Notice de Protection des données personnelles

1°) Collecte des données personnelles

DYOMEDEA recueille auprès de ses patients des données personnelles indispensables à la bonne exécution des analyses en respect des nombreux textes légaux ou obligations réglementaires applicables à l'activité de laboratoire d'analyses médicales et des recommandations de la CNIL auxquelles vient s'ajouter maintenant le Règlement Européen de Protection des Données (RGPD).

En accord avec les exigences répertoriées dans le Code de Conduite élaboré par la profession pour sa conformité au RGPD, DYOMEDEA s'engage à respecter :

- le principe de minimisation et d'exactitude en recueillant des données personnelles adéquates, exactes et seulement celles qui sont nécessaires à la finalité de la mission de laboratoire de biologie médicale.

- le principe de limitation de la conservation des données dans un environnement de confidentialité, de sécurité, pour une durée déterminée conforme à la législation en vigueur et variable selon la nature des données.

- le principe de suppression des données au delà du temps obligatoire de conservation

2°) Droits des patients

DYOMEDEA s'engage à respecter les différents droits que les patients peuvent exercer :

- le droit d'information à dispenser au patient par le laboratoire au préalable de l'étape de recueil, sur la nature des données collectées, la finalité de leur utilisation ainsi que celle des échantillons biologiques prélevés

- le droit d'accès sur demande du patient à ses données personnelles et à la communication du contenu du recueil effectué

- le droit de rectification en cas d'inexactitude ou de donnée erronée

- le droit à l'effacement si la nature des données recueillies est jugée sans rapport avec la finalité de leur utilisation ou si elles ne sont plus nécessaires à cette finalité.

- le droit à la limitation de l'utilisation des données lors de conditions particulières (juridiques, protection de mineurs, sécurité publique)

- le droit à la portabilité des données, le patient pouvant récupérer ses données pour nécessité de transfert à un tiers (autre laboratoire par exemple)

- le droit d'opposition du patient au traitement de ses données pour motif légitime (si besoin de confidentialité vis à vis d'un tiers par exemple) avec respect de son exigence de mise en œuvre d'une pseudonymisation de ses données.

- le droit du patient sur le sort de ses données après son décès en particulier la conservation, l'effacement, la communication en respect du code de santé publique (article L.1110-4)

Le patient pourra exercer ses droits directement auprès du biologiste coresponsable du laboratoire auquel il s'adresse ou sur demande par courrier postal adressée au siège social de DYOMEDEA, 480 avenue Ben Gourion à LYON 69009.

3°) <u>Nature des traitements des données et des mesures de sécurité</u>

Traitements

DYOMEDEA recueille les données personnelles de ses patients et les traite pour des finalités inhérentes à son activité et aux besoins de son métier de biologie médicale, les principaux traitements étant :

- Enregistrement des prescriptions d'analyses et constitution du dossier patient
- Enregistrement de la "fiche de suivi médical » avec renseignements cliniques
- Gestion des rendez-vous à domicile ou au laboratoire

- Transmission de prélèvements aux fins d'analyses vers d'autres laboratoires spécialisés ou non
- Gestion des analyses sur les plateaux technique et production des comptes rendus de résultats
- Diffusion des résultats par voie électronique ou matérielle par courrier aux professionnels de santé prescripteurs en ville ou en établissements de soins
- Mise à disposition des patients des comptes rendus au format pdf chiffré sur serveur web sécurisé
- Constitution des lots et télétransmission des feuilles de soins électroniques
- Réalisation d'études statistiques à usage interne
- Participation à des études épidémiologiques ou scientifiques

Données

Pour cela DYOMEDEA recueille les données personnelles suivantes en direct ou à l'aide de la carte VITALE

- Identité du patient : nom, prénom, date de naissance, sexe, adresse, numéros de téléphone fixe ou portable, adresse mail;
- numéro de Sécurité Sociale et taux de prise en charge (régime d'exonération, durée de validité des droits) pour l'édition des feuilles de soins et la télétransmission aux organismes assurant la gestion du régime obligatoire d'assurance maladie dont il dépend ;
- adhésion à un régime complémentaire: numéro d'adhérent et taux de prise en charge ;
- santé : prescriptions médicamenteuses ou de traitements divers, résultats et comptes rendus d'analyses antérieurs, coordonnées des médecins traitants, renseignements biologiques, cliniques et thérapeutiques, antécédents, traitements en cours ;
- informations relatives aux habitudes de vie avec l'accord du patient et uniquement si elles sont nécessaires à la réalisation ou à l'interprétation des examens demandés.

