OBJET

Ce document est la politique interne de protection des données à caractère personnel qui devra a minima être annexée à la Charte d'usage du système d'information.

RESUME

La politique de protection des données existe pour assurer un niveau de sécurité adéquat en termes de confidentialité, de disponibilité, d'intégrité des ressources en information et en données à caractère personnel de l'ensemble des établissements vis-à-vis de toutes les menaces qui pourraient l'affecter. L'organisme définit, applique, opère, surveille, réalise des revues, maintient, améliore le processus, les mesures relatifs au traitement des données et à la sécurité de l'information en se basant sur une approche des risques.

SOMMAIRE

Article 1. INTRODUCTION

Le présent document constitue la politique de protection des données à caractère personnel mise en œuvre par l'ensemble des établissements ALMAVIVA-SANTE dans le cadre de ses activités. La protection des données à caractère personnel fait partie de leurs valeurs essentielles.

Cette Politique de protection des données à caractère personnel a pour objet de fournir aux collaborateurs les informations importantes sur la manière de traiter les données à caractère personnel, et sur la manière dont les personnes concernées peuvent exercer leurs droits. Elle vise également à répondre aux exigences de la nouvelle réglementation relative à la protection des données à caractère personnel (Règlement n°2016/679 dit « RGPD »).

La présente politique formalisée de protection des données à caractère personnel est accessible et disponible en interne auprès des collaborateurs via l'intranet, l'affichage, ou le site internet de l'établissement.

Cette politique sera renouvelée à chaque nouvelle désignation de DPO et à défaut tous les trois ans.

Article 2. LA COLLECTE DES DONNEES

Dans un souci de transparence, les établissements prennent soins d'informer ses clients, salariés et partenaires économiques de chacun des traitements qui les concernent.

Les délégués à la protection des données se tiennent disponibles à l'adresse mail suivante pour apporter toute précision nécessaire concernant cette politique de protection des données à caractère personnel : dpo.groupe@almaviva-sante.com.

La collecte de données à caractère personnel a notamment pour objectif une gestion optimale des diverses relations avec les clients, les salariés et les partenaires économiques.

Article 3. LES FINALITES DES TRAITEMENTS

Les établissements de santé sont amenés à collecter et traiter des données de type administratifs, social et médical ; en relation avec leurs finalités ; selon l'article L6111-1 du code de la santé publique :

- Assurer le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes ;
- Délivrer les soins avec hébergement, sous forme ambulatoire ou à domicile ;
- Participer à la coordination des soins en relation avec les membres des professions de santé exerçant en pratique de ville et les établissements et services médico-sociaux ;
- Participer à la mise en œuvre de la politique de santé publique et des dispositifs de vigilance destinés à garantir la sécurité sanitaire ;
- Mener, en leur sein, une réflexion sur l'éthique liée à l'accueil et la prise en charge médicalisée.

Spécifiquement le service des ressources humaines, en respect du code du travail se consacre à :

- La gestion des candidatures et du recrutement
- La gestion du personnel
- La formation
- Les relations sociales et syndicales
- La gestion des carrières et des compétences
- Les systèmes d'informations des ressources humaines
- La gestion de la paie

- La gestion des intérimaires et des stagiaires
- L'organisation du travail

Ainsi, chaque traitement de données mis en œuvre dispose d'une finalité légitime, déterminée et explicite dans le cadre de ses activités, traduite dans le registre des activités de traitement de chacun des établissements.

Les grandes catégories de traitements recensés sont :

- Gestion des Patients ;
- Qualité et Gestion des Risques ;
- Gestion des Ressources Humaines ;
- Sécurité des biens, des personnes et du système d'information ;
- Communication.

Article 4. CATEGORIES DE DONNEES A CARACTERE PERSONNEL TRAITEES

La notion de « *données à caractère personnel* » désigne toute information se rapportant à une personne physique identifiée ou identifiable. Il est précisé que les données relatives aux entités, personnes morales, sociétés (à l'exclusion des personnes physiques membres/collaborateurs/salariés/dirigeants de ces entités) ne sont pas des données à caractère personnel.

Les établissements sont susceptibles selon les cas de traiter des données à caractère personnel :

- Relatives à l'identité des personnes (dont la civilité, nom, prénoms, date de naissance) ;
- Relatives aux moyens de contacter les personnes (telles que l'adresse postale professionnelle et le cas échéant personnelle, le numéro de téléphone fixe et/ou mobile professionnel et le cas échéant personnel, le numéro de télécopie, l'adresse email professionnelle et le cas échéant personnelle) ;
- Nécessaires pour le traitement du service demandé ou de toute autre demande.

