Ordre national des pharmaciens

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

GUIDE PRATIQUE

Le pharmacien d'officine et la protection des données personnelles

Mai 2023

Table des matières

Avant-Propos

La Commission nationale de l'informatique et des libertés (CNIL) a publié en juillet 2022 un référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie.

En complément de ce référentiel, l'Ordre des pharmaciens, en collaboration avec la CNIL, vous propose un guide avec des outils pratiques afin de vous accompagner dans la mise en conformité de votre activité.

Ce guide s'adresse plus particulièrement aux pharmaciens titulaires d'officine, en votre qualité de responsables de traitement.

Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données personnelles du 27 avril 2016 (RGPD), entré en application le 25 mai 2018, s'inscrit dans la continuité des principes déjà existants énoncés dans la loi Informatique et Libertés du 6 janvier 1978.

Il en change toutefois la logique passant d'un contrôle *a priori*, fondé sur des formalités préalables auprès de la CNIL (déclarations, autorisations, engagements de conformité, etc.) à un régime de responsabilisation des acteurs traitant des données personnelles, tels que les pharmaciens.

Ainsi, les déclarations et engagements de conformité à l'ancienne norme simplifiée que les pharmaciens ont connue, sont supprimés.

En contrepartie, en tant que responsables de traitement, les pharmaciens doivent s'assurer que les traitements mis en œuvre dans leur officine sont conformes au RGPD. À ce titre, ils peuvent se référer au référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie.

Ils doivent également tenir à jour une documentation de toutes les démarches entreprises pour démontrer leur conformité au RGPD et à la loi Informatique et Libertés modifiée.

Qu'est-ce qu'une donnée personnelle ou donnée à caractère personnel ?

Toute information permettant d'identifier, directement ou indirectement, une personne.

Exemples : nom, prénom, date de naissance, numéro de sécurité sociale, etc.

Parmi ces données figurent les données de santé qui revêtent un caractère sensible et doivent être particulièrement protégées.

Qu'est-ce qu'une donnée de santé ?

Toute donnée relative à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de soins de santé) qui révèle des informations sur l'état de santé de cette personne.

Exemples : une information concernant la maladie d'un patient, son handicap, une donnée clinique ou thérapeutique, physiologique ou biologique le concernant, le fait que le patient fasse l'objet d'une prise en charge en affection longue durée, etc.

Entrent dans cette définition, les données provenant tant d'un professionnel de santé que d'un dispositif médical ou du patient lui-même.

Qu'est-ce qu'un traitement de données personnelles ?

Toute opération ou tout ensemble d'opérations portant sur des données personnelles, quel que soit le procédé ou le support utilisé (papier, numérique, etc.), tels que la collecte, l'enregistrement, l'utilisation de toute donnée personnelle.

Qu'est-ce qu'un responsable de traitement ?

La personne, l'autorité publique, le service ou l'organisme qui détermine les raisons pour lesquelles les données sont collectées et traitées, ainsi que les moyens de ce traitement.

Exemples : le pharmacien titulaire est responsable des traitements informatiques et papiers mis en œuvre dans son officine.

IMPORTANT :
La protection des données s'applique tant aux données informatiques qu'aux données papiers (copies d'ordonnance par exemple).

Suis-je concerné par le RGPD en tant que pharmacien ?

Dans le cadre de la dispensation des médicaments[1] et la réalisation des autres missions confiées au pharmacien d'officine

En tant que pharmacien, vous êtes amené à recevoir des informations concernant vos patients (papier ou informatique) pour assurer notamment leur suivi pharmaceutique, tenir l'ordonnancier ou encore les registres pour les produits dont la délivrance est soumise à enregistrement obligatoire, réaliser des activités de télésoin, etc.

Vous êtes également amené à transmettre certaines informations sur vos patients dans le cadre de vos échanges avec les autres professionnels de santé qui interviennent dans la prise en charge ou encore dans le cadre de la télétransmission des feuilles de soins et factures subrogatoires.

