Annexe 1 à la convention de Médecine Préventive : Protection des données personnelles

1/ Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le Centre de gestion, sous-traitant (ST) s'engage à effectuer pour le compte de … *(dénomination de la collectivité ou de l'établissement)* responsable de traitement (RT) les opérations de traitement de données à caractère personnel définies ci-après.

2/ Finalités

Le Traitement a pour but d'assurer le suivi médical des agents des collectivités adhérentes au service de médecine préventive du Centre de Gestion du Loiret.

- Organiser les visites d'information et de prévention (visites périodiques, sur demande des collectivités, des agents ou des médecins … etc)
- Assurer le suivi des visites d'information et de prévention réalisées, le conseil à l'agent ou l'autorité territoriale en fonction de spécificités de son dossier ou poste/environnement de travail et l'édition des documents administratifs règlementaires (fiche de compatibilité).

La base légale du traitement est l'exécution d'un « contrat ».

3/ Les Données Personnelles traitées

Les données personnelles traitées sont les suivantes, *données d'identification, Données sur la vie personnelle et Données sur la vie professionnelle*

Les données sensibles traitées concernent les données de santé de l'agent sont les suivantes :

- Modes/Habitudes de vie
- Données biométriques (taille, poids, IMC)
- Résultats de tests (visiométrie, audiométrie, questionnaire psychologique)
- Pathologies et antécédents
- Vaccins
- Orientations et conseils/préconisations du médecin du travail à l'issue de la visite
- Décision de compatibilité de l'agent / Poste de travail (et potentielles restrictions/recommandations d'aménagement)
- Examens et expertises médicaux

4/Les catégories de personnes concernées

Les catégories des personnes concernées sont les agents titulaires et contractuels des collectivités adhérentes au service de médecine préventive.

5/ Informations mises à disposition par le responsable du traitement au sous-traitant

Le responsable de traitement s'engage à fournir au sous-traitant la liste des effectifs mise à jour de la collectivité, ainsi que les coordonnées des personnes contacts en charge du suivi de l'exécution de la mission. Il veillera à mettre en place les mesures nécessaires pour protéger les données échangées.

6/ Les destinataires des données :

Les destinataires internes des données sont les personnels habilités du service médecine préventive à traiter les informations : secrétaire, infirmier, médecin et autres professionnels de santé.
Sous conditions particulières réglementaires, le dossier de l'agent peut être transmis à la famille, à son médecin traitant ou à un avocat. Une copie peut être également au conseil médical.

7/ Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la convention.

- Traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'union ou du droit des états membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'union ou du droit de l'état membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre de la présente convention
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu de la présente convention :
  - Respectent 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
  - Prennent en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut
  - Informent le responsable de traitement et obtiennent son accord écrit en cas de recours à un autre sous-traitant

8/ Information des personnes

Les personnes concernées sont informées de ce traitement, plus précisément de la création de leur "dossier médical" directement par le personnel médical et paramédical lors de leur première visite. Ceci leur est rappelé lors des visites suivantes.
Pour rappeler à l'équipe médicale cette nécessité d'information, la date de notification à l'intéressé de cette information, ainsi que de ses droits et modalités de consultation et rectification est enregistrée dans le logiciel.

Un panneau d'information est affiché dans la salle d'attente.

9/ Exercice des droits des personnes

Les demandes de droit d'accès, de rectification et de droit à l'effacement sont à adresser au responsable du service de Médecine Préventive du CDG, medecine.preventive@cdg45.fr .

Le droit à l'effacement est possible et réalisé que si le dossier de l'agent est transféré à un autre service de médecine préventive.

L'agent peut refuser de donner certaines informations et/ou demander explicitement à ce que ne soient pas enregistrées certaines informations. Le personnel médical lui précise oralement.

Mesures de sécurité

- **Description générale de l'environnement système MEDTRA – AXESS SOLUTION**

L'application MEDTRA est composée d'un serveur virtuel d'application, d'un serveur virtuel de type BDD et d'un client lourd installé sur les postes dédiés aux professionnels de santé et au secrétariat de service de Médecine professionnelle

- **Sécurisation des données du CDG45**

L'ensemble des données propres à MEDTRA est localisé sur des infrastructures appartenant au CDG45. Les serveurs de données sont hébergés sur une machine virtuelle.

Cette infrastructure met en œuvre un cluster de serveurs physiques localisé dans une salle serveur et sécurisée par digicode ; avec système de climatisation.

Les moyens de sécurisation déployés au CDG45 assurent le cloisonnement réseau. Un firewall assure le cloisonnement des réseaux du siège du CDG45. Une journalisation des évènements de sécurité est effectuée. Elle met en œuvre une 'Appliance' collectrice spécialisée dans l'analyse. Un niveau de filtrage antivirus supplémentaire est assuré par les fonctions UTM du firewall protégeant les réseaux du siège du CDG45. Les flux correspondant aux principaux protocoles

sont examinés. Les postes de travail sont sécurisés par des anti-virus et anti-malwares, et un identifiant unique et mot de passe personnalisable et renouvelé.

Les utilisateurs opérant à l'extérieur des locaux du siège peuvent se connecter aux infrastructures centrales par le biais d'un VPN.

- **Accès à l'application MEDTRA – AXESS Solution**

L'authentification des utilisateurs CDG45 est individualisée au niveau de l'identifiants et du degré d'interaction avec l'applicatif.

- **Journalisation**

L'ensemble des accès aux applications MEDTRA – AXESS Solution est consigné au niveau de journaux internes. L'accès à ces journaux est restreint à l'administrateur du CDG45.

- **Mises à jour**

L'ensemble des hôtes et systèmes partie prenante dans l'infrastructure MEDTRA – AXESS Solution est mis à jour régulièrement, à l'annonce de mise à disposition de correctifs systèmes jugés stables.

Ceci vaut pour les serveurs physiques, les serveurs virtualisés, leurs composants logiciels standards (serveur web, bases de données, etc), les firewalls et les postes de travail des personnels du CDG45.

Notification des violations de données à caractère personnel

Le sous-traitant notifie par tout moyen, au responsable de traitement sans délai toute violation de données à caractère personnel après en avoir pris connaissance Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La documentation contient au moins :

- La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Durée de conservation des données

Le Dossier Médical est conservé 20 ans à compter de la dernière consultation. Les dossiers sont triés et archivés. Les fiches de visite et les certificats de compatibilité sont conservés 5 ans puis détruits à l'exception des fiches avec restrictions médicales qui sont conservées.

Sort final des données à la fin de la prestation

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement et à les détruire.

Données internes du responsable de traitement

En dehors de toute prestation de service, la Collectivité est informée que ses propres données internes pourront être traitées par le sous-traitant en tant que Responsable de Traitement, à des fins de gestion de la relation avec la Collectivité. Les rapports annuels sont conservés 5 ans puis archivés.

Contact : medecine.preventive@cdg45.fr