SE FAMILIARISER AVEC LE RGPD

(REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES)

KIT D'INFORMATION A DESTINATION DES ETABLISSEMENTS MEDICO-SOCIAUX

LES EDITIONS DE LA FEDERATION HOSPITALIERE DE FRANCE

FICHES PRATIQUES

VERSION n°1

SEPTEMBRE 2018

FÉDÉRATION HOSPITALIÈRE DE FRANCE

PREAMBULE

Le Règlement général pour la protection des données à caractère personnel (RGPD) est entré en application le 25 mai 2018. Ce texte impose désormais aux organismes publics et privés des règles plus strictes pour le traitement et la conservation des données à caractère personnel des individus. Le RGPD s'appliquant à toute personne morale ou physique, il appartient désormais aux ESMS de se conformer aux exigences renforcées par l'entrée en vigueur de cette nouvelle règlementation.

La loi informatique et libertés a été modifié par la loi ***n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.***

Dès lors, vous vous posez sûrement de nombreuses questions :

- *Quels sont les enjeux et les impacts du RGPD dans le secteur médico-social ?*
- *Quelles règles sont applicables au sein des ESMS et quelles sont leurs responsabilités dans le traitement et la conservation des données à caractère personnel ?*
- *Quelles démarches un ESMS doit-il entreprendre afin de se conformer au RGPD ?*
- *Qu'est-ce qu'une donnée à caractère personnel ?*
- *Qu'est-ce qu'un traitement de données ?*
- *Qu'est-ce qu'un DPD ? Les ESMS sont-ils concernés ?*

Ce guide vous permettra de répondre à ces questions et de mieux connaître les obligations des établissements médico-sociaux (ESMS).

Un ESMS est susceptible de collecter et de traiter des données personnelles d'ordre divers, à savoir des données RH, des données de santé relatives à la santé des résidents et sur leurs familles, etc.

La collecte, l'utilisation et l'accès à ces données est réglementé par le RGPD. Il en est de même de leur conservation. De plus, le RGPD est appelé à s'appliquer à de très nombreux domaines de la société et est susceptible de vous concerner individuellement dans des droits que vous serez susceptible d'exercer sur vos données personnelles : par exemple en tant que consommateur dans la vie de tous les jours ou utilisateur des réseaux sociaux. Ainsi, ce guide vous permettra de mieux appréhender le RGPD et les données personnelles dans et au-delà du secteur médico-social.

Le présent guide est constitué de façon gradué, avec des fiches allant de 1 à 10, vous permettant de progresser par étape pour comprendre le RGPD et l'adapter à votre établissement.

SOMMAIRE

Vos avis et questions complémentaires sont les bienvenus, n'hésitez pas à nous les transmettre sur question.autonomie@fhf.fr

FICHE 1

ENJEUX, IMPACTS DU RGPD

DEFINITIONS CLES

Dans un contexte actuel favorable à une massification des échanges de données grâce au développement du numérique, la législation s'adapte pour suivre les évolutions de notre société. **Le RGPD** s'inscrit dans la continuité de la loi française Informatique et Libertés de 1978 et **vient donc encadrer le traitement des données à caractère personnel et renforcer le contrôle sur leur utilisation.**

Qu'est-ce qu'une donnée à caractère personnel ? (Art 4.1 du RGPD)

Une donnée à caractère personnel ou donnée personnelle est une **information** sur une **personne physique**. Cette **information** (ou **plusieurs informations regroupées ensemble**) peut permettre **d'identifier directement** ou **indirectement** la personne.

Exemples de données à caractère personnel : nom, sexe de l'individu, photographie, données bancaires, numéro de sécurité sociale, opinions politiques, orientation sexuelle, …

L'actualité récente a démontré la nécessaire vigilance qu'il convient d'accorder à la divulgation des données à caractère personnel face à la recrudescence des cyber-attaques et au risque de détournement de ces données à des fins commerciales. **Le secteur de la santé et du médico-social** n'est pas épargné par ces actes et **est à fortiori, une cible privilégiée de ces menaces car il collecte des données à caractère personnel très sensibles, à savoir les données personnelles en santé.**

Qu'est-ce qu'une donnée personnelle en santé ? (Art 4.1 du RGPD)

Les données personnelles en santé sont des « 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 les informations sur l'état de santé** de cette personne ».

