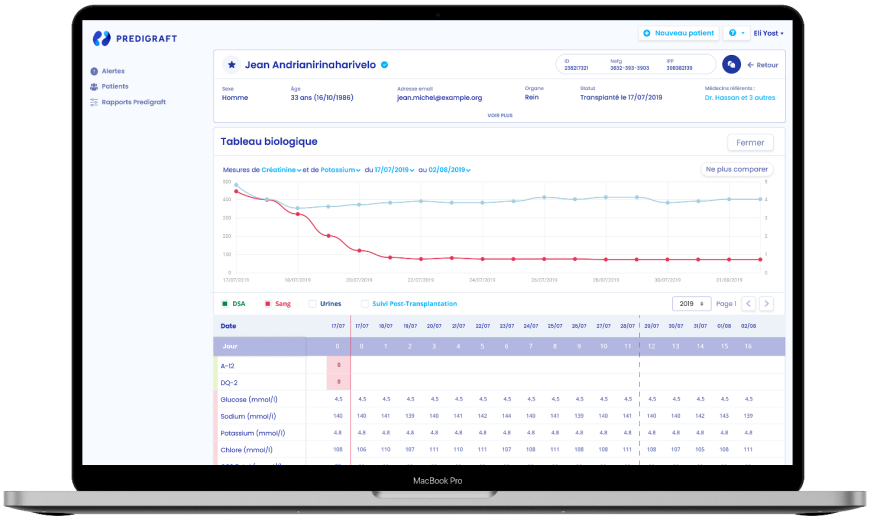
PREDIGRAFT

Politique de confidentialité de la solution Predigraft



CIBILTECH

Table des matières

1. Objet de la présente politique

CIBILTECH souhaite vous informer par l'intermédiaire de la présente politique de la manière dont sont traitées et protégées les données à caractère personnel traitées par la solution Predigraft.

Pour plus d'informations sur l'utilisation de la solution Predigraft, veuillez-vous référer aux Conditions Générales d'Utilisation.

2. Définitions

Consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Donnée personnelle ou donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Donnée de santé : les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne. Cela comprend :

- Les informations relatives à une personne physique collectées lors de son inscription sur la solution,
- Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques,
- Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

Responsable de traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ;

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le dispositif médical est appelé Predigraft et est composé de deux interfaces :

- Une interface pour les patients qui est accessible à partir d'une tablette ou d'un smartphone mobile (disposant d'un navigateur web). Elle permet aux patients d'échanger avec leur professionnel de santé.
- Une interface pour les professionnels de santé qui est accessible à partir d'un ordinateur (portable ou fixe), d'une tablette ou d'un smartphone mobile disposant d'un navigateur Web. Elle permet aux professionnels de santé de suivre leurs patients après la greffe.

La solution Predigraft est à la fois une plateforme d'échanges de données entre les professionnels de santé et les patients et aussi un dispositif médical d'aide à la décision.

3. L'établissement de santé est responsable de traitement

L'établissement de santé propose à ses patients d'utiliser la solution Predigraft en accès web ou sur une application mobile dans le cadre de l'amélioration du suivi médical de patients ayant reçu une greffe de rein.

L'établissement de santé a le statut de responsable du traitement des données personnelles au sens de la Réglementation Générale sur la Protection des Données (RGPD).

4. L'éditeur du logiciel, CIBILTECH, est sous-traitant de données personnelles, pour le compte du responsable de traitement

CIBILTECH est l'éditeur de la solution Predigraft.

À ce titre, CIBILTECH met à disposition et assure le maintien en condition opérationnelle de la solution Predigraft. CIBILTECH a donc le statut de sous-traitant au sens de la réglementation sur la protection des données[1].

CIBILTECH est une Société par Actions Simplifiée, immatriculée au RCS sous le numéro 848 185 765 et dont le siège social est situé au 130, rue de Lourmel 75015 PARIS (ci-devant et ci-après « CIBILTECH »).

5. Comment sont collectées les données personnelles ?

Les données relatives au patient sont collectées lors de la création des comptes dans la solution Predigraft et tout au long de son utilisation lorsque de nouvelles variables ou nouveaux documents y sont intégrés par le patient lui-même.

Ensuite ces données viennent s'ajouter aux autres données relatives au patient et qui sont utilisées par les professionnels de santé sans le cadre de son suivi médical.

