FEHAP
Santé Social - Privé Solidaire

RGPD : GUIDE PRATIQUE

POUR LES PETITS ÉTABLISSEMENTS SANITAIRES ET MÉDICO-SOCIAUX

10 fiches pour comprendre et mettre en œuvre le RGPD au sein de votre établissement

Ce guide a été réalisé par

Maitre Louvet

de Mon DPO Santé

Alors que la mise en conformité des établissements et structures de santé vis-à-vis du RGPD continue de se mettre en place, il nous est apparu essentiel de guider les petites structures dans cette démarche structurante, obligatoire et complexe.

C'est pourquoi nous avons voulu un guide directement opérationnel sous forme de fiches, destiné à faciliter la compréhension puis le démarrage de la mise en conformité.

Ce guide ne préjuge pas du travail, hélas très lourd à réaliser, mais va constituer une boussole pour le responsable de traitement de l'établissement (son Directeur Général) et son responsable de la mise en œuvre du RGPD (son Data Privacy Officer).

Nous vous en souhaitons bonne lecture, et la FEHAP reste à votre disposition pour vous aider dans son utilisation.

Bien à vous

Antoine Perrin,
Directeur Général FEHAP

edito

Fiche 1

COMPRENDRE
les principes et les enjeux du RGPD

Fiche 2

IMPLIQUER
ses responsables et sensibiliser ses personnels

Fiche 3

DÉSIGNER
un délégué à la protection des données (DPO)

Fiche 4

ÉLABORER
un programme de conformité

Fiche 5

CARTOGRAPHIER
les traitements et établir un registre

Fiche 6

RÉALISER
une analyse d'impact (PIA)

Fiche 1

COMPRENDRE LES PRINCIPES ET LES ENJEUX DU RGPD

Le Règlement Général de Protection des Données dit RGPD* (GPRD en anglais) est entré en application le 25 mai 2018. Il constitue le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel.

Le RGPD vise à renforcer la protection des données à caractère personnel en Europe. Il s'applique directement dans tous les pays de l'Union européenne et uniformise ainsi la législation en la matière au sein de tous les états membres.

La loi française du 6 janvier 1978 dite « loi Informatique et libertés » a été modifiée le 20 juin 2018 (JO du 21 juin 2018) pour être adaptée aux nouvelles règles du RGPD.

Le RGPD vise à favoriser la confiance des titulaires des données vis-à-vis des responsables du traitement et de leurs sous-traitants. Ces derniers sont notamment tenus d'assurer de la sécurité et de garantir la confidentialité des données qu'ils traitent.

Le titulaire des données est placé au cœur du nouveau dispositif légal. Le responsable du traitement a une obligation de transparence vis-à-vis des titulaires qui dispose de larges prérogatives pour contrôler l'utilisation qui est faite de ses données.

D'autre part, le RGPD consacre de nouveaux principes s'ajoutant à ceux déjà consacrés par la directive de 1995. Il s'agit en premier lieu du principe de responsabilité (ou accountability en anglais). Il s'agit également du principe de la vie privée dès la conception / vie privée par défaut ou celui du droit à l'oubli ou encore celui du droit à la portabilité.

Le principe de responsabilité est au stade de sa mise en œuvre également désigné par le terme conformité.

⚠ La conformité est avant tout une démarche que l'établissement devra mettre en œuvre afin de s'assurer qu'il se rapproche toujours plus d'un référentiel cible de principes, d'obligations et de bonnes pratiques.

Concrètement, le RGPD supprime, sauf exception en matière de recherche en santé, les formalités préalables de déclaration ou d'autorisation antérieurement en vigueur. Les établissements sont en contrepartie tenus à différentes mesures internes (notamment établir un registre, réaliser des analyses d'impact, stipuler certaines clauses contractuelles avec les sous-traitants). Sauf en ce qui concerne la désignation du DPO, ces mesures n'ont pas à être enregistrées ou déposées auprès de la CNIL. Elle peut cependant en demander la justification à tout moment.

Nous vous proposons de vous guider dans cette mise en conformité par un cheminement en dix étapes. Chacune de ses étapes fait l'objet d'une fiche.

À RETENIR

Le RGPD vise à établir la confiance des titulaires des données au travers de la responsabilité des acteurs qui doivent agir en transparence.