Exemples de données personnelles en santé : antécédents médicaux, un numéro ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé, informations obtenues lors de l'examen d'une partie du corps, …

Cette réglementation s'impose aux ESMS et aux prestataires qu'ils emploient (professionnels de santé, entreprises chargées de la maintenance, de la logistique etc). **Les établissements doivent donc garantir le plus haut niveau de protection des données et prendre les mesures appropriées afin d'assurer leur conservation et leur confidentialité.**

FICHE 1

LES ENJEUX ET IMPACTS DU RGPD

DEFINITIONS CLES

Ce nouveau cadre juridique n'impose pas de déclarer les données à la CNIL. Désormais, la réglementation impose aux établissements d'apporter la preuve de leur mise en conformité.

Pour assurer le respect de la mise en œuvre du RGPD, la CNIL se voit doter d'une pluralité d'attributions :

- Enquêtes
- Audits de protection des données
- Accès aux locaux et aux données
- Possibilité de prononcer des sanctions administratives

Le RGPD réaffirme cinq grands principes (précités) de loi Informatique et libertés. Par ailleurs, il introduit les points suivants :

- Les conditions du consentement (Art. 7) : tout traitement de données à caractère personnel nécessite un consentement préalable, recueilli par le responsable du traitement. Ce dernier doit en apporter la preuve.
- Le droit à l'oubli (Art. 17) : dans certains cas énoncés à l'Art.17, tout citoyen peut exiger l'effacement de ses données personnelles dans les meilleurs délais.
- Le droit à la portabilité (Art.20) : toute personne peut demander la réception de ses données et leur transmission à un autre responsable de traitement.
- La responsabilisation (Art.24) : le responsable du traitement (le directeur d'établissement) doit être en mesure de démontrer la conformité de ces traitements au RGPD.
- La notification aux personnes concernées (Art.33) : toute violation de données doit être notifiée par les établissements aux personnes concernées et à la CNIL (dans les 72h après en avoir pris connaissance), si celle-ci est susceptible un risque élevé pour les droits et libertés personnes physiques.

FICHE 1

LES ENJEUX ET IMPACTS DU RGPD

DEFINITIONS CLES

En cas de manquement dans la protection des données, les textes prévoient des sanctions financières. A titre informatif, les amendes peuvent aller jusqu'à 20 millions d'euros, ou 4% du chiffre d'affaire mondial annuel si cette seconde valeur est supérieure. Les sanctions administratives **peuvent être complétées par des condamnations pénales** prévues aux articles 226-16 et suiv. et R625-10 et suiv. du Code pénal. Toute violation du RGPD peut : engager la responsabilité du responsable du traitement (préjudice moral et matériel subi par la personne concernée), entrainer une **perte de confiance des usagers** envers l'établissement et porter atteinte à son image.

Réglementation :

- RGPD Article 58, nouvelles attributions de la CNIL
- RGPD Article 4.1
- Loi informatique et libertés de 1978, article 2