[1] Dont le RGPD : (RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

6. Quelles sont les finalités de la collecte de vos données personnelles et les bases légales associées ?

L'objectif principal de la solution Predigraft est d'améliorer la qualité des soins apportés aux patients ayant reçu une greffe de rein. Pour atteindre cet objectif, des traitements de données personnelles sont réalisés.

Traitements de données personnelles réalisés par l'établissement de santé

Les traitements réalisés dans le cadre de la solution destinée aux médecins répondent aux finalités suivantes :

- Échanger à distance avec les patients ;
- Permettre la transmission de résultats d'analyse ou examens issus de laboratoires d'analyses, sous forme de PDF ou de photographie. Ces documents sont transmis au dossier patient du médecin et ce dernier pourra les retrouver en ouvrant son dossier patient dans l'interface dédiée au professionnel de santé ;
- Fournir aux professionnels de santé les informations sur des paramètres biologiques, cliniques et histologiques du patient ;
- Permettre aux professionnels de santé de consulter les documents médicaux et d'utiliser certaines données nécessaires à la création d'une évaluation iBox concernant la probabilité de survie du greffon du patient ;
- Présenter une représentation graphique des informations transmises ;
- Mettre à disposition du patient du contenu d'accompagnement thérapeutique sous différentes formes (vidéos, articles…).

Bases légales des traitements

Conformément à la Réglementation sur la Protection des Données Personnelles, tout traitement de données doit s'appuyer sur une base légale bien identifiée.

Les traitements de données personnelles des patients dans le cadre du suivi médical s'appuient sur l'intérêt public car les établissements de santé assurent le diagnostic, la surveillance et le traitement des malades et mènent des actions de prévention et d'éducation à la santé, conformément à l'article L6111-1 du Code de Santé Publique.

Les traitements des données personnelles des patients, en particulier des données de santé, réalisés spécifiquement dans le cadre de la solution Predigraft dédiée aux patients relèvent quant à eux du consentement du patient, qui est demandé dès sa première connexion.

Le patient peut donc retirer à tout moment son consentement au traitement de ses données personnelles dans le cadre de la solution et cela entraînera la clôture de son compte.

En revanche, le retrait de ce consentement n'empêchera pas le suivi médical réalisé par l'établissement de santé via l'interface dédiée au professionnel de santé car cet outil restera utilisé par les professionnels de santé.

Traitements de données réalisés par CIBILTECH, l'éditeur de la solution

Les traitements des données des patients reposent sur leur consentement mais il faut savoir que CIBILTECH s'appuie aussi sur l'exécution du contrat de licence et maintenance conclu avec l'établissement de santé pour :

- Fournir des services de maintenance/résoudre des bogues ou des incidents,
- Gérer l'hébergement et la sauvegarde des données,
- Faciliter l'import des données de l'hôpital vers la solution,
- Assurer la sécurité grâce à l'authentification, aux journaux de connexion et à la gestion des incidents,
- Effacer les données à la demande du client ou de la personne concernée,
- Simplifier et sécuriser la saisie des données, notamment via l'import de documents contenant des données ainsi que l'extraction de texte.

NB : Lorsqu'un patient accepte de participer au programme ETAPES, ses données font l'objet d'un traitement permettant d'obtenir des métriques qui sont transmises aux différentes institutions en charge de l'évaluation du programme. Cette transmission est une obligation légale. Une précision importante : les métriques transmises ne permettent pas de remonter à l'individu.

7. Quelles données sont traitées et combien de temps sont-elles conservées ?

Catégories de données traitées	Durées de conservation des données
Données obligatoires • Données nécessaires à la création du compte : o Adresse email du patient fournie par le médecin lors de la création du compte patient, o Mot de passe.	Durée de l'utilisation de la solution + 1 mois à partir de la clôture du compte du patient.
• Données relatives aux connexions / actions au cœur du logiciel (logs) : date / heure de connexion, adresse IP, actions réalisées	6 mois glissants

• Données facultatives : Historique des documents transmis (résultats d'analyses, examens).	**Conservation en base active :** Les données sont traitées et donc conservées pendant la durée d'utilisation de la solution tant que la personne a besoin d'être suivie et ne s'oppose pas au traitement de ses données dans Predigraft. **Archivage** : l'archivage des données est réalisé pendant la durée du contrat entre CIBILTECH et l'établissement de santé et ce pendant 10 ans après la fin du suivi afin que l'établissement de santé puisse faire face à d'éventuels contentieux/recours en justice/ enquêtes. NB : Les données du patient seront conservées dans la solution pour permettre l'usage par un autre hôpital le cas échéant (donc conservation au-delà du contrat). Les données suivent le patient.