Les établissements de santé sont susceptibles selon les cas de traiter les données à caractère personnel suivantes :

- Données d'identification ;
- Données relatives à la vie personnelle (ex : mariage) ;
- Données relatives à la vie professionnelle (ex : formation) ;
- Informations d'ordre économique et financière (ex : RIB) ;
- Données de connexion (ex : création code d'accès logiciel) ;
- Données relatives à la localisation (ex : GPS).

Le cas échéant, si la finalité le légitime, des données sensibles telles que :

- L'origine raciale ou ethnique (ex : formulaire soin) ;
- Les convictions religieuses (ex : directive anticipée) ;
- Les données génétiques ;
- Les données biométriques ;
- Les données de santé ;
- Vie et orientation sexuelle (ex : formulaire don du sang) ;
- Numéro d'identifiant national unique.

Article 5. LA PERTINENCE DES DONNEES

Les établissements collectent et traitent les données à caractère personnel de manière loyale, licite et transparente.

Pour chacun des traitements mis en œuvre, les établissements s'engagent à ne collecter et n'exploiter que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Ils veillent par ailleurs à ce que les données soient exactes, si nécessaire, mises à jour et, à mettre en œuvre des procédés pour permettre l'effacement ou la rectification des données inexactes de manière à ce qu'elles ne deviennent pas obsolètes.

Article 6. LA CONSERVATION LIMITEE DES DONNEES

Les établissements font en sorte que les données soient conservées sous une forme permettant l'identification des personnes concernées uniquement pendant la durée nécessaire au regard des finalités pour lesquelles elles sont traitées.

Nous conservons les données que vous nous avez transmises dans le cadre des traitements liés à la gestion des contrats passés ainsi que pendant les durées légales applicables après la fin des contrats.

Article 7. COOKIES

Le site internet des établissements utilise des « *cookies* » (fichier de taille limité, généralement constitué de lettres et de chiffres, envoyé par le serveur internet au fichier cookie du navigateur situé sur le disque dur de votre ordinateur) afin de permettre la navigation.

Ces « *cookies* » ont pour finalité exclusive de permettre ou de faciliter la communication par voie électronique. Ils sont nécessaires à la fourniture du service de communication en ligne.

Article 8. TRANSMISSION DES DONNEES

Nous ne transmettons par principe les données à caractère personnel à aucun tiers autre que ceux mentionnés ci-après, sauf demande dans le cadre de l'exercice des droits couverts par le 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 ou dans le strict objectif d'atteindre les finalités pour lesquelles les données ont été collectées, et toujours dans le respect des règles de confidentialité.

La transmission de données à caractère personnel ne peut se faire qu'aux catégories de destinataires suivantes :

- Membres et personnels de l'établissement : les données à caractère personnel sont transmises aux membres et personnels qui ont besoin de les traiter pour les finalités rappelées précédemment.
- Prestataires techniques et informatiques en charge de la gestion du réseau informatique et du site internet : le réseau informatique, le site internet et les archives sont gérés et hébergés par des prestataires, notamment informatiques. Les données à caractère personnel peuvent être traitées, stockées par ces prestataires.

- Sous-traitant : maintenance des logiciels administrés par les prestataires dédiés ou leurs sous-traitants dans le cadre de l'exécution du contrat.
- Organismes d'état, de tutelle, de contrôle à des fins d'obligations légales. (URSAFF, CPAM, …).
- Mutuelles.

En tout état de cause, les établissements s'engagent à ne pas céder les données à caractère personnel à des tiers qui auraient pour activité ou finalité l'acquisition de nouveaux prospects en vue d'envoi de prospections commerciales.

Les établissements peuvent toutefois être amenés à devoir communiquer les données à caractère personnel pour se conformer à une obligation légale, à la demande d'une autorité administrative ou judiciaire qui en ferait la demande ou pour l'exercice d'un intérêt légitime.

Article 9. MESURES DE SECURITE

Une importance particulière est accordée à la sécurité des données à caractère personnel.

Des mesures techniques et organisationnelles appropriées sont mises en œuvre pour que les données soient traitées de façon à garantir leur protection contre la perte, la destruction ou les dégâts d'origine accidentelle qui pourraient porter atteinte à leur confidentialité ou à leur intégrité.

Lors de l'élaboration et de la conception, ou lors de la sélection et de l'utilisation des différents outils qui permettent le traitement des données à caractère personnel, le responsable de traitement s'assure, le cas échéant auprès des éditeurs de tels outils, qu'ils permettent d'assurer un niveau de protection optimal des données traitées.