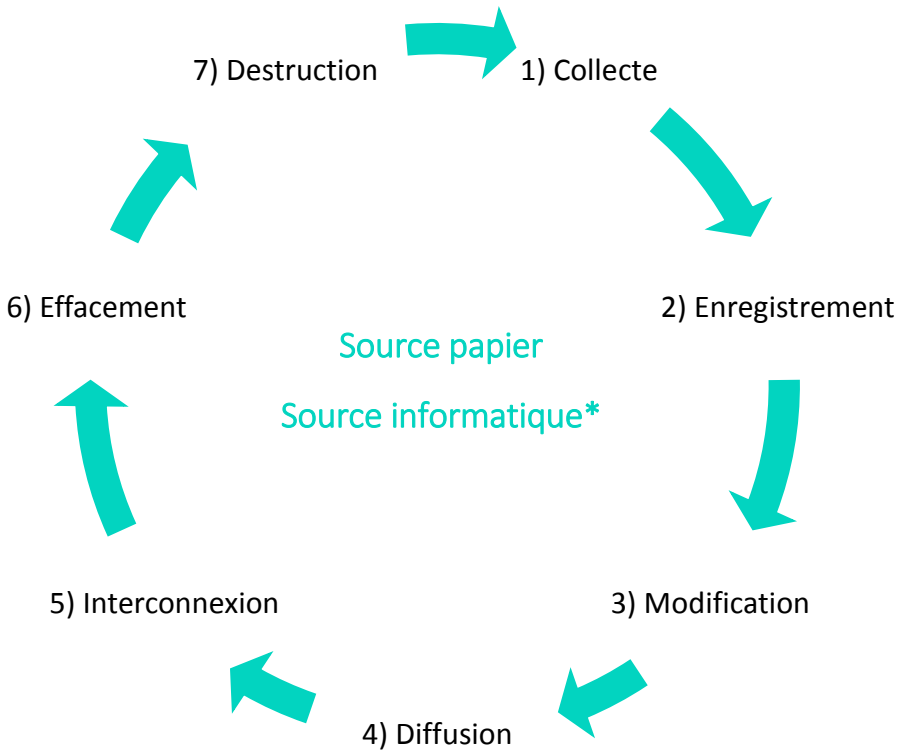
FICHE 2

LA COLLECTE ET LE TRAITEMENT DE DONNEES

Lorsqu'un organisme traite des données personnelles, il est qualifié de « **Responsable du traitement** ». Le **directeur d'un établissement médico-social** en sa qualité de représentant de l'établissement est le responsable du traitement.

Selon l'**article 4 du RGPD**, est un traitement de données personnelles :

*« 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** ».*



**Il est important de noter que le RGPD s'applique aussi bien aux données personnelles sur support papier que sur support informatique.*

FICHE 2

LA COLLECTE ET LE TRAITEMENT DE DONNEES

A titre d'exemple et pour illustrer la définition de l'article 4 du RGPD, lorsqu'un résident ou un salarié communique à l'établissement des données personnelles (carte d'identité, RIB, nom, prénom, n° de téléphone, etc.), ce dernier les collecte. Ces informations peuvent par la suite être retranscrites sur un logiciel informatique (tableau excel par exemple, dossier résident informatisé), numérisées, retranscrites sous format papier ou rangées dans un dossier papier. Les données peuvent alors être organisées ou structurées puis conservées (dans une armoire si dossier papier, sous logiciel informatique si les données sont informatisées, etc.). Le fichier contenant les données pourra ensuite être modifié (suppression, mise à jour d'une donnée). De même, ce fichier pourra être consulté par toutes les personnes autorisées et être transmis à des tiers ou à une autre personne de l'organisme (le fichier est envoyé par courriel par exemple). Enfin, ce fichier pourra être détruit par la personne qui l'a créée (par exemple, l'établissement décide de détruire le fichier car elle n'a plus besoin des informations qui s'y trouvent).

L'activité d'un établissement nécessite de nombreuses données personnelles qui sont réglementées par le RGPD :

Par exemple, lorsqu'un établissement recrute un/une infirmier(ère), l'établissement demandera au nouveau salarié de lui communiquer plusieurs données personnelles : RIB, carte d'identité, diplôme, numéro de sécurité sociale etc.

Le traitement de ces informations aura une ou plusieurs finalités : permettre par exemple à l'établissement de rémunérer le salarié, d'effectuer les démarches nécessaires pour les déclarations sociales obligatoires, etc.

L'établissement ne peut cependant collecter que les données personnelles qui sont « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Ainsi, l'établissement ne peut demander comme condition sine qua non au recrutement, des informations qui ne seront pas utiles pour le recrutement du salarié : par exemple les opinions politiques, les convictions religieuses, etc.

De même, **lorsqu'un établissement dispose d'un système sous surveillance vidéo** (vidéosurveillance ou vidéo protection), **un tel système, précise la CNIL, ne peut « être utilisé pour s'assurer que le personnel fait correctement son travail ».** En effet, un tel système doit avant tout être mis en place pour garantir la sécurité des biens et des personnes.

FICHE 2

LA COLLECTE ET LE TRAITEMENT DE DONNEES

Données relevées comme sensible au sens du RGPD, **le traitement des données de santé est *a priori* interdit et n'est autorisé que sous certaines exceptions : traitement dans le cadre de la gestion des soins, des systèmes de santé, etc.** Dans le cadre de la prise en charge et du suivi médical des résidents, **l'établissement collecte et traite donc des données de santé à caractère personnel pour lesquelles, il doit garantir un niveau de sécurité maximale.**

« Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.
Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (9) au bénéfice de cette personne physique;

- *un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé;*
- *des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques;*
- *et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro. »*

Les données que vous collectez doivent respecter les principes du RGPD. Elles doivent être adéquates, pertinentes et limitées au traitement.