8. À qui vos données peuvent-elles être transmises ?

Les destinataires internes de CIBILTECH

Par défaut les données ne sont pas accessibles par CIBILTECH. Elles peuvent être rendues accessibles au service maintenance uniquement si l'anomalie à résoudre ne peut pas être traitée sans cet accès. Il s'agit d'opérations très exceptionnelles, encadrées par une procédure stricte, définie en amont, et qui nécessite la présence d'un médecin.

Les prestataires de CIBILTECH (ou sous-traitant au sens de l'article 28 du RGPD)

CIBILTECH fait appel à Coreye-Pictime pour l'hébergement des données d'Predigraft. Il s'agit d'un hébergeur certifié Hébergeur de Données de Santé (HDS).

Pour plus d'informations : https://pictime-groupe.com/certification-hds

CIBILTECH peut faire appel à des sous-traitants pour la gestion de la maintenance de la solution.
Un contrat est mis en place avec tous les sous-traitants et des engagements de confidentialité sont systématiquement signés individuellement par chaque intervenant.

9. Vos données sont-elles transmises hors de l'UE ?

Les données sont hébergées par l'hébergeur de données de santé, Coreye-Pictime, en France.

10. Quels sont mes droits sur mes données personnelles et comment les exercer ?

Conformément à la Loi Informatique et Libertés modifiée et la réglementation européenne sur la protection des données personnelles, vous disposez de droits sur les données vous concernant.

Organisation de la gestion des demandes d'exercice de droits :

CIBILTECH n'est pas habilitée à accéder aux données contenues dans la solution Predigraft, en particulier aux données de santé. Cela l'empêche de répondre à des demandes d'exercice de droits car CIBILTECH ne connaît pas l'identité des personnes dont les données sont traitées.

Les personnes qui souhaitent exercer leurs droits devront donc s'adresser à l'hôpital.

Si CIBILITECH reçoit une demande d'exercice de droit, la demande sera transmise au responsable de traitement concerné, c'est-à-dire à l'hôpital.

Droit d'accès

Vous avez le droit de demander aux administrations, sociétés commerciales ou organismes, quelles informations ils détiennent sur vous dans leurs fichiers. Ce droit d'accès vous permet de vérifier l'exactitude de ces informations et, au besoin, de les faire rectifier ou effacer.

En justifiant de votre identité, vous pouvez interroger le responsable du traitement ou du fichier concerné afin d'obtenir :

- L'intégralité des informations vous concernant,
- L'origine de ces informations,
- Le but du traitement ou du fichier, les destinataires des informations et les éventuels transferts hors de l'Union Européenne.

Vous pouvez exercer vos demandes de droit d'accès auprès de l'hôpital.

Droit de rectification

Vous pouvez demander la rectification des informations inexactes ou incomplètes vous concernant. Ce droit permet d'éviter qu'un organisme n'utilise ou ne diffuse des informations erronées sur vous.

Vous pouvez exercer vos demandes de droit de rectification auprès de l'hôpital.

Droit à l'effacement des données

Vous avez le droit de demander à un organisme l'effacement de données à caractère personnel vous concernant, si au moins une de ces situations correspond à votre cas :

- Vos données sont utilisées à des fins de prospection ;
- Les données ne sont pas ou plus nécessaires au regard des objectifs pour lesquelles elles ont été initialement collectées ou traitées ;
- Vous retirez votre consentement à l'utilisation de vos données ;

- Vos données font l'objet d'un traitement illicite (par exemple, publication de données piratées) ;
- Vos données ont été collectées lorsque vous étiez mineur dans le cadre de la société de l'information (blog, forum, réseau social, site web…) ;
- Vos données doivent être effacées pour respecter une obligation légale ;
- Vous vous êtes opposé au traitement de vos données et le responsable du fichier n'a pas de motif légitime ou impérieux de ne pas donner suite à cette demande.

Toutefois, dans certains cas, ce droit sera écarté car il ne doit pas aller à l'encontre :

- De l'exercice du droit à la liberté d'expression et d'information ;
- Du respect d'une obligation légale ;
- De l'utilisation de vos données si elles concernent un intérêt public dans le domaine de la santé ;
- De leur utilisation à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- De la constatation, de l'exercice ou de la défense de droits en justice.