Les établissements mettent ainsi en œuvre des mesures qui respectent les principes de protection dès la conception et de protection par défaut des données traitées prônés par le RGDP. A ce titre, recourir à des techniques d'anonymisation ou de chiffrement des données lorsque cela s'avère possible et/ou nécessaire.

Lorsqu'il y a recours à un prestataire, les établissements ne lui communique des données à caractère personnel qu'après lui avoir imposé le respect de ses propres principes en matière de sécurité.

Description des mesures de sécurité mises en œuvre

Techniques :

- Chiffrement des données : procédés cryptographiques permettant de chiffrer les données empêchant un utilisateur tiers non autorisé de capter les données ainsi chiffrées. Seul un mécanisme de clé de déchiffrement permet d'accéder au contenu.
- Sauvegarde : des moyens de sauvegarde avec des processus de restauration de données sont mis en place afin de sécuriser les contenus et assurer la pérennité des données en cas de panne, ou perte accidentelle ou non, de contenu partiel ou total.
- Résilience : des moyens techniques (onduleur ou équivalent) adaptés sont mis en œuvre afin d'assurer le fonctionnement des systèmes en cas de panne ou de sollicitation extrême.
- Protection contre les cyberattaques : des moyens de protections dimensionnés (antivirus, firewall, Watchgard, VPN, …) sont en place et mis à jour régulièrement afin de lutter contre les menaces de cybercriminalité.

Organisationnelles :

L'ensemble des locaux contenant des données à caractère personnel ou des moyens de lecture automatisés sont sécurisés. Le cas échéant, un contrôle d'accès est mis en place. Les locaux sont

fermés et accessibles aux seules personnes autorisées. Les documents papiers contenant des données à caractère personnel sont tenus sous clés, les locaux sensibles (ex : les salles serveurs) disposent de systèmes de protection adaptés contre les incendies, les inondations, la foudre et les catastrophes naturelles.

Article 10. RESPECT DES DROITS DES PERSONNES CONCERNEES

Dans la cadre de la mise en œuvre de ces traitements, les établissements informent les personnes concernées de la base légale et de la finalité des traitements portant sur leurs données à caractère personnel, des destinataires de ces traitements, de la durée de conservation des informations collectées ainsi que de leurs droits.

Lorsqu'ils s'appliquent, les moyens nécessaires pour assurer aux personnes concernées sont mis en œuvre :

- Le droit à l'information ;
- Le recueil du consentement (lorsqu'il s'applique) ;
- Le droit d'accès ;
- Le droit de rectification ;
- Le droit de suppression (droit à l'oubli) ;
- Le droit à la portabilité des données à caractère personnel (lorsqu'il s'applique) ;
- Le droit à la limitation du traitement ;
- Le droit d'opposition ;
- Le droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés,
- Le droit de définir des directives relatives à la conservation, à l'effacement et à la communication des données à caractère personnel après la mort.

Les données peuvent être rectifiées, complétées, mises à jour, verrouillées ou effacées lorsqu'elles sont inexactes, incomplètes, équivoques, périmées, ou lorsque leur collecte, utilisation, communication ou conservation est interdite.

Les personnes concernées pourront faire exercice de leurs droits dans le respect du RGPD et des autres règlements encadrant le droit à certaines données et notamment le code de santé publique, le code du travail, le code de sécurité social, le code de l'action sociale et des familles et la convention collective de l'hospitalisation privé ; auprès de leur responsable du traitement ou de leur délégué à la protection des données.

Article 11. NOUS CONTACTER POUR FAIRE VALOIR VOS DROITS

Les demandes d'exercice de droits prévus par le RGPD s'effectuent, sauf demandes contraires, par voie électronique à l'adresse suivante : dpo.groupe@almaviva-sante.com.

Ces demandes peuvent également s'effectuer auprès du **DPO en région Ile de France** à l'adresse suivante : ALMAVIVA SANTE- Clinique Arago 187 Rue Raymond Losserand – 75014 Paris, ou dpo.idf.groupe@almaviva-sante.com.

Auprès du **DPO en région SUD** à l'adresse suivante : ALMAVIVA SANTE- Clinique Chantecler 240 Avenue des Poilus – 13012 Marseille, ou dpo.sud.groupe@almaviva-sante.com.

Et ce, dans le respect des conditions et délais impartis par la réglementation applicable (article 12 RGPD). Les établissements informent toute personne concernée qui souhaiterait exercer ses droits en cas d'impossibilité de donner suite à sa demande.

Article 12. POLITIQUES ASSOCIEES

- ALMA-ENR.RGPD.007 Charte d'usage du système d'information ;
- ALMA-ENR.RGPD.018 Gouvernance RGPD ;
- ALMA-PRC.COM.005 Politique de Communication.