EXEMPLE DE REGISTRE

Pour faciliter la tenue du registre, ESEA vous propose un modèle de registre de base, inspiré du modèle fournit par la CNIL. Ce registre est destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre structure **en tant que responsable de traitement**. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la règlementation.

Composition du document

1. Une première page du registre recense les informations communes à toutes vos activités de traitement.

    - Les coordonnées de votre structure
    - Les coordonnées du délégué à la protection des données (DPO) si vous en disposez
    - La liste des activités de votre structure impliquant le traitement de données personnelles.

2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.

    Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.

Registre des activités de traitement

Coordonnées du responsable de la structure *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	

Activités de la structure impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Messagerie sécurisée de Santé*
Activité 2	
Activité 3	
Activité 4	
Activité 5	
Activité 6	
Activité 7	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

Fiche de registre de l'activité 1

Messagerie sécurisée de Santé

Date de création de la fiche	**17/05/2019**
Date de dernière mise à jour de la fiche	**17/05/2019**
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	
Nom du logiciel ou de l'application *(si pertinent)*	**ProMess (service de messagerie sécurisée de santé ESEA)**

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Permettre l'échange de données de santé au moyen d'un service de messagerie sécurisée de santé entre professionnels de santé et, plus largement, entre les professionnels des secteurs sanitaire, social et médico-social habilités par une loi à collecter et à échanger des données de santé à caractère personnel (ci-après dénommés " professionnels habilités ") dans le cadre de la prise en charge, par ces professionnels, des personnes concernées par les données échangées

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

1. patients
2. professionnels utilisateurs

Catégories de données collectées

Listez les différentes données traitées

1. *Données relatives aux patients:*
   - les données d'identification (nom, prénom, date et lieu de naissance, sexe),
   - *les coordonnées (adresse, numéros de téléphone, adresses de courriel) ;*
2. *Données relatives aux professionnels utilisateurs finaux dits professionnels habilités :*
   - les données d'identification (état civil), l'identifiant du professionnel (numéro d'enregistrement au répertoire partagé des professionnels de santé (RPPS), numéro d'enregistrement au répertoire ADELI ou numéro d'identification local) et les données relatives au moyen d'authentification ;
   - les coordonnées professionnelles (adresse, numéros de téléphone, adresse de courriel) ;
   - le(s) titre(s) professionnel(s) ;
   - les adresses de messagerie sécurisées de santé créées ;

- les données techniques nécessaires à la fourniture du service de messagerie sécurisée de santé (adresse IP, cookies) ;
- les traces des actions opérées sur la messagerie sécurisée de santé.

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

Données relatives aux patients:

- les informations strictement nécessaires à la prise en charge des personnes et relatives à leur état de santé, à leur situation sociale ou à leur autonomie
- éventuellement l'identifiant national de santé

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

- Le service de messagerie sécurisée ne se substitue en aucun cas au dossier médical, sanitaire ou médico-social des personnes concernées (les patients) que doivent tenir les professionnels habilités en vertu des obligations légales et réglementaires qui leur incombent. Il constitue uniquement un outil professionnel d'échange sécurisé de données de santé, et non un nouvel espace de stockage.
- Afin d'être conforme, un service de messagerie doit comporter un système permettant d'organiser la suppression des boîtes aux lettres (BAL) en cas d'inactivité complète, caractérisée par l'absence d'authentification de l'utilisateur pendant une période maximale d'un an.
- Les traces techniques sont conservées pendant un an

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Les destinataires des messages échangés au moyen de leurs messageries sécurisées de santé, ayant la qualité de " professionnels habilités " telle que définie en préambule de la présente fiche registre. Les professionnels de santé et les professionnels habilités sont soumis au secret professionnel prévu à l'article 226-13 du code pénal. Les personnes en charge de l'administration de la messagerie peuvent accéder aux données relatives aux professionnels utilisateurs finaux dans le strict cadre de leurs missions et dans le respect du secret des correspondances privées. Elles doivent, en outre, être soumises à une clause de confidentialité.

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☒ Non

Si oui, vers quel(s) pays :

……..……..……..

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

[X] Contrôle d'accès des utilisateurs

Décrivez les mesures : - Comptes nominatifs individuels (CPS ou autres moyens d'authentification forte)

[X] Mesures de traçabilité

Nature des traces : identifiant, date et heure de connexion, actions, adresse IP

Durée de conservation : 1 an

[X] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

- Au niveau de l'hébergement HDS : antivirus, mise à jour et correctifs de sécurité, pare-feu
- Au niveau du poste : < A préciser en fonction des mesures prises>

[X] Sauvegarde des données

Décrivez les modalités :

- Au niveau de l'hébergeur HDS :
  - ☐ Sauvegarde différentielle hebdomadaire sur un serveur de fichier délocalisé
  - ☐ Sauvegarde totale Mensuelle sur support de stockage mort
- Au niveau du poste : < A préciser en fonction des mesures prises>

[X] Chiffrement des données

Décrivez les mesures (e*xemple : site accessible en https, utilisation de TLS, etc.)* :

- Au niveau de l'hébergeur HDS :
  - ☐ accès Webmail en https
  - ☐ accès Client de messagerie en Imaps/SMTPs
  - ☐ Chiffrement (SMIME) des messages échangés hors MSsanté
  - ☐ Stockage Chiffré
- Au niveau du poste : < A préciser en fonction des mesures prises>