÉES CONCERNÉES :**

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 ;
- Les logs d'utilisation et de connexion qui rendent compte des "actions métiers" des Utilisateurs Freemium au sein de la Plateforme Doctolib ainsi que les logs techniques qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur Freemium afin que Doctolib puisse assurer le fonctionnement et l'accès aux fonctionnalités demandées.

**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 :**

Sauf instruction particulière de la part du Responsable de traitement, Doctolib appliquera les durées de conservation telles que recommandées par la CNIL ou la législation applicable.

En l'absence d'instruction contraire de la part du Responsable de traitement 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.

## TRAITEMENT N°9 : AMÉLIORATION DES SERVICES, PRODUCTION DE STATISTIQUES ET ANONYMISATION DES DONNÉES

**OPÉRATIONS DE TRAITEMENT :**

Les Services Doctolib impliquent la collecte, l'enregistrement, l'organisation, la conservation, l'extraction, la consultation et l'utilisation, la communication par transmission, l'anonymisation et l'effacement des Données à caractère personnel listées ci-dessous.

**FINALITÉS DU TRAITEMENT :**

- Amélioration des Services ;

- Production de statistiques pour le compte de l'Utilisateur/Abonné ;
- Anonymisation des données.

**BASE LÉGALE DU TRAITEMENT** :

Il appartient au Responsable de traitement de déterminer cette base légale avant toute opération de Traitement.

**PERSONNES CONCERNÉES :**

Abonné et Utilisateur tels que définis dans le Contrat.

**TYPES DE DONNEES A CARACTERE PERSONNEL** :

Dans un souci de minimisation des Données à caractère personnel traitées, le Responsable de traitement doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle.

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

- **Informations relatives à l'Acteur de santé**: genre, adresse postale (ville) ;
- **Données professionnelles de l'Acteur de santé :** spécialité, motifs de consultation disponibles, heure d'ouverture et de fermeture, particularités liées au lieu de consultation ;
- Les **logs d'utilisation et de connexion** qui rendent compte des "actions métiers" des Utilisateurs au sein de la Plateforme Doctolib ainsi que les **logs techniques** qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par l'Utilisateur/Abonné afin que Doctolib puisse assurer le fonctionnement et l'accès aux fonctionnalités demandées ;
- **Informations relatives au Patient ou au Proche :** Genre, date de naissance (mois / année), lieu de naissance, adresse postale (ville de résidence) ;
- **Données d'assurance** : statut d'assuré, 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,
- Statut du rendez-vous ;
- **Données de santé** : date/heure et lieu du rendez-vous, spécialité du médecin et nature de la consultation ;
- **Le flux vidéo** permettant la vidéo transmission entre le Patient et l'Acteur de santé lors de la Téléconsultation ;
- **Information de session de Téléconsultation** : erreur & bug, heure de début et de fin de la Téléconsultation, débit vidéo et sonore, information concernant l'état des Équipements utilisés pour la Téléconsultation (niveau de batterie, accès caméra et micro), retour d'information sur la Téléconsultation.

Sauf instruction particulière de la part du Responsable de traitement, Doctolib traite toutes les Données à caractère personnel mentionnées ci-dessus afin de fournir le Service, objet du Contrat.

Ces données sont susceptibles d'être utilisées pour la création de statistiques et de faire l'objet d'une anonymisation.

**DESTINATAIRES ET SOUS TRAITANTS ULTÉRIEURS:**

Se référer à la liste mentionnée à l'article 11 du présent Accord.

**DURÉE DE CONSERVATION:**

Une durée de conservation précise des données doit être fixée par le Responsable de traitement et communiquée à Doctolib.
A défaut d'une telle instruction de la part du Responsable de traitement, Doctolib appliquera les durées de conservations telles que recommandées par la CNIL ou la législation applicable.

# ANNEXE 2 : MESURES TECHNIQUES ET ORGANISATIONNELLES

## Annexe 2- A : Mesures techniques et organisationnelles standard

***[Note : cette annexe 2-A est applicable par défaut (hors cas où un Connecteur entre la Plateforme et les systèmes d'informations tiers est mis en place - ce cas est régi par l'annexe 2-B. Pour plus de précisions sur l'annexe applicable, se référer au Contrat d'Abonnement.]***

**SÉCURITÉ DU PRODUIT**

- **Vérification** d'identité: 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.