Réglementation :

- RGPD Article 4 et 9
- Loi informatiques et libertés Article 2

FICHE 3

IDENTIFIER LES PERSONNES SUSCEPTIBLES DE COLLECTER/TRAITER DES DONNEES PERSONNELLES

En ESMS, plusieurs personnes, de différents services sont susceptibles de traiter des données personnelles : *le directeur de l'établissement, les professionnels administratifs, hôteliers, techniques, de santé, d'animation, d'accueil, ainsi que le responsable informatique et les prestataires avec qui l'établissement échange des données.*

Dans un contexte de fluidité du parcours patient, de développement du numérique en santé, de l'essor de l'interopérabilité des systèmes d'informations, de déploiement des structures de coopération et de décloisonnement entre les professionnels, on fait face à une multiplication des acteurs collectant, traitant, échangeant et accédant aux données personnelles en santé.

Pour autant, force est de constater que plus il y a d'acteurs concernés, plus il y a de risques de divulgation de l'information.

Quelles données personnelles ces fonctions et services sont susceptibles de traiter ?

Médecin coordonnateur	Données relatives à la santé du résident Données relatives à la pathologie, au diagnostic, à la prescription
Ressources humaines	Données relatives aux salariés de l'établissement Données telles que le RIB, la carte d'identité, le diplôme, l'expérience professionnelle, la rémunération…
Personnel d'accueil	Données relatives aux visiteurs Données telles que le nom, le prénom, la date et l'heure de la visite, le lien familial avec le résident…
Référent information / sécurité	Images de vidéo-surveillance/vidéo protection

FICHE 3

IDENTIFIER LES PERSONNES SUSCEPTIBLES DE COLLECTER/TRAITER DES DONNEES PERSONNELLES

Lorsque les différents services d'un établissement traitent et conservent des données personnelles, seules certaines personnes doivent être autorisées à accéder à ces données.

Une personne ne peut être autorisée à accéder qu'aux données qui lui sont nécessaires pour exercer sa fonction :

- Par exemple, le médecin coordonnateur ne peut accéder aux données qui concernent la rémunération d'un salarié, sa situation matrimoniale, son adresse, etc. Ces données sont conservées et traitées par le service ressources humaines et seul ce service a le droit d'accéder à de telles données personnelles.
- De même, les personnes travaillant dans le service des ressources humaines, administratif, accueille, etc. ne peuvent accéder aux images de vidéosurveillance/vidéo protection. Seul des personnes habilitées peuvent accéder à ces données, comme par exemple un référent sécurité, peuvent accéder à ces données

Rappel : le traitement doit avoir une finalité, ne collectez que les données personnelles dont vous avez besoin. Si les informations que vous collectez n'ont aucun lien avec le traitement que vous souhaitez en faire, ne les collectez pas.

Réglementation :

- RGPD Article 5
- Loi informatiques et libertés Article 6

FICHE 4

FOCUS SUR LE CONSENTEMENT

Pour être licite, un traitement doit trouver son fondement dans l'une des conditions prévues à l'article 6 du RGPD. Le consentement constitue l'une des bases légales pouvant constituer ce fondement, mais souffre d'exceptions et ne doit pas être systématiquement recueilli. En effet, un traitement peut être licite en trouvant un autre fondement que le consentement.

Toutefois, vous devez pour chaque traitement informer les personnes concernées.

En dehors du consentement, le traitement peut être licite lorsque :

- Il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (Ex* : contrat de vente, de travail, devis etc.). Autres exemples : gestion de paie, etc.
- Lorsque le traitement de données vient en complément d'un contrat mais n'est pas nécessaire à son exécution, la personne doit être libre de ne pas consentir au traitement sans que cela impact la bonne exécution du contrat*. Par exemple, si vous souhaitez utiliser le nom, le prénom et la photo du salarié pour mettre ces informations sur le site internet de l'établissement à titre de publicité, vous devez demander l'accord du salarié. Si celui-ci refuse, cela ne doit pas nuire à l'exécution de son contrat de travail.
- Il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (ex* : le registre du personnel, etc.).
- Il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (ex* : en cas d'épidémie, dans les situations de catastrophe naturelle ou d'origine humaine, etc.).
- Il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (ex* : constitution de fichiers de police, de l'administration fiscale, etc.).
- Il est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (ex* : la prévention de la fraude, les transferts au sein d'un groupe, la sécurité des réseaux, etc.)