POUR ALLER PLUS LOIN

https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

*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 : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Fiche 2

IMPLIQUER SES RESPONSABLES ET SENSIBILISER SES PERSONNELS

La mise en conformité d'un établissement est **l'affaire de tous** et doit dès lors concerner l'ensemble des acteurs : direction – personnels administratifs – personnels soignants et de vie, qu'ils soient vacataires, permanents, salariés ou libéraux.

☞ Le directeur devra instaurer un comité de pilotage qui comprendra au minimum :

- Le directeur
- Les membres du comité de direction
- Un représentant des personnels soignants : médecin – cadre de santé – infirmier
- Un représentant des fonctions administratives
- Un représentant de la fonction informatique - interne ou externalisée
- S'il existe, un représentant de la fonction qualité

⚠ Le comité de pilotage devra être créé à titre **permanent** (cf. fiche 10) et se réunir **périodiquement** sous la présidence du directeur et en présence du DPO (cf. fiche 3). Une périodicité mensuelle est recommandée tout au moins durant la période initiale de mise en conformité.

Le directeur pourra confier au DPO (cf. fiche 3) l'animation du Comité de pilotage.

☞ Le directeur devra également programmer une **sensibilisation** en premier lieu des membres du comité de pilotage puis élargit à l'ensemble des personnels de l'établissement.

Elle devra être approfondie et renouvelée en fonction des personnels concernés. La sensibilisation de la direction et des personnels à la protection des données fait partie des missions du DPO (cf. fiche 3.)

Cette sensibilisation devra expliquer les principes fondamentaux du RGPD et faire une large place à leur traduction concrète sur les pratiques de prise en charge, de soins et d'accueil.

Cette sensibilisation pourra être conduite lors de réunions, mais également à l'aide de formations individuelles en ligne (MOOC).

La CNIL a lancé le 11 mars 2019 son propre MOOC gratuit et ouvert à tous. Il s'articule autour de quatre modules d'environ 5 heures.

La CNIL délivre des attestations aux personnes ayant suivi l'intégralité de ce MOOC.

À RETENIR

La première action du directeur devra consister à mettre en place un comité de pilotage de et de programmer à brève échéance des actions de sensibilisation.

POUR ALLER PLUS LOIN

La CNIL lance sa formation en ligne ouverte à tous
https://www.cnil.fr/fr/la-cnil-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous

Le MOOC de la CNIL
https://atelier-rgpd.cnil.fr/

Fiche 3

DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

La désignation d'un DPO est **obligatoire*** pour les établissements sanitaires et médico-sociaux dans la mesure où ceux-ci traitent des données de santé. Le DPO doit être désigné auprès de la CNIL.

DPO est le « chef d'orchestre » de la conformité en matière de protection des données au sein de l'établissement. Il est chargé d'informer et de conseiller l'établissement au travers du directeur que les employés.

Il contrôle également le respect du RGPD du droit national en matière de protection des données et rapporte directement au directeur en cas de non-conformité.

Enfin, il est le point de contact de la CNIL au sein de l'établissement et coopère avec elle lorsque nécessaire.

Afin d'assurer ses missions, le délégué doit notamment :

- Réaliser l'inventaire des traitements de données de l'établissement
- S'informer sur les nouvelles règles applicables
- Sensibiliser la direction et les salariés
- Assurer un pilotage de la conformité

La fonction de DPO peut être interne, c'est-à-dire exercée par un salarié de l'établissement sur 1/8e ou ¼ d'ETP par exemple ou externe c'est-à-dire confiée à un prestataire extérieur. Le DPO interne ou externe peut être également mutualisée entre plusieurs établissements.

S'il est interne, le DPO devra être rattaché directement au directeur à la direction de l'établissement.

⚠ Le DPO ne peut pas être un membre de la direction sous peine de **conflit d'intérêts.**

Le candidat à la fonction de DPO devra idéalement réunir les quatre compétences suivantes :

- Connaitre le droit de la protection des données
- Être à l'aise avec les systèmes d'information et leur sécurité
- Connaître les fondamentaux de l'assurance qualité
- Comprendre les métiers de l'établissement

Le DPO interne devra disposer d'une fiche de poste et d'une lettre de mission.