Dans le cadre de la gestion de votre officine

Vous êtes amené à recevoir des informations concernant votre personnel pour accomplir les formalités administratives afférentes à leur embauche, mettre à leur disposition des outils informatiques, organiser leur travail, gérer leurs formations et leur carrière, tenir le registre unique du personnel ou encore lorsque vous gérez leur paie.

Vous êtes également amené à collecter certaines informations concernant vos fournisseurs, dans le cadre de la gestion des factures et leur paiement.

> **!** **IMPORTANT :**
> Ces informations que vous recevez et/ou transmettez sont majoritairement des données personnelles. Dans toutes ces situations où vous utilisez des données personnelles, vous êtes concerné par le RGPD. Les pharmaciens titulaires sont responsables de la conformité au sein de leur officine.

[1] Médicaments, produits ou objets mentionnés à l'article L. 4211-1 du code de la santé publique et marchandises autorisées par l'arrêté du 15 février 2002 fixant la liste des marchandises dont les pharmaciens peuvent faire le commerce dans leur officine

Où en êtes-vous dans votre conformité au RGPD ?

☐ Avez-vous désigné un DPO ?

Qu'est-ce qu'un DPO ?

Le DPO (*data protection officer* ou délégué à la protection des données) conseille et accompagne les organismes qui le désignent pour mettre en conformité leurs traitements de données personnelles.

Pour en savoir plus :
Le délégué à la protection des données (DPO)
Le guide du délégué à la protection des données

En tant que pharmacien d'officine, avez-vous l'obligation de désigner un DPO ?

La CNIL estime que la désignation d'un DPO devrait en principe être nécessaire pour les officines de pharmacie déclarant une activité globale annuelle de plus de 2 600 000 € HT. Les pharmaciens titulaires, en tant que responsables de traitement, restent néanmoins libres de leur choix sous réserve de pouvoir le justifier.

Pour en savoir plus :
Rubrique 11 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
La CNIL adopte un référentiel sur la gestion des officines de pharmacie

Qui choisir en qualité de DPO ?

Avant de désigner un DPO, il convient de s'assurer que le DPO détient les compétences requises, qu'il dispose de moyens suffisants et qu'il a la capacité d'agir en toute indépendance.

Pour en savoir plus :
Désigner un délégué à la protection des données (DPO) ou modifier une désignation
Guide pratique RGPD (notamment fiche 2)

Comment désigner un DPO ?

En complétant le formulaire en ligne de la CNIL : Désigner un délégué à la protection des données (DPO) ou modifier une désignation

☐ Avez-vous identifié les données personnelles que vous traitez dans le cadre de votre activité ?

Il convient d'identifier l'ensemble des données à caractère personnel utilisées dans le cadre de votre activité et d'établir une liste des traitements de ces données (appelée « cartographie des traitements »).

Seules les données à caractère personnel pertinentes et strictement nécessaires pour atteindre l'objectif de votre traitement doivent être traitées.

Pour en savoir plus :
Rubrique 5 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie

☐ Tenez-vous un registre de vos activités de traitements (registre RGPD) ?

Vous devez recenser et décrire l'ensemble des traitements de données à caractère personnel mis en œuvre au sein de votre officine dans un registre.

Ce document permet de refléter la réalité de vos traitements et sert d'outil de pilotage et de démonstration de votre conformité au RGPD.

Pensez à mettre à jour ce registre en fonction des évolutions de vos traitements.

Pour en savoir plus :
Le registre des activités de traitement

BOITE À OUTILS :
Des modèles de fiches de registre pré-remplis et à adapter pour les traitements concernant vos patients ou votre personnel figurent dans les fiches n° 1 et n° 2 de ce guide.

☐ Protégez-vous ces données ?

En tant que responsable de traitement, vous devez mettre en place toutes les mesures pour sécuriser les données que vous traitez et prendre toutes les précautions pour garantir la confidentialité des données. Cela vise à empêcher leur destruction, perte, altération, divulgation ou accès non autorisé, de manière accidentelle ou illicite.

Exemples : armoire fermée à clé, logiciel protégé par un antivirus, etc.