FICHE 5

INFORMER LES RESIDENTS ET VOS SALARIES SUR LES DROITS DONT ILS DISPOSENT SUR LEURS DONNEES PERSONNELLES

Informez vos salariés ainsi que les résidents des traitements que vous effectuez et droits dont ils disposent. *L'article 5 du RGPD précise que les données doivent être traitées « de manière licite, loyale et transparente ».* Cette information peut se faire sur divers supports dont par exemple, par voie d'affichage (règlement de fonctionnement par exemple), remise de documents, annexes, mention dans le contrat de travail ou le contrat de séjour, etc.
Cette information doit être fournie en des termes simples, compréhensibles et doit être facilement accessible (adaptez la communication de l'information en fonction des personnes).

Selon l'article 13 du RGPD cette information doit comporter les éléments suivants :

- **L'identité et les coordonnées du responsable du traitement** (à savoir en ESMS le directeur de l'établissement)
- **Le cas échéant, les coordonnées du délégué à la protection des données** ;
- **Les finalités du traitement** auquel sont destinées les données à caractère personnel ainsi que la **base juridique du traitement** (La base juridique est ce qui autorise le traitement par exemple information collectée via le consentement de la personne, dans le cadre de l'exécution d'un contrat, etc.)
- **Les destinataires des données** personnelles (Quelles sont les personnes qui peuvent accéder à ces données ?) ;
- **La durée de conservation des données** à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- **L'existence du droit de demander** au responsable du traitement l'accès aux données à caractère personnel, **la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;**
- **Dans certains cas le droit de demander l'effacement** des données personnelles ;
- **Le droit d'introduire une réclamation auprès de la CNIL** ;
- Des informations sur la question de **savoir si l'exigence de fourniture de données** à caractère personnel **a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat** et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données :

Réglementation :

- RGPD Article 6 et 7
- Loi informatiques et libertés Article 7
- RGPD Article 13

*Les exemples relèvent d'une publication internet de la CNIL : Règlement européen : le consentement est-il obligatoire ? https://www.cnil.fr/fr/cnil-direct/question/1308

FICHE 6

ADAPTER LA CONSERVATION DE VOS DONNEES

L'établissement peut conserver les données personnelles pour une durée n'excédant pas celle nécessaire aux finalités du traitement.

La durée de conservation des données personnelles peut être défini par la loi, ou en cette absence, il appartient au responsable du traitement de définir les modalités de conservation des données au regard de la nature des données personnelles et de la finalité du traitement.

Certains textes peuvent imposer des durées de conservation précises :

- 1 mois pour les images de vidéosurveillance (2)
- 20 ans à compter de la dernière consultation du patient pour le dossier médical (3)
- 10 ans à compter de la date de décès, lorsque le patient est décédé moins de 10 ans avant son dernier passage en établissement ;

Lorsque la finalité du traitement est atteinte, vous pouvez (4) :

- Effacer les données ;
- Archiver les données (pendant une durée nécessaire à la réalisation du traitement) ;
- Anonymiser les données afin qu'elles ne puissent pas être identifiées. La technique de l'anonymisation peut notamment être utile selon la CNIL pour utiliser les données à des fins de statistique

Par exemple en établissement :

- Lorsqu'un salarié quitte votre établissement, le service ressources humaines conservera pendant 5 ans les fiches de paies ;
- Lorsque vous avez donné une réponse négative à un candidat, et que le candidat ne vous a pas informé de son intention de détruire son dossier de candidature, vous ne pouvez conserver le dossier que pendant 2 ans ;
- Lorsqu'un résident décède en établissement vous pouvez conserver son dossier médical pendant 10 ans à compter de la date du décès.

Réglementation :

- RGPD c) Article 5
- Loi informatiques et libertés 5° Article 6

FICHE 7

SECURISER VOTRE SYSTEME INFORMATIQUE ET VOS LOCAUX

Le RGPD s'applique aux **données papiers et informatiques**. Ces données personnelles sont vulnérables et ne doivent pas subir d'incidents de sécurité : perte, accès non-autorisé, virus informatique, etc. C'est pourquoi, ces données doivent faire l'objet de mesures de sécurité adaptées.