⚠ Les délégations de pouvoir au bénéfice du DPO ne sont pas admises. L'établissement, personne morale, reste seul responsable – notamment devant la CNIL – de sa conformité au RGPD.

La désignation du DPO se fait en ligne sur le site de la CNIL à l'adresse suivante
https://www.cnil.fr/fr/designation-dpo.

À RETENIR

L'établissement doit désigner son DPO dès le début de son projet de conformité au RGPD.

Le délégué à la protection des données
https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo

*Article 37 du RGPD

Fiche 4

ÉLABORER UN PROGRAMME DE CONFORMITÉ

La conformité au RGPD est un projet visant à atteindre rapidement un niveau cible de conformité notamment au travers de la réalisation d'une cartographie et le déploiement de différents outils de conformité, dont le registre et l'analyse d'impact.

Ce projet de mise en conformité au RGPD devra dès son début se construire en un programme de conformité qui aura vocation à se poursuivre une fois le projet terminé et sans limite de durée, au même titre que l'identitovigilance ou la sécurité des soins, par exemple.

☞ Ce programme empruntera aux exigences suivantes de la gestion de projet :

- Un chef de projet qui sera très logiquement le DPO interne ou externe (cf. fiche 3)
- Un comité de pilotage (cf. fiche 2)
- Des réunions projet périodiques animées en principe par le DPO, assorties d'un ordre du jour et d'un compte rendu systématique
- Un outil de travail collaboratif : messagerie d'équipe, agenda projet, espace de partage de fichier, etc.
- Un plan d'assurance qualité, logiquement élaboré par le DPO

☞ L'établissement de dotera également d'un plan projet/programme à vocation permanente, incluant notamment :

- Une liste des tâches programmées, divisées en sous-tâches, ainsi de suite
- Associé à une matrice des responsabilités
- Assortie d'un planning
- Géré à l'aide d'un tableur placé sur un espace partagé

Ce plan devra également organiser les actions programmées suivant des niveaux de priorité, en fonction des risques que font peser les traitements de l'établissement sur les droits et libertés des personnes concernées.

☞ Le plan programme devra être mis en cohérence avec les éventuels autres plans d'action de l'établissement :

- En premier lieu concernant ses systèmes d'information
- Également concernant ses programmes de certifications
- Ainsi que ses plans de progrès en matière d'assurance qualité, par exemple

À RETENIR

L'établissement aura intérêt à enregistrer son registre ainsi que l'ensemble de ses outils et de sa documentation de conformité dans des fichiers versionnés et verrouillés, et à placer ces fichiers sur un espace partagé et sauvegardé.

SE PRÉPARER EN 6 ÉTAPES :

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

Fiche 5

CARTOGRAPHIER LES TRAITEMENTS ET ÉTABLIR UN REGISTRE

Suivant le nouveau principe de responsabilité (cf. fiche 1), le RGPD a supprimé l'obligation de procéder à des formalités auprès de la CNIL préalablement à la mise en œuvre d'un traitement (déclarations ou autorisation selon le cas). En revanche, l'établissement sera tenu d'établir un registre des activités de traitement* afin d'être en mesure de documenter sa conformité et d'en justifier dans le cas où la CNIL lui en faisait la demande.

L'établissement du registre des activités de traitement nécessitera la réalisation préalable d'une cartographie des traitements. Cette tâche sera essentielle à la conformité de l'établissement.

L'objectif de cette cartographie sera d'identifier les traitements de données, les catégories de données traitées, les éventuels sous-traitants intervenant dans leur traitement et les personnes ayant accès aux données ou auxquelles elles sont communiquées en dehors de l'établissement.

☞ L'établissement emprunter une démarche consistant à croiser plusieurs sources d'information issues notamment :

- D'un échange avec les différents responsables des services métier ou support : comptabilité, ressources humaines, informatique, PCME, médecin coordinateur, etc. sur leurs pratiques
- Des documents concernant l'infrastructure informatique et de la liste des applications déployées (qui ne se confonde pas avec un traitement)
- Des procédures qualité et des certifications en cours ou déjà obtenues

L'Établissement pourra utilement consulter les différentes normes et dispenses de déclaration élaborées par la CNIL antérieurement au RGPD et qui constituent toujours des référentiels de bonnes pratiques. Il s'agit notamment de la norme simplifiée NS-046 concernant la gestion du personnel et l'autorisation unique n° AU-047 concernant l'accueil et l'hébergement des personnes handicapées ou des personnes âgées dépendantes.