- **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 obtenu via email ou sms.

- **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 login, 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 au bout de 7 jours).
    2. Par code PIN :
        a. Les codes PIN trop 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 tentatives de connexion par mot de passe réussie depuis une nouvelle machine sont notifiées à l'utilisateur par le 2FA.

**SÉCURITÉ DE LA PLATEFORME**

- **Mises à jour de sécurité automatiques** : les correctifs de sécurité sont qualifiés et appliqués automatiquement sur nos composants.

- **Systèmes d'exploitation à jour et renforcés**.

- **Veille en sécurité :** nous surveillons en continu les menaces, vulnérabilités ou vecteurs d'attaques, qu'ils soient connus ou nouveaux.
  Pare-feux et systèmes de filtrage des accès dédiés (proxy, vpn...).
  Protection contre les attaques de déni de service distribuées (DDoS).
  Protection contre les attaques logicielles (WAF).

- **Traçabilité :** nous enregistrons toute action, surveillons et alertons pour tout événement de sécurité.

- **Centres de données sécurisés** : HDS, ISO 27001, Tier 3, sécurité physique forte, personnel sur le site 24 heures sur 24 et 7 jours sur 7.

**DISPONIBILITÉ**

- Toutes les données sont répliquées dans plusieurs centres de données.
- Chaque centre de données possède plusieurs liens réseaux vers l'extérieur.
- Tous les services et composants sont couverts par des procédures de reprise d'activité, le plus souvent automatiques.
- Toute défaillance est détectée automatiquement et provoque une alerte grâce à un système de surveillance

complet de chaque composant technique et de chaque service métier.
- Mise en place d'une politique de sauvegarde et de récupération des données permettant notamment de lutter contre une attaque ransomware sur notre base de données.

**CHIFFREMENT DES DONNÉES**

**Chiffrement des communications :**
- Toutes les données échangées avec et entre les systèmes sont chiffrées grâce aux protocoles TLS.
- Les accès techniques sont réalisés à travers une connexion chiffrée et authentifiée fortement, avec validation systématique par un pair.
- La confidentialité des consultations vidéos réalisées via le service Doctolib est assurée par un chiffrement des flux de bout en bout Patient/Acteur de santé.

**Stockage des données :**
- L'intégralité de nos bases de données est chiffrée au repos.
- Les clés de chiffrement sont chiffrées avec une clé maître créée selon les règles de l'art et sont hébergées chez Atos au sein d'un dispositif matériel sécurisé.
- Les Données de santé inscrites dans le Logiciel de gestion de cabinet ainsi que les Données issues d'une Téléconsultation sont chiffrées de bout-en-bout par l'application Doctolib avec des clés stockées de manière sécurisée sur le matériel des Utilisateurs.
- Les Documents sont protégés par différentes techniques de chiffrement.
- Ces données ne peuvent être visibles que pour l'Utilisateur. Doctolib est toujours en charge du stockage et de la disponibilité des données mais sans pouvoir lire les informations de santé. Aucun acteur et intermédiaire du système d'information ne peut lire ces données.

**CONTRÔLE D'ACCÈS DES EMPLOYÉS**

La politique du moindre accès est appliquée, seuls les accès nécessaires correspondants à la mission de l'employé dans l'entreprise lui sont accordés.

Seul un accès temporaire aux données peut être accordé par l'Utilisateur lui-même à un membre de l'équipe support, si nécessaire et dans le cas d'une investigation.

Seules quelques personnes accréditées et sensibilisées membres de l'équipe infrastructure de Doctolib peuvent éventuellement accéder aux données dans le cas d'une défaillance liée au stockage des données.