L'article 32 du RGPD, des mesures techniques et organisationnelles doivent être prises afin de garantir un niveau de sécurité adapté au risque.

La CNIL recommande de recenser les différents traitements effectués et les supports sur lesquels sont conservées les données. Ce recensement vous permettra d'anticiper les différents risques :

- Accès non autorisés ;
- Vol de données et utilisation illicite (par exemple à la suite du piratage du système informatique) ;
- Divulgation des données personnelles (exemple divulgation des données bancaires, de sécurité sociale, de données de santé)
- Modifications des données non prévues dues par exemple à un accès non autorisé ;
- Disparition des données due par exemple à une défaillance informatique ;
- Cambriolage.

Les données peuvent être stockées :

- Sur des ordinateurs, des serveurs, des disques durs,
- Des clés USB, etc.
- Lorsque les données figurent sur support papier : dans des classeurs, des armoires, etc.

Pour protéger l'accès aux données personnelles stockées sur support :

1) **Limitez l'accès aux différents supports de stockage** : Les utilisateurs ne doivent avoir accès qu'aux données dont ils ont strictement besoin pour l'exercice de leur mission (le responsable RH a accès aux données RH, le médecin coordonnateurs et l'ensemble du personnel médical aux données médicales qui leur sont strictement nécessaires, le directeur d'établissement et le référent informatique aux données de vidéosurveillance et de vidéo protection)

2) **Appliquez des mots de passe pour accéder à vos ordinateurs et à vos dossiers**. Les mots de passe doivent être les plus complexes possibles (lettre majuscule, chiffres, caractères spéciaux). Ne communiquez pas vos mots de passe à des tiers. Stockez-les de manière très sécurisée.

FICHE 7

SECURISER VOTRE SYSTEME INFORMATIQUE ET VOS LOCAUX

3) **Mettez en place un historique des consultations** afin d'identifier si des personnes non autorisées ont accéder à un dossier.

4) **Sécurisez le plus possible vos postes de travail, votre réseau internet** (anti-virus, pare-feu, mises à jour régulières).

5) **N'autorisez pas l'accès de certains fichiers**, données sur certains supports (téléphone mobile par exemple).

6) **Effectuez des sauvegardes régulières.**

7) **Protéger et limitez l'accès aux locaux** (accès par badge limité, accès limité aux armoires contenant des données personnelles papier, prévoir un accès limité et des procédures lorsque des personnes tierces ont accès à des locaux sensibles, plombier qui doit accéder à une pièce à la suite d'une panne par exemple).

8) **Protéger l'archivage et les habilitations pour accéder aux archives.**

9) **Sécurisez vos locaux contre les intrusions non-autorisées et informez votre personnel sur les risques encourus.**

FICHE 8

ELABORER UN REGISTRE DE TRAITEMENT DE DONNEES

Le registre des activités de traitement est prévu par *l'article 35 du RGPD.*

Ce registre permet de recenser les différents traitements et d'identifier :

- Les catégories de données traitées
- Les activités pour lesquelles les données sont traitées
- Les objectifs poursuivis par le traitement
- Les catégories de personnes concernées
- D'identifier la sensibilité des données personnelles
- La durée de conservation des données
- Les destinataires des données
- Et les mesures de sécurité adaptées

Le registre peut vous aider à mieux gérer la conformité de l'établissement au RGPD. Il facilitera l'établissement de la preuve de la conformité de l'établissement au RGPD.

Un exemple type de registre est disponible sur le site internet de la CNIL https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

FICHE 9

DESIGNER UN DELEGUE A LA PROTECTION DES DONNEES

Pilote du dispositif de protection des données personnelles au sein de l'organisme, le **délégué à la protection des données** (DPD ou *DPO en anglais)* s'impose aux organismes publics (article 37 du RGPD), et doit donc **obligatoirement être désigné dans un ESMS public**.

Qu'est-ce qu'un DPD ?

L'article 38 du RGPD précise que le DPD est associé à toutes les questions relatives à la protection des données à caractère personnel. De plus, selon l'*article 39 RGPD* le DPD :

Délégué à la protection des données

- **informe et conseille** le responsable du traitement ainsi que les salariés qui procèdent au traitement sur leurs obligations en matière de traitement des données.