> **IMPORTANT :**
> Assurez-vous que votre destinataire est bien habilité à recevoir les données que vous lui transmettez.

Pour en savoir plus :
Rubrique 10 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
Guide de sécurité des données personnelles de la CNIL
Sécurité des données
ANSSI - Les bonnes pratiques

☐ Informez-vous les personnes concernées par ces traitements ?

Les personnes (patients, salariés, etc.) dont vous traitez les données doivent être informées de l'existence des traitements de leurs données et de leurs droits (tels que droits d'accès, rectification, opposition, effacement, etc.).

Il convient d'informer les personnes concernées de façon claire, simple, concise et facilement accessible.

> **IMPORTANT :**
> - Utiliser un vocabulaire simple, des phrases courtes et un style direct.
> - Ne pas noyer l'information dans un document de 20 pages ou en bas de page dans une taille de police illisible.
> - Faciliter l'accès aux mentions pour que les personnes puissent voir immédiatement comment et où accéder à l'information.
> - Penser toujours à mettre à jour vos mentions en cas de changement.

BOITE À OUTILS :
Modèles de mentions d'information pour vos patients ou votre personnel dans les fiches n° 1 et n° 2 de ce guide.

Pour en savoir plus :
Conformité RGPD : comment informer les personnes et assurer la transparence ?

☐ Avez-vous mis en place une procédure de traitement des demandes d'exercice de droits ?

Les personnes (patients, salariés, etc.) dont vous traitez les données disposent de droits sur leurs données qu'elles peuvent exercer directement auprès de l'officine : droit d'accès à toutes les données les concernant, droit de rectification, droit d'effacement, droit à la limitation du traitement, droit de s'opposer au traitement de leurs données, selon les conditions prévues par le RGPD et le cas échéant, d'autres textes applicables.

Chaque officine doit donc mettre en place une procédure afin de répondre à toutes les demandes d'exercice de droits des personnes. Le responsable de traitement doit répondre à ces demandes dans un délai de 1 mois (pouvant être prolongé de 2 mois en raison de la complexité et du nombre de demandes) ou, s'il s'agit de données de santé, dans un délai de 8 jours (porté à 2 mois lorsque les informations datent de plus de 5 ans).

Pour en savoir plus :
Rubrique 9 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
Respecter les droits des personnes

☐ Comment répondre à une demande d'accès concernant une personne décédée ?

Qui peut former une demande d'accès dans ce cadre ?

Les ayants droit, le concubin ou le partenaire lié par un pacte civil de solidarité (PACS) peuvent demander accès aux données d'une personne décédée sous certaines conditions. Notamment cet accès ne peut s'exercer que si la personne ne s'y est pas opposée de son vivant. Ils doivent pouvoir justifier de leur qualité par tous moyens.

Pour des ayants droit, il s'agit d'apporter la preuve de la qualité d'héritier.

Exemples : livret de famille, acte de notoriété, certificat d'hérédité, attestation de porte-fort.

Pour des concubins, il s'agit d'apporter la preuve de la vie commune, de sa stabilité, de son caractère notoire et de la mise en commun même partielle de moyens matériels.

Exemples : certificat de concubinage s'il en existe, bail commun, factures, courriers, photographies, témoignages écrits.

Pour des partenaires liés par un PACS, il convient de justifier de la conclusion du PACS non dissous à la date du décès.

Comment former une demande d'accès ?

La demande doit être expressément fondée sur un ou plusieurs des trois motifs prévus par l'article L. 1110-4 du code de la santé publique :

- connaître les causes de la mort,
- défendre la mémoire du défunt,
- faire valoir ses droits.

L'indication de la volonté de connaître les causes de la mort n'appelle pas de précision supplémentaire. En revanche, la volonté de défendre la mémoire du défunt ou de faire valoir ses propres droits doit être explicitée par le demandeur.

À quelles informations médicales peuvent-ils accéder ?

Le code de la santé publique ne prévoit pas, pour les proches, l'accès à l'intégralité du dossier médical du patient décédé. Le pharmacien n'est ainsi tenu de communiquer au demandeur que les seules informations nécessaires à la réalisation de l'objectif qu'il poursuit.