**MEILLEURES PRATIQUES DE SÉCURITÉ APPLICATIVE**

**Stockage des mots de passe** : hachés grâce à une fonction de hachage robuste (bcrypt).
**Rate limit** : les services et Utilisateurs sont protégés contre des attaques visant l'épuisement de nos ressources (Déni de Service), des attaques par force brute et la récupération automatisée de nos données grâce à un algorithme intelligent qui contrôle le partage et l'accès aux services et bloque les requêtes automatiques.
**CYCLE DE DÉVELOPPEMENT LOGICIEL SÉCURISÉ (S-SDLC)**

**Sensibilisation, formation à la sécurité :** les développeurs sont formés et sensibilisés aux bonnes pratiques en termes de développement d'application sécurisé.
**Sécurité dès la conception** : chaque nouvelle fonctionnalité dans le produit Doctolib est conçue en collaboration avec les experts sécurité.
**Revue de code source :**
La sécurité du code source de Doctolib est analysée automatiquement à chaque modification.
Des revues manuelles du code source sont effectuées lors de la modification d'un composant sensible.

**Recherche de vulnérabilités :**
**Tests d'intrusion :**
Doctolib mandate régulièrement des entreprises reconnues pour effectuer des tests d'intrusion sur nos applications et plateformes.

**Programme de prime à la vulnérabilité (bug bounty)**:
Les salariés et des chercheurs externes sont récompensés lorsqu'ils identifient une faille de sécurité dans le produit Doctolib.

**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)

## Annexe 2-B Mesures techniques et organisationnelles spécifiques

***[Note : cette annexe 2-B est applicable uniquement dans le cas où un Connecteur a été mis en place pour assurer l'interopérabilité entre la Plateforme et les systèmes d'information tiers. Pour plus de précisions sur l'annexe applicable, se référer au Contrat d'Abonnement.]***

**SÉCURITÉ DU PRODUIT**

- Vérification d'identité: 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.

- 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 obtenu via email ou sms.

- 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 login, 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 au bout de 7 jours).
    2. Par code PIN :
        a. Les codes PIN trop 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 tentatives de connexion par mot de passe réussie depuis une nouvelle machine sont notifiées à l'utilisateur par le 2FA.

**SÉCURITÉ DE LA PLATEFORME**

- Mises à jour de sécurité automatiques : les correctifs de sécurité sont qualifiés et appliqués automatiquement sur nos composants.

- Systèmes d'exploitation à jour et renforcés.

- Veille en sécurité : nous surveillons en continu les menaces, vulnérabilités ou vecteurs d'attaques, qu'ils soient connus ou nouveaux.
  Pare-feux et systèmes de filtrage des accès dédiés (proxy, vpn...).
  Protection contre les attaques de déni de service distribuées (DDoS).
  Protection contre les attaques logicielles (WAF).

- Traçabilité : nous enregistrons toute action, surveillons et alertons pour tout événement de sécurité.

- Centres de données sécurisés : HDS, ISO 27001, Tier 3, sécurité physique forte, personnel sur le site 24 heures sur 24 et 7 jours sur 7.

**DISPONIBILITÉ**

- Toutes les données sont répliquées dans plusieurs centres de données.
- Chaque centre de données possède plusieurs liens réseaux vers l'extérieur.
- Tous les services et composants sont couverts par des procédures de reprise d'activité, le plus souvent automatiques.
- Toute défaillance est détectée automatiquement et provoque une alerte grâce à un système de surveillance complet de chaque composant technique et de chaque service métier.
- Mise en place d'une politique de sauvegarde et de récupération des données permettant notamment de lutter contre une attaque ransomware sur notre base de données.

**CHIFFREMENT DES DONNÉES**

**Chiffrement des communications :**

- Toutes les données échangées avec et entre les systèmes sont chiffrées grâce aux protocoles TLS.

- Les accès techniques sont réalisés à travers une connexion chiffrée et authentifiée fortement, avec validation systématique par un pair.
- La confidentialité des consultations vidéos réalisées via le service Doctolib est assurée par un chiffrement des flux de bout en bout Patient/Acteur de santé.