- **contrôle** le respect du RGPD et de la loi informatique et libertés en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- **dispense** des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifie l'exécution de celle-ci ;

- **coopère** avec la CNIL ;

- **fait office de point de contact** pour la CNIL sur les questions relatives au traitement, etc.

L'établissement peut nommer un DPD interne à l'établissement, mais il est possible pour plusieurs établissements de mutualiser un DPD. Le DPD avoir doit des « **connaissances spécialisées du droit et des pratiques en matière de protection des données** », article 37.5 du RGPD.

La fonction de DPD ne doit pas donner lieu à **conflits d'intérêts**. La CNIL précise qu'il ne peut occuper au sein de l'organisme « des fonctions au sein de l'organisme le conduisant à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »). L'existence d'un conflit d'intérêts est donc appréciée au cas par cas » (**https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees**). Par exemple, le responsable RH ne peut être DPD, etc.

FICHE 10

POUR ALLER PLUS LOIN, FOCUS SUR L'APPLICATION DU RGPD DANS LA VIE DE TOUS LES JOURS

Le RGPD s'applique à de nombreux pans de la vie quotidienne. Chaque individu transmet au quotidien de nombreuses données personnelles. Le RGPD entend règlementer la collecte et le traitement de ces données : une personne doit savoir pourquoi un commerçant souhaite collecter certaines données, dans quelle mesure il compte utiliser les données, combien de temps il les conservera, etc.

- *En tant que consommateur*

Lorsqu'un commerçant vous propose une carte de fidélité, vous transmettez des données personnelles. Ces données seront traitées par le commerçant. Par exemple, celui-ci utilisera votre adresse postale pour vous envoyer des promotions à votre domicile.
Autre exemple, lorsque vous passez une commande sur internet, vous transmettez des données personnelles : nom, prénom, adresse mail, adresse postale, numéro de carte bleue etc.
Ces informations seront par exemple utilisées pour passer la transaction, livrer votre colis à l'adresse demandée.

De même, l'utilisation des données personnelles dans le commerce fait au quotidien l'actualité, au fil des évolutions technologiques. Dernièrement, la CNIL s'est intéressée aux enceintes connectées (5). Ces dernières ne sont censées collecter et traiter des données personnelles que pour certaines finalités bien précises (une parole est prononcée pour être retranscrite et donner une réponse adaptée, par exemple l'utilisateur demande à l'enceinte de chercher et de lancer un morceau de musique ou alors de fournir la météo du jour). Ces enceintes ne doivent pas enregistrer les conversations des utilisateurs à leur insu (bien que connectée, l'enceinte ne doit pas enregistrer une conversation à l'intérieur du foyer pour ensuite réutiliser les informations).

- *Utilisateur des réseaux sociaux et des applications mobiles*

En tant qu'utilisateur des réseaux sociaux et/ou applications de téléphones mobiles, vous transmettez des données personnelles.
Par exemple, lorsque vous installez une application sur votre téléphone portable, cette application sera amenée à collecter des données personnelles (géolocalisation, nom, prénom, etc.).
Le RGPD impose que ces données personnelles soient collectées avec votre consentement.

- *En tant qu'assuré, etc.*

DOCUMENTATIONS ET LIENS UTILES

1. Vidéosurveillance de la voie publique et des lieux ouverts au public
   https://www.service-public.fr/particuliers/vosdroits/F2517

2. Article R1112-7 du Code de la santé publique
   https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=3315B1101FCBF5CA86B52E539C094FC8.tplgfr21s_2?idArticle=LEGIARTI000036658351&cidTexte=LEGITEXT000006072665&categorieLien=id&dateTexte

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

5. Enceintes intelligentes : des assistants vocaux connectés à votre vie privée
   https://www.cnil.fr/fr/enceintes-intelligentes-des-assistants-vocaux-connectes-votre-vie-privee

En complément du guide : Fiche pratique élaborée par la DGCCRF sur le RGPD, « Protection des données personnelles : quelles sont vos droits ? », septembre 2018
https://www.economie.gouv.fr/files/files/directions_services/dgccrf/documentation/fiches_pratiques/fiches/RGPD-septembre-2018.pdf