Mesures de sécurité

DYOMEDEA s'engage à renforcer la sécurité de ses systèmes d'informations qu'il détient en propre ou via ses sous-traitants et à mettre en œuvre les mesures correspondantes aux exigences de sécurité suivantes :

- pour le traitement des données à la conception des traitements avant leur mise en œuvre lors de tests et de l'évaluation des risques potentiels (protection by design) ou pour les traitements déjà en cours lors de l'étude d'impact (PIA) sur la vie privée des personnes concernées

- pour l'accès aux données seulement réservé aux personnels habilités et selon leur fonction dans l'entreprise laboratoire en appliquant le principe de moindre privilège.

- pour l'authentification des intervenants utilisateurs à l'aide de dispositifs d'authentification sécurisés (identifiant, mot de passe, certificat)

- pour l'intégrité des données par la mise en place d'une traçabilité permanente des accès aux données, avec conservation des traces et des moyens de supervision des accès

- pour les transferts électroniques des données par la mise en œuvre de flux chiffrés garantissant la confidentialité et l'intégrité à l'aide de moyens conformes à l'état de l'art (VPN SSL, FTPS, Web sécurisé https), d'échanges via messageries sécurisées type MSS validés par des conventions de preuve.

- pour l'hébergement des données en hébergement externe (cloud) en faisant appel à un sous-traitant hébergeur agréé HDS garantissant intégrité, disponibilité et maintient en conditions opérationnelles des accès, en hébergement interne (serveurs virtualisés) en faisant appel à un sous-traitant info-gérant chargé de la supervision de l'infrastructure informatique complète (serveurs, liens intersites, réseaux, matériel périphérique)

- pour la sauvegarde des données et la continuité de l'activité en mettant en place des procédures de sauvegarde adaptées, avec tests de restauration, des modalités de suppression effective de données; en programmant un plan de reprise ou de continuité d'activité (PRA,PCA) permettant d'assurer une continuité de service même en conditions de situation dégradée.

Enfin au-delà des seules exigences de protection de données personnelles de ses patients DYOMEDEA s'engage plus largement à l'aide de son sous-traitant infogérant conformément au cahier des charges établi pour l'appel d'offres d'info-gérance :

- à prendre en compte l'ensemble des mesures nécessaires à la supervision de tous les systèmes d'information au sein du laboratoire

- à sécuriser les postes de travail à l'aide des moyens appropriés (pare-feu, anti-virus) en interne mais aussi dans le cadre de la mobilité pour les postes nomades, limitation d'accès et politique de mot de passe

- à sécuriser les procédures de la maintenance informatique (suivi des interventions, revue des contrats fournisseurs, inventaire et suivi du matériel périphérique, politique de mise à jour de logiciel métier et bureautique)

- à sécuriser le réseau interne, pilotage par active directory, cloisonnement des sous-réseaux, sécurisation des wifi, outil de supervision en temps réel

- à sécuriser les locaux (salle info, accès, badges, détection incendie et DDE)

4°) <u>Incidents et violations de données</u>

DYOMEDEA respectera l'obligation de notification aux autorités compétentes de toute situation de violation de la sécurité pouvant entrainer accidentellement ou non, la destruction, perte, altération ou divulgation non autorisée de données à caractère personnel.

Après évaluation des risques encourus et de l'impact des conséquences éventuelles de l'incident sur la vie personnelle des patients, les procédures mises en place devront permettre d'établir une déclaration dans les délais requis et d'avertir les patients concernés.

LA DIRECTION DE DYOMEDEA