Pour en savoir plus :
Article 85 de la loi Informatique et Libertés
Articles L.1110-4, L.1111-7 et R.1111-7 du code de la santé publique

☐ Avez-vous défini des durées de conservation des données ?

Comment définir des durées de conservation et d'archivage ?

Pour définir des durées de conservation et d'archivage, vous pouvez vous poser les questions suivantes :

- Ai-je des obligations légales de conserver les données pendant un certain temps ?
- Jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ?
- Dois-je conserver ces données plus longtemps en archivage pour me protéger en cas de contentieux ?
- Si oui, ai-je besoin de toutes ces informations ? Pendant combien de temps ?
- Quelles sont les règles d'archivage des données à respecter ? Quelles sont les règles de suppression des données ?

Pour en savoir plus :
Rubrique 7 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
Guide pratique CNIL sur les durées de conservation (notamment le point n° 2.9)
Référentiel des durées de conservation dans le domaine de la santé hors recherches
Durée de conservation des documents liés à l'activité pharmaceutique de l'officine

☐ Avez-vous encadré vos relations avec vos sous-traitants ?

Qu'est-ce qu'un sous-traitant ?

Tout prestataire qui traite des données personnelles en votre nom et pour votre compte est considéré comme un sous-traitant au sens de l'article 28 du RGPD.

Exemples : prestataires informatiques (hébergement, maintenance, infogérance), éditeurs de logiciels ou de comptabilité, etc.

Avez-vous identifié vos sous-traitants ?

En principe, les éditeurs de logiciels n'ont pas accès et ne traitent pas de données personnelles. Dans ce cas, ils ne sont pas considérés comme sous-traitants. Toutefois, si leur rôle ne se cantonne pas simplement à la conception ou au développement du logiciel, mais qu'ils accèdent à certaines données, les hébergent et/ou les intègrent dans le système informatique des officinaux, dans ce cas, ils peuvent être considérés comme vos sous-traitants.

Comment encadrer vos relations avec vos sous-traitants ?

Il vous faut conclure un contrat de sous-traitance avec eux afin d'encadrer leurs missions, en accord avec la réglementation.

IMPORTANT :
Vous restez responsable de tout manquement commis par vos sous-traitants.

BOITE À OUTILS :
Modèle d'annexe de sous-traitance dans la fiche n° 3 de ce guide.

Pour en savoir plus :
Travailler avec un sous-traitant

☐ Transférez-vous des données hors de l'Union européenne ?

Vous devez identifier si certains de vos prestataires sont situés hors de l'Union européenne (UE) ou transfèrent hors de l'UE les données à caractère personnel que vous détenez. Si tel est le cas, il convient de prendre les mesures nécessaires pour assurer un niveau de protection des données suffisant et approprié.

Pour en savoir plus :
Transférer des données hors de l'UE

☐ Avez-vous réalisé des analyses d'impact pour vos traitements ?

Le RGPD impose au responsable du traitement de réaliser, dans certains cas, une analyse d'impact relative à la protection des données (AIPD).

Qu'est-ce qu'une analyse d'impact ?

Il s'agit d'une analyse détaillée permettant d'évaluer la nécessité et la proportionnalité d'un traitement de données au regard des principes prévus par le RGPD, ainsi que ses éventuels risques sur la sécurité des données.

Devez-vous réaliser une analyse d'impact pour les traitements que vous mettez en œuvre ?

La CNIL estime que la réalisation d'une AIPD devrait en principe être nécessaire pour les officines de pharmacie déclarant une activité globale annuelle de plus de 2 600 000 € HT.

