Annexe relative aux obligations de la collectivité/l'établissement « responsable de traitement » et du CDG56 « sous-traitant » en matière de protection des données

1. Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer **pour le compte** du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

2. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les services objets de la convention.

Le responsable de traitement s'engage à documenter par écrit toute instruction concernant le traitement de données personnelles par le sous-traitant.

La nature des opérations réalisées sur les données ainsi que la ou les finalité(s) du traitement sont précisés aux articles 3 à 5 de la convention.

Les données à caractère personnel strictement demandées sur les agents auprès de la collectivité/l'établissement sont : nom, prénom, date de naissance, nature du contrat (avec date de début et de fin le cas échéant), et de manière facultative les risques auxquels les agents sont exposés (article 3 de la convention) ; auxquelles s'ajoutent après autorisation des agents les informations de leur dossier médical.

Les catégories de personnes concernées sont les agents de la collectivité/l'établissement (article 1 de la convention).

Les destinataires de ces données sont les médecins de prévention et par délégation les infirmiers en santé au travail et les assistants de centre (article 3 de la convention).

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires visées aux articles 3 à 5 de la convention.

3. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la convention ;

2. 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 Etats 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'Etat 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 ;

3. **garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat ;

4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :
   - 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

5. prendre 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 ;**

6. informer le RT et obtenir son accord écrit en cas de recours à autre sous-traitant ;

7. **Droit d'information des personnes concernées**
   Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8. **Exercice des droits des personnes**
   Dans la mesure du possible, le sous-traitant aidera le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

   Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au responsable du traitement.

9. **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.

10. **Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**
Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. **Mesures de sécurité**

Description générale de Medtra
L'application Medtra est un logiciel métier dédié aux professionnels de santé du CDG56. Les données de santé sont exclusivement hébergées sur les serveurs du CDG56.

Le portail Medtra est une application full-web, proposée en mode hébergé (SaaS) par l'éditeur Axess. Medtra est exclusivement propriétaire des codes d'accès à la base de données du portail et de l'application.

Une machine virtuelle dédiée lance également par tâche planifiée la synchronisation d'une partie des données (dates de consultation, nature de la visite médicale et conclusion) entre l'instance Medtra du CDG56 et le portail Medtra hébergé.

Sécurisation des données côté CDG56
Le serveur de base de données, les images des postes VDI, la machine virtuelle servant à la synchronisation sont hébergées sur l'infrastructure de virtualisation du CDG56.

Cette infrastructure met en œuvre un cluster de serveurs physiques répartis entre deux salles distinctes sécurisées par authentification par badge selon l'habilitation ; toutes avec système de climatisation.

Les autres moyens de sécurisation déployés au CDG56 assurent le cloisonnement réseau ainsi que les postes de travail par des anti-virus et Malwares, et un identifiant unique et mot de passe personnalisable. 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 de cluster de firewall protégeant les réseaux du siège du CDG56. Les flux correspondant aux principaux protocoles sont examinés.

Sécurisation des données du Portail
Le serveur hébergeant le portail est hébergé et opéré par Axess-Online, acteur certifié 'hébergement de données de santé' (HDS). Axess Online fait partie du même groupe qu'Axess Solution Santé, l'éditeur de Medtra.

Axess Online héberge ses machines dans des baies situées dans un datacenter à Lyon (datacenter principal) répondant aux plus hautes normes de sécurité et de redondance. Axess Online dispose également de baies dans deux datacenters secondaires à Saint-Denis (93) et Nanterre (92).

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

Accès à l'application
L'application Medtra n'est accessible qu'au moyen d'un 'bureau' publié. Les bureaux sont accessibles avec un client Receiver. Les flux réseau entre l'utilisateur et l'infrastructure sont cryptés. Les utilisateurs s'identifient par un identifiant unique et un mot de passe personnalisable.

Accès au portail Medtra
Les accès au portail Medtra s'opèrent exclusivement sous protocole HTTPS. L'ensemble des communications sont cryptées. Ceci vaut tant pour les accès utilisateurs (collectivités et gestionnaires) que pour les accès techniques (synchronisation de données de rendez-vous). Les utilisateurs s'identifient par un identifiant unique et un mot de passe personnalisable.

Journalisation
L'ensemble des accès à l'application Medtra est consigné au niveau des journaux produits par ;

- Active Directory (logon, horodatage)
- Passerelle NetScaler (logon, horodatage, éléments de session, adresse IP)
- DirectAccess (logon, horodatage, éléments de session, adresses IP)
- Citrix Director (logon, élements de session)
- Medtra (logon, éléments de session, historique des actions)

Mises à jour
L'application Medtra et le portail Medtra sont mis à jour régulièrement, directement par l'éditeur.

12. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

- à renvoyer les données à caractère personnel selon les modalités prévues à l'article 8 de la convention.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

13. **Délégué à la protection des données**

Le sous-traitant communique au responsable de traitement **le nom et les coordonnées de son délégué à la protection des données,** s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. **Registre des catégories d'activités de traitement**

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

- les catégories de traitements effectués pour le compte du responsable du traitement.

4. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données visées au point 2.
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant