Commission nationale de l'informatique et des libertés

Délibération n° 2019-057 du 9 mai 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires

NOR : *CNIL1920561X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 54-II ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Valérie PEUGEOT, commissaire, en son rapport et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Adopte le référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires annexé à la présente délibération.

Décide que le référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires entre en vigueur le lendemain de sa publication au *Journal officiel* de la République française.

Décide que toute modification apportée à un traitement de données à caractère personnel qui aurait été régulièrement constitué antérieurement à la date d'entrée en vigueur du présent référentiel et qui y serait conforme impose aux responsables de traitement concernés de procéder à une déclaration de conformité.

La présidente,
M.-L. DENIS

ANNEXE

RÉFÉRENTIEL RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE À DES FINS DE GESTION DES VIGILANCES SANITAIRES

1. **A qui s'adresse ce référentiel ?**

Ce référentiel encadre exclusivement les traitements de données à caractère personnel :

– constitués pour gérer les vigilances sanitaires ;
– et mis en œuvre par des fabricants, entreprises, exploitants, organismes responsables de la mise sur le marché d'un médicament, d'un dispositif ou d'un produit et dénommés, ci-après, responsables de traitement.

Par application des dispositions du 1° de l'article 65 de la loi du 6 janvier 1978 modifiée, les traitements de données à caractère personnel mis en œuvre par les professionnels de santé et les systèmes ou services de soins de santé (p. ex. : établissements de santé, maisons de santé, centres de santé, agences sanitaires, etc.) ne sont pas concernés par ce référentiel.

2. **Portée du référentiel**

Ce référentiel précise le cadre juridique, issu du règlement général sur la protection des données (RGPD) et des dispositions nationales, applicable aux traitements de données à caractère personnel constitués dans le cadre des vigilances sanitaires. Il couvre le périmètre des vigilances sanitaires mentionnées dans l'arrêté du 27 février 2017 fixant la liste des catégories d'événements sanitaires indésirables pour lesquels la déclaration ou le signalement peut s'effectuer au moyen du portail de signalement des événements sanitaires indésirables.

Les responsables de traitement qui adressent à la CNIL une déclaration de conformité, pour les traitements de données à caractère personnel répondant aux exigences fixées par le présent référentiel, via le formulaire de déclaration de conformité à remplir sur le site internet de la CNIL, sont autorisés à les mettre en œuvre.

Tout traitement de données à caractère personnel qui excède le cadre ou les exigences définis par le présent référentiel doit en revanche faire l'objet d'une demande d'autorisation spécifique conformément aux dispositions de l'article 66-III de la loi du 6 janvier 1978 modifiée.

Les responsables de traitement doivent mettre en œuvre toutes les mesures appropriées (techniques et organisationnelles) afin de garantir la protection des données personnelles traitées, à la fois dès la conception du traitement et par défaut. Ils doivent, en outre, démontrer cette conformité tout au long de la vie des traitements. Les traitements mis en œuvre dans le cadre du référentiel doivent également être inscrits dans le registre des activités de traitement prévu à l'article 30 du RGPD (voir les modèles de registres sur le site cnil.fr).

Les principes dégagés par la CNIL, dans ce référentiel, constituent une aide à la réalisation de l'analyse d'impact à la protection des données que les responsables de traitement concernés doivent mener. Les responsables de traitement pourront ainsi définir les mesures leur permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7 du référentiel), de garantir les droits des personnes (points 8 et 9 du référentiel) et la maîtrise de leurs risques (points 10 à 12 du référentiel).

3. **Objectif(s) poursuivi(s) par le traitement (FINALITÉS)**

Un traitement mis en œuvre aux fins de gestion des vigilances sanitaires a pour finalité de permettre la prévention, la surveillance, l'évaluation, la gestion des événements sanitaires indésirables mis en place par le responsable de traitement.

Le traitement vise à permettre :

– la collecte, l'enregistrement, l'analyse, le suivi, la documentation, la transmission et la conservation des données relatives à l'ensemble des événements sanitaires indésirables ;
– la gestion des contacts, par le responsable de traitement, avec la personne lui ayant notifié l'événement sanitaire indésirable (membre d'une association agréée, professionnel de santé, membre d'une autorité sanitaire, patient, etc.) ou le professionnel de santé pouvant être interrogé pour obtenir, dans le respect du secret médical, des précisions sur l'événement sanitaire indésirable signalé (professionnel suivant la personne victime de l'événement sanitaire indésirable, etc.).

Les informations recueillies pour ces finalités ne pourront pas être réutilisées pour poursuivre une autre finalité que celle prévue dans le cadre du présent référentiel.

4. **Base(s) légale(s) du traitement**

Dans le cadre des vigilances sanitaires entrant dans le champ du présent référentiel, le respect des obligations légales imposées au responsable de traitement par les dispositifs de vigilance sanitaire prévus notamment par le code de la santé publique est retenu comme base légale du traitement de données à caractère personnel constitué.

La collecte de données de santé dans le cadre des vigilances sanitaires est nécessaire pour des motifs d'intérêt public ; elle a notamment pour objectif de garantir le respect de normes élevées de qualité et de sécurité des soins de santé et des médicaments, des dispositifs ou des produits conformément aux dispositions de l'article 9 du RGPD et de l'article 66 de la loi du 6 janvier 1978 modifiée.

5. **Données personnelles concernées**

Seules des données pertinentes au regard de l'objectif du traitement, à savoir la gestion des vigilances sanitaires, peuvent être collectées et traitées. A ce titre, le responsable de traitement peut collecter et traiter, en fonction de l'objectif poursuivi par le traitement et des situations :

a) Les données relatives à la personne exposée strictement nécessaires à l'appréciation de l'événement sanitaire indésirable :

– données permettant d'identifier indirectement la personne exposée à l'événement sanitaire indésirable (informations signalétiques telles que l'âge, l'année ou la date de naissance, le sexe, le poids, la taille) ou numéro d'identification de la personne (code alphanumérique, code alphabétique d'identification tel que prévu par les formulaires existant) permettant de garantir le respect de sa vie privée, à l'exclusion du numéro d'inscription au répertoire national d'identification des personnes physiques et de l'identifiant national de santé ;
– données relatives à l'identification du produit concerné par le signalement de l'événement sanitaire indésirable : type de médicament, de dispositif ou de produit utilisé, numéro de série, etc. ;
– données de santé, notamment : traitements administrés, résultats d'examens, nature du ou des effets indésirables, antécédents personnels ou familiaux, maladies ou événements associés, facteurs de risques, informations relatives au mode de prescription et d'utilisation des médicaments et à la conduite thérapeutique du prescripteur ou des professionnels de santé intervenant dans la prise en charge de la maladie ou de l'événement sanitaire indésirable.

En complément de ces données, le responsable de traitement peut également collecter et traiter d'autres données sous réserve qu'elles soient strictement nécessaires à l'appréciation de l'événement sanitaire indésirable (vie professionnelle, consommation de tabac, alcool, drogue, habitudes de vie et comportements). Des données relatives à l'origine ethnique peuvent être collectées par le responsable de traitement lorsqu'un document de présentation des caractéristiques du médicament, du dispositif ou du produit validé par une autorité compétente (p. ex. : résumé des caractéristiques du produit pour les médicaments, résumé des caractéristiques du dispositif médical, etc.) fait état, en s'appuyant sur des travaux scientifiques, de la circonstance que l'origine ethnique des personnes peut avoir une incidence sur son efficacité ou sa sécurité.

b) Les coordonnées de la personne ayant procédé à la notification de l'événement sanitaire indésirable ou de tout professionnel de santé susceptible d'apporter des précisions (nom, prénom, coordonnées postales, électroniques, téléphoniques, le cas échéant spécialité du professionnel de santé). Selon les situations, la personne ayant procédé à la notification peut être : le membre d'une autorité sanitaire, un professionnel de santé, la personne exposée à l'événement sanitaire indésirable ou son entourage, le(s) titulaire(s) de l'autorité parentale, l'ayant droit en cas de décès, une association de patients agréée, etc. La notification de l'événement sanitaire indésirable, qui serait réalisée directement par la personne exposée, a pour effet de lever le secret de son identité, et doit être limitée à ce que le responsable de traitement a besoin de connaître pour satisfaire à ses obligations en matière de vigilances sanitaires et pour une durée strictement limitée à ce qui est nécessaire pour répondre auxdites obligations.