Pour en savoir plus :
Rubrique 11 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
La CNIL adopte un référentiel sur la gestion des officines de pharmacie
L'analyse d'impact relative à la protection des données (AIPD)

Fiches pratiques

FICHE N° 1 - **Quelles sont vos obligations à l'égard de vos patients ?**

- ☐ Informer vos patients du traitement de leurs données personnelles
- ☐ Tenir et mettre à jour votre registre RGPD

FICHE N° 2 – **Quelles sont vos obligations à l'égard de votre personnel ?**

- ☐ Informer votre personnel du traitement de leurs données personnelles
- ☐ Imposer une obligation de confidentialité auprès de votre personnel
- ☐ Tenir et mettre à jour votre registre RGPD

FICHE N° 3 – **Comment gérer les relations avec vos sous-traitants ?**

- ☐ Encadrer vos relations avec vos sous-traitants
- ☐ Respect de ses obligations par votre sous-traitant

FICHE N° 4 – **Quelles sont vos obligations en cas d'installation d'un dispositif vidéo ?**

- ☐ Informer les personnes filmées
- ☐ Formalités à accomplir

FICHE N° 5 – **Comment réagir en cas de violation de données ?**

- ☐ Identifier la violation de données personnelles
- ☐ Tenir un registre des violations
- ☐ Notifier la violation à la CNIL ?
- ☐ Communiquer la violation aux personnes concernées ?

FICHE N° 6 – **Comment réagir en cas de contrôle de la CNIL ?**

- ☐ Déroulement d'un contrôle de la CNIL
- ☐ Issue d'un contrôle de la CNIL
- ☐ Préparation à un contrôle de la CNIL

FICHE N° 1 - Quelles sont vos obligations à l'égard de vos patients ?

Dans le cadre de l'exercice de votre profession, vous êtes amené à collecter les données personnelles de vos patients afin d'assurer leur **suivi pharmaceutique**.

Pour en savoir plus :
Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie
La CNIL adopte un référentiel sur la gestion des officines de pharmacie

☐ **Informer vos patients du traitement de leurs données personnelles**

BOITE À OUTILS :
Pour informer vos patients, vous pouvez utiliser le modèle de mention d'information figurant ci-après.

Comment informer ? Soit par voie d'affichage (écriteau, écran digital exposé sur les comptoirs de la pharmacie), soit par le biais d'une notice d'information remise au patient.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

MENTION D'INFORMATION POUR LA GESTION ET LE SUIVI DES PATIENTS

Vos données personnelles, notamment les données concernant votre santé, votre identifiant national de santé (INS) et votre numéro de sécurité sociale (NIR), font l'objet d'un traitement mis en œuvre par la pharmacie [1] _____ _____, en notre qualité de responsable de traitement, à des fins de gestion et de suivi de nos patients, conformément aux dispositions du code de la santé publique, au Règlement européen général sur la protection des données du 27 avril 2016 et à la loi Informatique et Libertés modifiée.

La base juridique de ce traitement repose sur nos obligations légales en matière de prise en charge sanitaire et de gestion administrative de la patientèle.[2]

Vos données sont destinées aux personnes habilitées de la pharmacie ainsi qu'à des prestataires agissant en qualité de sous-traitants en charge de la maintenance du système d'information, en particulier de l'application dédiée au suivi des patients.[3]

Elles sont également transmises à des destinataires externes, notamment la sécurité sociale, les organismes d'assurance maladie complémentaire et les professionnels de santé intervenant dans votre prise en charge.

Dans ce contexte, vos données ne font l'objet d'aucun transfert en dehors de l'Union européenne.[4]

Votre dossier patient est conservé pendant 3 ans à compter de la dernière intervention sur le dossier, puis archivé sur un support distinct pendant 15 ans, sauf disposition légale ou réglementaire contraire. Ainsi, par exception[5] :

- Les copies d'ordonnance de médicaments classés comme stupéfiants ou relevant de la réglementation des stupéfiants sont conservées pendant 3 ans (Art. R. 5132-35 du code de la santé publique) ;
- Le registre comptable des médicaments stupéfiants et les documents attestant de leur destruction sont conservés pendant 10 ans (Art. R. 5132-36 du code de la santé publique) ;
- Le registre des préparations magistrales ou officinales est conservé pendant 10 ans (Art. R. 5125-45 du code de la santé publique) ;
- Le registre spécial des médicaments dérivés du sang est conservé pendant 40 ans (Art. R. 5121-195 du code de la santé publique) ;
- En cas de télétransmission, le double électronique des feuilles de soins transmises ainsi que leurs accusés de réception sont conservés pendant 90 jours au moins (art. R. 161-47 du code de la sécurité sociale).

Conformément au Règlement européen général sur la protection des données et à la loi Informatique et Libertés modifiée, vous disposez d'un droit d'accès et de rectification de vos données à caractère personnel, et sous certaines conditions, d'opposition, d'effacement, de portabilité ou de limitation du traitement. Ces droits peuvent être exercés auprès de[6] _____ en adressant un courrier électronique à l'adresse suivante[6] : _____ ou par courrier postal à[6] :

_____ _____.

Il est également possible, si vous l'estimez nécessaire, d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

---

[1] Indiquer le nom de la pharmacie

[2] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre *(vous pouvez vous référer au point 4 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie)*

[3] Conserver uniquement ce qui est applicable

[4] À adapter si transfert en dehors de l'UE : préciser les États concernés et les modalités de transfert en cas de non-adéquation (clauses contractuelles types, mesures supplémentaires, etc.)

[5] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre et des durées de conservation que vous avez fixées *(vous pouvez vous référer au point 7 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie et au tableau accessible sur le site de l'Ordre national des pharmaciens)*

[6] À compléter

BONNES PRATIQUES :

Cette mention d'information peut être complétée par d'autres documents distincts afin d'informer vos patients de tout autre traitement ou transmission de leurs données personnelles à des tiers.

Exemple : À l'occasion des tests antigéniques effectués en officine à des fins de diagnostic du SARS-CoV-2, le ministère des Solidarités et de la Santé avait proposé une notice d'information à destination des patients.

BONNES PRATIQUES :

Depuis l''entrée en vigueur du décret n° 2023-251 du 3 avril 2023 relatif au dossier pharmaceutique, un dossier pharmaceutique (DP) peut être ouvert automatiquement par le Conseil national de l'ordre des pharmaciens (CNOP), après en avoir informé les patients au préalable et sauf opposition de leur part dans un délai de 6 semaines.

Si le patient n'a pas de DP :
La création automatique d'un DP repose sur une information préalable et individuelle par le CNOP. Le CNOP a besoin des coordonnées des patients pour pouvoir leur transmettre les informations relatives au nouveau régime DP.
Dès le premier passage d'un patient en pharmacie après la parution du décret, vous devrez l'informer et collecter ses coordonnées (e-mail ou adresse postale) dans votre logiciel. Ces coordonnées seront automatiquement transmises au CNOP.

@ Si le patient vous a fourni son adresse de messagerie, il recevra un e-mail de la part du CNOP.
✉ Si le patient vous a fourni son adresse postale, votre logiciel éditera automatiquement un courrier que vous imprimerez et remettrez en main propre au patient.

Cet e-mail ou courrier contient les éléments utiles permettant au patient d'activer son DP sans délai ou de s'opposer à sa création, dans un délai de 6 semaines. Sans action de sa part et passé ce délai, le DP sera automatiquement créé par le CNOP.

Si le patient dispose déjà d'un DP :
Afin d'informer les patients disposant déjà d'un DP, le CNOP a besoin de leurs coordonnées pour pouvoir leur transmettre les informations relatives au nouveau régime DP.
Dès le premier passage d'un patient en pharmacie après la parution du décret, vous devrez l'informer et collecter ses coordonnées (e-mail ou adresse postale) dans votre logiciel. Ces coordonnées seront automatiquement transmises au CNOP.

@ Si le patient vous a fourni son adresse de messagerie, il recevra un e-mail de la part du CNOP.
✉ Si le patient vous a fourni son adresse postale, votre logiciel éditera automatiquement un courrier que vous imprimerez et remettrez en main propre au patient.

Cet e-mail ou courrier informe le patient qu'il dispose déjà d'un DP et indique les modalités de clôture de ce DP s'il le souhaite (via un formulaire disponible sur le site de l'Ordre).

☐ Tenir et mettre à jour votre registre RGPD

BOITE À OUTILS :
Pour le traitement relatif à la gestion et au suivi de vos patients, vous pouvez utiliser le modèle de fiche de registre pré-rempli figurant ci-après.