Vous pouvez exercer vos demandes d'effacement auprès de l'hôpital.

Droit à la limitation du traitement

Le droit à la limitation de vos données est un droit qui complète vos autres droits (rectification, opposition…). Si vous contestez l'exactitude des données utilisées par l'organisme ou que vous vous opposez à ce que vos données soient traitées, la loi autorise l'organisme à procéder à une vérification ou à un examen de votre demande pendant un certain délai. Pendant ce délai, vous avez la possibilité de demander à l'organisme de geler l'utilisation de vos données. Concrètement, il ne devra plus utiliser les données mais devra les conserver.

Inversement, vous pouvez demander directement la limitation de certaines données dans le cas où l'organisme souhaite les effacer. Cela vous permettra de conserver les données par exemple afin d'exercer un droit.

Vous pouvez exercer vos demandes de limitation du traitement auprès de l'hôpital.

Droit d'opposition au traitement

Le droit d'opposition vous permet de vous opposer à ce que vos données soient utilisées par un organisme pour un objectif précis. Vous devez mettre en avant « des raisons tenant à votre situation particulière », sauf en cas de prospection commerciale, à laquelle vous pouvez vous opposer sans motif.

Dans ce cas, l'établissement de santé ne traitera plus les données personnelles, à moins de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Vous pouvez exercer vos demandes d'opposition au traitement auprès de l'hôpital.

Droit à la portabilité de vos données

Vous avez le droit de demander à l'établissement de santé de vous transmettre les données personnelles qui vous concernent et que vous avez fournies. Il devra les fournir ou les transférer à l'établissement de votre choix dans un format structuré, couramment utilisé et lisible par machine.

Ce nouveau droit s'applique si ces trois conditions sont toutes réunies :

- Le droit à la portabilité est limité aux données personnelles fournies par la personne concernée.
- Il ne s'applique que si les données sont traitées de manière automatisée (les fichiers papiers ne sont donc pas concernés) et sur la base du consentement préalable de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée.
- L'exercice du droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers, dont les données se trouveraient dans les données transmises suite à une demande de portabilité.

Les personnes doivent exercer leurs demandes de portabilité auprès de l'hôpital.

Droit de définir le sort de vos données après le décès

Vous avez la possibilité de communiquer à votre établissement de santé des directives relatives à la conservation, à l'effacement et à la communication de vos données personnelles après votre décès.

Vous devrez contacter l'hôpital pour mettre en place ce droit.

Droit d'introduire une réclamation auprès de l'autorité de contrôle (la Commission Nationale Informatique et Libertés)

Vous avez le droit d'introduire une réclamation auprès de la CNIL si vous considérez que le traitement de données à caractère personnel qui vous concerne constitue une violation du Règlement Européen sur la Protection des Données.

11. Quelles mesures de sécurité sont mises en place pour protéger mes données ?

CIBILTECH met en œuvre toutes les mesures techniques et organisationnelles afin d'assurer la sécurité des traitements de données à caractère personnel et leur confidentialité.

CIBILTECH prend toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, afin de préserver la sécurité des données et, notamment, d'empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Parmi les mesures de sécurité mises en place autour de la solution Predigraft, on trouve notamment :

- La sensibilisation de tous les collaborateurs à la protection des données personnelles et à leur sécurité ;
- La protection physique des locaux de CIBILTECH et des locaux où les données sont hébergées (niveau de sécurité élevé des Datacenters) ;
- Des procédés d'authentification conformes à l'état de l'art ;
- Une gestion rigoureuse des accès et des habilitations ;
- La journalisation des connexions ;

- Le chiffrement de certaines données ;
- Le cloisonnement des environnements de développement, test/qualification, production et démonstration ;
- La gestion de l'hébergement des données réalisées par un hébergeur certifié HDS ;
- La gestion de la continuité de services.

Comment nous contacter – Coordonnées du Délégué à la Protection des données ?

Si l'utilisateur a des questions ou des réclamations concernant le respect par CIBILTECH de la présente politique, ou si l'utilisateur souhaite faire part à CIBILTECH de recommandations ou des commentaires visant à améliorer la qualité de la présente politique, l'utilisateur peut contacter CIBILTECH par écrit à l'adresse suivante :

- Par voie postale :

Délégué à la Protection des Données

CIBILTECH

130 rue de Lourmel

75015 Paris, France

- Par email :

privacy@cibiltech.com