Normes et dispenses adaptées par la CNIL
https://www.cnil.fr/fr/liste-des-normes-et-des-dispenses

Destiné à permettre à l'établissement de documenter la conformité de ses traitements, le registre sera aussi un outil de pilotage. L'établissement comptant moins de 250 salariés sera dispensé de faire figurer au registre ses traitements occasionnels comme l'envoi ponctuel d'invitations à un évènement.

☞ Le registre devra contenir les informations suivantes :

- Les parties intervenant dans le traitement des données, notamment le responsable du traitement et les sous-traitants
- L'objectif poursuivi par le traitement (la gestion administrative des patients par exemple)
- Les catégories de données traitées (identité, informations professionnelles, données de santé, etc.)
- Les personnes ayant accès aux données et celles à elles sont communiquées
- La durée de conservation des données
- Les mesures prises pour assurer la sécurité des données : contrôle d'accès, chiffrement, antivirus, etc.

Lorsque l'établissement interviendra comme sous-traitant, il devra tenir un registre spécifique à ses activités de sous-traitant. Le registre devra être actualisé au fil de l'eau. Cette tâche pourra être confiée au DPO (cf. fiche 3).

À RETENIR

Les petits établissements pourront efficacement tenir leur registre sur un tableur de type Excel protégé contre les modifications accidentelles et placé dans un espace partagé comme par exemple SharePoint.

Modèle de registre proposé par la CNIL
https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

*Article 30 du RGPD

Fiche 6

RÉALISER UNE ANALYSE D'IMPACT (PIA)

Les établissements sanitaires et médico-sociaux ont l'obligation de réaliser une analyse d'impact relative à la protection des données (AIPD/PIA[1]) concernant les traitements de données de santé qu'ils mettent en œuvre pour la prise en charge des personnes[2].

Il s'agira concrètement de la gestion administrative du malade/patient (GAM/GAP) et du dossier patient informatisé (DPI) pour les établissements sanitaires ou du dossier résident et du dossier de soins pour les établissements médico-sociaux.

Un PIA est un outil permettant de construire un traitement respectueux de la vie privée et de démontrer sa conformité au RGPD. Il est en partie basé sur une méthode **d'analyse de risques** éprouvée dans le domaine de la sécurité des systèmes d'information (EBIOS).

☞ Le PIA repose sur les deux piliers suivants :

- Les principes et droits fondamentaux, « non négociables », fixés par la loi. Le PIA viendra vérifier qu'ils s'imposent, quelles que soient la nature, la gravité et la vraisemblance des risques encourus
- Une analyse des risques sur la vie privée des personnes concernées, confrontés aux mesures techniques et d'organisation prévues pour protéger les données personnelles

☞ Concrètement, un PIA comprendra quatre volets de questions à renseigner :

- Le contexte du traitement (données, processus et les supports)
- Le respect des principes fondamentaux (nécessité, proportionnalité, protection des droits des personnes)
- Une évaluation des risques d'atteinte à la vie privée au regard des mesures de sécurité existantes
- Une conclusion incluant l'avis des personnes concernées et celui du DPO

☞ Le PIA est par essence un travail collaboratif qui réunira à l'échelle de l'établissement :

- Les responsables administratifs et médicaux ayant conçu ou choisi le traitement et qui le mettront en œuvre et qui auront la responsabilité de répondre aux questions
- Le DPO qui aura la tâche d'évaluer les réponses et de proposer d'éventuelles améliorations ; le DPO émettra, au final, un avis motivé sur la mise en œuvre ou pas du traitement
- Les représentants des patients / des résidents qui devront être consultés sur le PIA
- Le directeur agissant comme représentant du responsable du traitement qui validera ou pas le PIA et la mise en œuvre consécutive du traitement

Dans le cas où le PIA conclurait à un niveau de risque résiduel trop élevé nonobstant les mesures de protection prévues, l'établissement aura l'obligation[3] de consulter la CNIL avant toute mise en œuvre du traitement. L'établissement pourra conduire son analyse d'impact avec le logiciel PIA téléchargeable gratuitement sur le site de la CNIL :
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

⚠ Pour les traitements déjà existants à date d'entrée en application du RGPD, le PIA devra être réalisé au plus tard dans les trois ans, soit avant le 25 mai 2021, à la condition que le traitement concerné ait en son temps fait l'objet des formalités applicables auprès de la CNIL.

Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données
https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Voir également le guide de la CNIL figurant dans la bibliographie proposée à la fin de ce guide.

[1] Article 35 du RGPD.

[2] Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (JORF du n°0256 du 6 novembre 2018)

[3] Article 36 du RGPD

Fiche 7

INFORMER LES TITULAIRES DES DONNÉES

Le RGPD vient renforcer l'information[1] que l'établissement doit donner aux personnes concernées par ses traitements de données.

Concrètement, il s'agira principalement de l'information des patients ou des résidents et parfois leurs proches, des salariés de l'établissement, mais également des intervenants extérieurs, des personnes physiques représentants les fournisseurs, des contacts en relation avec l'établissement, des internautes visitant le site internet et dans certains cas les visiteurs.

Le RGPD exige que l'information soit complète et précise. Elle devra être également compréhensible et accessible.

Le RGPD ne prescrit pas de forme particulière pour l'information. L'établissement pourra par conséquent avoir recours au moyen le plus efficace compte tenu de son fonctionnement.

Concrètement, l'information figurera dans le livret d'accueil remis systématiquement lors de l'admission du patient ou de l'entrée d'un résident ; de même pour le livret d'accueil des salariés. Elle pourra faire l'objet d'un affichage dans l'établissement, à l'accueil ou aux admissions par exemple s'agissant des patients. L'information devra figurer obligatoirement le site internet s'agissant des visiteurs du site.

Il n'est ni requis ni nécessaire que l'information fasse l'objet d'une clause contractuelle. En revanche, le contrat d'hébergement et le contrat de travail, par exemple, pourront renvoyer au livret d'accueil.

L'information de la personne concernée devra porter sur les principaux points suivants :

- Identité et coordonnées du responsable du traitement, soit la personne morale administrant l'établissement
- L'objectif du traitement (à quoi vont servir les données collectées)
- La base légale du traitement de données, c'est-à-dire ce qui donne le droit à l'établissement de traiter les données parmi les six fondements mentionnés l'article 6 du RGPD, notamment une mission d'intérêt public, le respect d'une obligation réglementaire, l'exécution d'un contrat, etc.
- Les destinataires ou catégories de destinataires des données, c'est-à-dire qui accédera aux données ou les recevra, y compris les sous-traitants
- La durée de conservation des données, ou critères permettant de la déterminer)
- Les droits des personnes concernées : des droits d'accès, de rectification, d'effacement et à la limitation et dans certains cas le droit d'opposition et droit à la portabilité
- Les coordonnées du DPO, s'il a été désigné, ou d'un point de contact sur les questions de protection des données personnelles
- Le droit d'introduire une réclamation auprès de la CNIL

À RETENIR

L'information RGPD devra être clairement articulée avec celle concernant les droits du patient prévue par le code de la santé publique[2].

Comment informer les personnes et assurer la transparence
https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

Exemples de mention d'information
https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

[1] *Article 13 du RGPD*
[2] *Articles L1111-7 et R1111-1 du Code de la santé publique*

Fiche 8

ASSURER LA CONFORMITÉ DES RELATIONS AVEC LES SOUS-TRAITANTS

Le RGPD vient renforcer l'encadrement de la relation entre le responsable du traitement et le sous-traitant dont les obligations sont étendues. Le sous-traitant assume à présent une responsabilité qui lui est propre dans la protection des données.

Le sous-traitant au sens du RGPD est un fournisseur ou un prestataire bien particulier en ce qu'il traite des données pour le compte de l'établissement.

Parmi les sous-traitants de l'établissement, on trouvera en premier lieu les prestataires informatiques notamment en charge de l'hébergement et/ou de la maintenance des applications utilisées par l'établissement. Il s'agira également des prestataires de téléphonie ou ceux intervenant sur les dispositifs de téléphonie, badge et de vidéosurveillance.

Pourront-être des sous-traitants, certains fournisseurs/prestataire de restauration ou de lingerie dès lors qu'ils auront communication des noms des patients/résident ou des salariés. Pourront-être enfin avoir la qualité de sous-traitants au sens du RGPD, les professionnels de santé extérieurs, y compris les pharmacies, les laboratoires de biologie, les cabinets de radiologie et les fournisseurs de dispositifs médicaux adaptés au patient.