6. **Destinataires des données**

Seuls les employés habilités du responsable de traitement doivent pouvoir, sous la responsabilité de ce dernier, accéder aux données à caractère personnel traitées, dans la limite de leurs attributions respectives et pour ce qui les concerne, notamment :

- le responsable de la vigilance, ainsi que ses collaborateurs et agents intervenant dans le processus de gestion des vigilances sanitaires ;
- les personnels du service des audits, de manière ponctuelle et motivée, pour vérifier le respect des exigences réglementaires ;
- les personnels habilités en charge de la gestion des réclamations, en fonction des dossiers qu'elles ont à traiter.

Peuvent également être destinataires des données nécessaires à l'exercice de leurs missions, exclusivement dans le cadre de leur activité de vigilance :

- les sous-traitants intervenant pour le compte et sous la responsabilité de l'organisme, dans la limite de leurs fonctions et dans les conditions définies par le contrat de sous-traitance. En cas de recours à un sous-traitant, le contrat qui lie le responsable de traitement au sous-traitant doit faire mention des obligations qui lui incombent en matière de protection des données (article 28 du RGPD). Le guide du sous-traitant édité par la CNIL précise ses obligations et les clauses à intégrer dans les contrats ;
- les autres sociétés du groupe auquel l'organisme appartient qui participent à l'exploitation ou à la commercialisation du médicament, du dispositif ou du produit mis en cause ;
- les tiers dont un médicament, un dispositif ou un produit pourrait être mis en cause, à l'exception des données directement identifiantes de la personne exposée à l'événement sanitaire indésirable qui aurait notifié l'événement ;
- les professionnels de santé participant au suivi du patient et les professionnels de santé ou autres professionnels pouvant apporter un complément ;
- les organismes notifiés en charge de l'évaluation d'un médicament, d'un dispositif ou d'un produit, à l'exception des données directement identifiantes de la personne exposée à l'événement sanitaire indésirable qui aurait notifié l'événement ;
- les organismes publics nationaux (p. ex. : agences régionales de santé, agences sanitaires, etc.) ou étrangers en charge des vigilances dans le cadre de l'exercice de leurs missions telles que définies par les textes, les autorités ou agences sanitaires nationales étrangères et les autorités ou agences sanitaires internationales (p. ex. : Agence européenne des médicaments), à l'exception des données directement identifiantes de la personne exposée à l'effet indésirable qui aurait notifié l'événement.

7. **Durées de conservation**

Les données collectées et traitées pour gérer les vigilances sanitaires ne peuvent être conservées de façon indéfinie. Une durée de conservation précise doit être préalablement fixée en fonction de la finalité du traitement.

Au regard des finalités du traitement, les données sont conservées en base active pendant la durée d'utilisation courante des données. Elles sont ensuite conservées en archivage intermédiaire pendant la durée légale ou réglementaire applicable à chaque vigilance sanitaire. En l'absence de durée légale ou réglementaire, les données ne peuvent être conservées au-delà d'une période de soixante-dix ans à compter de la date du retrait du marché du médicament, du dispositif ou du produit.

A l'expiration de ces délais, les données sont supprimées ou archivées sous une forme anonymisée.

La conservation et l'archivage des données doivent être réalisés dans des conditions de sécurité conformes aux dispositions de l'article 32 du RGPD.

8. **Information des personnes**

Un traitement de données à caractère personnel doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées (personnes exposées à l'événement sanitaire indésirable, personne ayant notifié l'événement sanitaire indésirable et professionnel de santé ayant suivi la personne concernée par l'événement). Le responsable de traitement prend les mesures appropriées pour fournir à la personne concernée une information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Dès le stade de la collecte, les personnes concernées par le traitement doivent être individuellement informées des modalités de traitement de leurs données dans les conditions prévues par les articles 13, le cas échéant, 14 du RGPD, 69 et 70 de la loi Informatique et libertés.

En cas de notification de l'événement sanitaire indésirable par la personne qui y est exposée, une information particulière doit lui être fournie préalablement, afin de l'informer que le secret de son identité ne sera pas préservé.

Le support d'information est libre (oral ou écrit).

Si la personne concernée en fait la demande, elle peut obtenir la mise à disposition d'un support d'information écrit.

En cas de notification de l'événement sanitaire indésirable par une personne autre que celle qui y est exposée, l'information est réalisée par le notificateur sur la base des éléments d'information écrits remis par le responsable de traitement au notificateur.

Le responsable de traitement doit à tout moment justifier que l'information des personnes concernées a été délivrée, à charge pour le responsable de traitement de recueillir auprès du notificateur la preuve de cette délivrance.

Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs droits.

9. **Droits des personnes**

Les personnes concernées par le traitement (personnes exposées à l'événement sanitaire indésirable, personne ayant notifié l'événement sanitaire indésirable et professionnel de santé ayant suivi la personne concernée par l'événement) disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD :

- droit d'accès ;
- droit de rectification ;
- droit à la limitation du traitement (par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander au responsable de traitement le gel temporaire de ses données le temps que celui-ci procède aux vérifications nécessaires).

Dans la mesure où le traitement est fondé sur le respect d'une obligation légale, les personnes concernées par la collecte des données ne disposent ni du droit d'opposition, ni du droit à l'effacement des données, ni du droit à la portabilité des données. Les personnes concernées en sont informées préalablement.

10. **Sécurité**

De manière générale, le responsable du traitement doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique du présent référentiel, soit le responsable de traitement adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir :

Catégories	Mesures
Former les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (*login*) unique à chaque utilisateur
	Utiliser un moyen d'authentification forte, appuyé sur un annuaire vérifié
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session

Catégories	Mesures
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (*firewall*) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention à distance sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant ne passe dans les URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les traceurs (*cookies*) non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique.
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, *etc.*)
Sécuriser les échanges avec d'autres organismes	Envoyer les données de façon chiffrée (soit en chiffrant directement les données ou en utilisant un tunnel chiffré)
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles publié par la CNIL.

Toute violation de données devra être notifiée à la CNIL dans les conditions prévues à l'article 33 du RGPD.

Il est demandé, qu'en cas de recours à un prestataire extérieur pour le stockage et la conservation des données de santé à caractère personnel par le responsable de traitement, ce prestataire soit un hébergeur de données de santé agréé ou certifié. Par exception, lorsque le responsable de traitement n'est pas établi en France, le responsable de traitement doit démontrer que le prestataire auquel il recourt présente des garanties de sécurité équivalentes.

Le recours aux services d'un sous-traitant devra s'effectuer dans les conditions prévues à l'article 28 du RGPD.

11. **Transfert de données hors de l'Union européenne**

Les données indirectement identifiantes des personnes exposées à un événement sanitaire indésirable et les données directement identifiantes des personnes ayant notifié l'événement sanitaire indésirable peuvent faire l'objet d'un transfert hors de l'Union européenne si les conditions suivantes sont réunies :

– les dispositions de l'article 6 relatives aux destinataires des données sont respectées ;
– le transfert de données est strictement nécessaire à la mise en œuvre du dispositif de vigilance.

Le transfert peut être effectué dans le cadre de la déclaration de conformité au présent référentiel lorsque l'une des conditions suivantes est remplie :

– le transfert s'effectue à destination d'un pays ou d'une organisation internationale reconnu par la Commission européenne comme assurant un niveau de protection adéquat, conformément à l'article 45 du RGPD (décision d'adéquation) ;
– le transfert s'effectue moyennant des garanties appropriées, listées à l'article 46, paragraphe 2, du RGPD (notamment : clauses contractuelles types approuvées par la Commission européenne, règles d'entreprise contraignantes, code de conduite, mécanisme de certification) ;
– en l'absence d'une décision d'adéquation ou de garanties appropriées, le transfert peut être fondé sur l'une des exceptions prévues par l'article 49 du RGPD lorsqu'un tel transfert n'est pas répétitif, massif ou structuré.

Le responsable de traitement doit avoir préalablement informé les personnes concernées du transfert de leurs données à caractère personnel vers des pays tiers à l'Union européenne, de l'existence ou de l'absence d'une décision d'adéquation ou de garantie appropriée et des moyens d'en obtenir une copie conformément à l'article 13, paragraphe 1, point *f*, du RGPD.

12. **Analyse d'impact sur la protection des données (AIPD)**

Conformément à l'article 35 du RGPD, le responsable de traitement doit réaliser une analyse d'impact sur la protection des données.

Pour réaliser son analyse d'impact, le responsable de traitement pourra se reporter :

– aux principes contenus dans ce référentiel ;
– aux outils méthodologiques proposés par la CNIL sur son site web.

Le cas échéant, le délégué à la protection des données (DPO) devra être consulté.

Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si, à l'issue de l'analyse d'impact, il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (risque résiduel restant trop élevé).