**Interopérabilité inter-systèmes**

- En la présence d'un Connecteur entre les systèmes d'informations de l'Abonné/Utilisateur et les systèmes d'informations de Doctolib, afin de garantir l'interopérabilité des systèmes, les flux et Documents transmis via les APIs font l'objet d'un déchiffrement par l'application Doctolib avant transmission.
- L'Abonné/Utilisateur se verra transmettre une paire de clés secrètes (une clé principale et une clé de secours) de la part de Doctolib afin de permettre à son Système d'Information de s'authentifier auprès du système Doctolib. L'Abonné/Utilisateur est responsable de la confidentialité de cette paire de clés et d'assurer sa protection selon les meilleures pratiques, notamment son chiffrement au repos des clés et le contrôle d'accès.
- L'Abonné/Utilisateur devra s'assurer que son système d'information est capable de s'authentifier automatiquement avec la seconde clé secrète si la clé principale est refusée par Doctolib.
- En cas de suspicion de compromission d'une des clés secrètes, l'Abonné/Utilisateur devra prévenir Doctolib sans délai, afin d'enclencher une procédure de renouvellement des clés.
- L'Abonné/Utilisateur se verra proposer par Doctolib de restreindre l'utilisation des clés secrètes à un ensemble d'adresses IP fixes du système d'information de l'Abonné/Utilisateur. Dans le cas où L'Abonné/Utilisateur choisirait de ne pas restreindre l'utilisation des clés secrètes à ses adresses IP fixes, il est convenu que l'Abonné/Utilisateur comprend, qu'en cas de compromission d'une de ses clés, Doctolib ne pourra être tenu responsable d'une utilisation frauduleuse des dites clés par une personne ou un système non habilité.

**Stockage des données :**

- L'intégralité de nos bases de données est chiffrée au repos.
- Les clés de chiffrement sont chiffrées avec une clé maître créée selon les règles de l'art et sont hébergées chez Atos au sein d'un dispositif matériel sécurisé.
- Les Données de santé inscrites dans le Logiciel de gestion de cabinet ainsi que les Données issues d'une Téléconsultation sont chiffrées de bout-en-bout par l'application Doctolib avec des clés stockées de manière sécurisée sur le matériel des Utilisateurs.
- Ces données ne peuvent être visibles que pour l'Utilisateur. Doctolib est toujours en charge du stockage et de la disponibilité des données mais sans pouvoir lire les informations de santé. Aucun acteur et intermédiaire du système d'information ne peut lire ces données.

**CONTRÔLE D'ACCÈS DES EMPLOYÉS**

La politique du moindre accès est appliquée, seuls les accès nécessaires correspondants à la mission de l'employé dans l'entreprise lui sont accordés.

Seul un accès temporaire aux données peut être accordé par l'Utilisateur lui-même à un membre de l'équipe support, si nécessaire et dans le cas d'une investigation.

Seules quelques personnes accréditées et sensibilisées membres de l'équipe infrastructure de Doctolib peuvent éventuellement accéder aux données dans le cas d'une défaillance liée au stockage des données.

**MEILLEURES PRATIQUES DE SÉCURITÉ APPLICATIVE**

Stockage des mots de passe : hachés grâce à une fonction de hachage robuste (bcrypt).
Rate limit : les services et Utilisateurs sont protégés contre des attaques visant l'épuisement de nos ressources (Déni de Service), des attaques par force brute et la récupération automatisée de nos données grâce à un algorithme intelligent qui contrôle le partage et l'accès aux services et bloque les requêtes automatiques.

**CYCLE DE DÉVELOPPEMENT LOGICIEL SÉCURISÉ (S-SDLC)**

Sensibilisation, formation à la sécurité : les développeurs sont formés et sensibilisés aux bonnes pratiques en termes de développement d'application sécurisé.
Sécurité dès la conception : chaque nouvelle fonctionnalité dans le produit Doctolib est conçue en collaboration avec les experts sécurité.
Revue de code source :
La sécurité du code source de Doctolib est analysée automatiquement à chaque modification.
Des revues manuelles du code source sont effectuées lors de la modification d'un composant sensible.

Recherche de vulnérabilités :
Tests d'intrusion :
Doctolib mandate régulièrement des entreprises reconnues pour effectuer des tests d'intrusion sur nos applications et plateformes.

Programme de prime à la vulnérabilité (bug bounty):
Les salariés et des chercheurs externes sont récompensés lorsqu'ils identifient une faille de sécurité dans le produit Doctolib.

**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 signature d'un engagement de confidentialité, 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)