Le RGPD impose à présent que le responsable du traitement (l'établissement) formalise par écrit* les huit clauses suivantes aux termes desquelles le sous-traitant (en synthèse) :

- Ne traite les données à caractère personnel que sur instruction du responsable du traitement
- Veille à ce que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité
- Prend toutes les mesures de sécurité de son système d'information requises par le RGPD
- Ne recrute pas lui-même un sous-traitant sans l'autorisation du responsable du traitement et sans imposer lui-même à son sous-traitant les mêmes clauses que celles auxquelles il est tenu
- Aide le responsable du traitement à répondre aux demandes des personnes concernées (cf. fiche 9)
- Aide le responsable du traitement à garantir l'information des personnes concernées (cf. fiche 6)
- Au choix du responsable du traitement, supprime toutes les données ou les lui renvoie au terme de la prestation, et détruit les copies existantes
- Met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations et pour permettre la réalisation d'audits

S'agissant des contrats de sous-traitance en cours, l'établissement aura intérêt à procéder à une revue des contrats et avenants RGPD reçus par l'établissement à l'aide d'une grille d'audit construite sur la base de la liste des clauses ci-dessous. En cas de non-conformité, les sous-traitants devront être fermement invités à proposer un avenant conforme.

L'établissement pourra utilement se doter un tableau de pilotage de ses contrats de sous-traitance qui sera annexé à son registre des activités de traitement (cf. fiche 4).

Ce qui change pour les sous-traitants
https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

Voir également le guide de la CNIL consacré aux sous-traitants figurant dans la bibliographie proposée à la fin de ce guide.

*Article 28 du RGPD

Fiche 9

LIMITER LA CONSERVATION DES DONNÉES

La durée de conservation des données à caractère personnel détenues par l'établissement est un sujet important de la conformité au RGPD.

⚠ Cette fiche n'a pas pour sujet vocation à recenser les durées légales de conservation qui dépendront des informations et des supports concernés ainsi que du statut de l'établissement. Elle a en revanche pour objectif de présenter les principes propres du RGPD en la matière et leur mise en œuvre sur un plan pratique.

La question des durées de conservation des données au regard du RGPD devra être gérée en étroite collaboration avec la fonction qualité dans l'établissement.

Le RGPD pose le principe que les données à caractère personnel ne peuvent être conservées que pour la durée strictement nécessaire aux finalités pour lesquelles elles ont été collectées. L'établissement ne pourra conserver ces données que dans le cadre d'un archivage sécurisé, pour une durée prévue par la loi et dans un objectif très précis par exemple permettre à l'établissement d'assurer en justice sa défense en cas de mise en cause de sa responsabilité.

👉 En résumé, une application conforme du RGPD impliquera la gestion de trois phases :

- Le traitement est en cours : la donnée figure dans le dossier actif
- Le traitement est terminé : la donnée est placée en archive sécurisée
- L'archivage est terminé : la donnée supprimée (sauf si basculée en archives publiques dites «définitives»)

Pour mémoire : la CNIL demande que les données figurant au dossier de soins soient archivées dans un délai de 5 ans[1] à compter de la dernière intervention sur le dossier médical puis conservées 15 ans, soit 20 ans[2] au total.

⚠ Une durée indéterminée ou non renseignée sera assimilée à une durée illimitée qui constituerait une violation des principes et des règles du RGPD.

👉 L'archivage sécurisé devra répondre aux exigences suivantes :

- Être sélectif : il ne doit concerner que les données nécessaires à la finalité de l'archivage
- D'accès restreint aux personnes ayant besoin d'en connaître au regard de la finalité, tout accès devra être autorisé par un responsable désigné et tracé
- Au plan technique, être situé sur une base distincte de la base active physiquement ou sinon logiquement

À RETENIR

L'établissement aura fort intérêt sur le plan de sa conformité au RGPD à se doter d'une politique d'archivage et de tableaux de gestion.

Limiter la conservation des données
https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

Recommandation de la CNIL sur l'archivage électronique dans le secteur privé[3]
https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651957

[1] *Norme simplifiée NS-050 : https://www.cnil.fr/fr/declaration/ns-050-cabinet-medical-et-paramedical*
[2] *Article R 1112-7 du Code de la santé publique*
[3] *Délibération n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel*

Fiche 10

ÉTABLIR LES PROCÉDURES ESSENTIELLES

Si le RGPD n'impose pas l'établissement des deux procédures objet de cette fiche, elles constituent de bonnes pratiques que l'établissement pourra très utilement suivre. Elles lui permettront à la fois de s'assurer de bien réagir face à certaines demandes ou évènements, mais également de justifier, en cas de contestations, du sérieux de sa démarche de conformité.

Ces procédures essentielles seront en principe et a minima les deux suivantes :

- Comment réagir en cas de demande d'une personne concernée par le traitement (DPC) ?
- Comment réagir en cas d'atteinte aux données ?

La procédure de gestion des demandes des personnes concernées devra contenir notamment les informations suivantes :

- Les rôles et responsabilités au sein de l'établissement dans la prise en charge des demandes (responsable informatique, médecins, DPO, etc.)
- Les vérifications à opérées concernant la recevabilité du demandeur
- Une typologie des demandes (accès, effacement, etc.) et les actions à réaliser en fonction (recherches, copies, etc.)
- Les modalités de communications des données au demandeur
- Les délais de réponse à respecter

La procédure sera complétée par un tableau des demandes (souvent désigné « registre des DPC ») permettant une documentation et un pilotage des demandes satisfaites et des demandes en cours.

Comment répondre à une demande de droit d'accès ?
https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-dacces

La procédure de gestion des atteintes aux données devra contenir notamment les informations suivantes :

- Les rôles et responsabilités au sein de l'établissement dans la prise en charge des demandes (responsable informatique, médecins, DPO, etc.)
- Les types d'évènements susceptibles de constituer une atteinte aux données à caractère personnel
- La procédure de notification à la CNIL, et le cas échéant aux personnes concernées, et ses délais

L'établissement devra en effet signaler une violation à la CNIL dans les 72 heures si celle-ci est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Si ces risques sont élevés, l'établissement devra également les informer.

La rédaction de cette procédure devra être conduite en très forte proximité avec la fonction informatique de l'établissement.

À RETENIR

La procédure de gestion des atteintes aux données devra être clairement articulée avec celle concernant l'information du directeur général de l'ARS en cas d'évènement indésirable concernant le système d'information de l'établissement.

Cette procédure devra également s'accompagner d'une main courante des évènements (souvent désigné « registre des atteintes ») destinée à documenter les notifications effectuées par l'établissement. Elle reprendra l'ensemble des rubriques figurant dans la notification à la CNIL.

Notifier une violation de données personnelles
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Annexe 1

GLOSSAIRE

Nous avons choisi de ne faire figurer ci-dessous les définitions du RGPD* utiles à la compréhension du présent guide.

DONNÉE À CARACTÈRE PERSONNEL

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

DONNÉES CONCERNANT LA SANTÉ

Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

TRAITEMENT DE DONNÉES

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

RESPONSABLE DU TRAITEMENT

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

SOUS-TRAITANT

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traitent des données à caractère personnel pour le compte du responsable du traitement.

DESTINATAIRE

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoivent communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

BIBLIOGRAPHIE

Annexe 2

La liste ci-dessous n'est pas exhaustive et se limite aux sujets directement en lien avec le présent guide.

Mémento RGPD à l'usage du directeur d'établissement – DGOS, 25 juin 2019
https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/memento-rgpd

Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises
BPI France Le Lab - Commission Nationale Informatique et Libertés (CNIL) – avril 2018
https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf

Le Guide du sous-traitant – Commission Nationale Informatique et Libertés (CNIL), édition septembre 2017
https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

La sécurité des données personnelles - – Commission Nationale Informatique et Libertés (CNIL), édition 2018
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

GUIDE DE L'HYGIÈNE INFORMATIQUE – RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 2017
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)
1. La Méthode - Commission Nationale Informatique et Libertés (CNIL), février 2018
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)
2. Les modèles - Commission Nationale Informatique et Libertés (CNIL), février 2018
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)
3. Les bases de connaissances - Commission Nationale Informatique et Libertés (CNIL), février 2018
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf

UNE QUESTION ?

rgpd@fehap.fr