FICHE DE REGISTRE DE GESTION ET SUIVI DES PATIENTS

Date de création de la fiche[1]	
Date de dernière mise à jour de la fiche[1]	
Nom du responsable de la mise en œuvre du traitement et fonction occupée[1]	
Nom du logiciel ou de l'application[2] *(si pertinent)*	
Nom et coordonnées du DPO[1] *(si une désignation a eu lieu)*	

Objectifs poursuivis *(Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités)*

Le logiciel[2] _____ permet la gestion et le suivi pharmaceutique des patients de l'officine. Il sert à mon activité de dispensation des médicaments, produits ou objets mentionnés à l'article L. 4211-1 du code de la santé publique et des marchandises autorisées par l'arrêté du 15 février 2002 fixant la liste des marchandises dont les pharmaciens peuvent faire le commerce dans leur officine, et à la réalisation des autres missions de santé publique confiées aux pharmaciens d'officine.

Catégories de personnes concernées *(Listez les différents types de personnes dont vous collectez ou utilisez les données)*

- Patients
- Professionnels de santé
- Le cas échéant, famille du patient
- [3] _____

Catégories de données collectées *(Cochez et listez les différentes données traitées.* N.B. *: L'utilité du recueil de chacune de ces catégories de données doit pouvoir être justifiée)*

☒État-civil, identité, données d'identification :

- **Patient :** nom, prénom, date de naissance, adresse postale, adresse électronique et numéro de téléphone, identifiant national de santé (INS), numéro de sécurité sociale et taux de prise en charge, adhésion à des organismes d'assurance maladie complémentaire
- **Médecin prescripteur et autres professionnels intervenant dans la prise en charge du patient :** nom, prénom, numéro d'identification, spécialité, situation conventionnelle, adresse postale, adresse électronique ou de messagerie sécurisée de santé et numéro de téléphone

☒Vie personnelle : nom et coordonnées des personnes mandatées pour le retrait des produits délivrés et le lien avec le patient (avec l'accord du patient et pour sa prise en charge uniquement)

☒Données de connexion au dossier du patient : traces fonctionnelles et techniques

☐Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, etc.)*

☐Autres catégories de données[4] : _____

Des données particulièrement sensibles sont-elles traitées ? *(La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et*

[1] À compléter
[2] Indiquer le nom de votre logiciel ou de votre application
[3] À compléter si pertinent
[4] À compléter si pertinent

biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes. Il s'agit des données relatives aux condamnations pénales ou aux infractions. Il s'agit du numéro d'identification national unique (NIR ou numéro de sécurité sociale)).

☒ Oui ☐ Non
Si oui, lesquelles ? : Données de santé, NIR

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ? *(Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre)*

[1] Le dossier patient :
3 (par exemple) ☐Jours ☐Mois ☒Ans
+ archivé : 15 ans

Les copies d'ordonnance de médicaments classés comme stupéfiants ou relevant de la réglementation des stupéfiants (art. R. 5132-35 du code de la santé publique) :
3 ☐Jours ☐Mois ☒Ans

Le registre comptable des médicaments stupéfiants et les documents attestant de leur destruction (art. R. 5132-36 du code de la santé publique) :
10 ☐Jours ☐Mois ☒Ans

Le registre des préparations magistrales ou officinales (art. R. 5125-45 du code de la santé publique) :
10 ☐Jours ☐Mois ☒Ans

Le registre spécial des médicaments dérivés du sang (art. R. 5121-195 du code de la santé publique) :
40 ☐Jours ☐Mois ☒Ans

En cas de télétransmission, le double électronique des feuilles de soins transmises ainsi que leurs accusés de réception (art. R. 161-47 du code de la sécurité sociale) :
Au moins 90 ☒Jours ☐Mois ☐Ans

Autre durée[1] : ☐Jours ☐Mois ☐Ans

Catégories de destinataires des données

Destinataires internes

- Personnel de la pharmacie
- [1] _____

Organismes externes

- Professionnels de santé et professionnels concourant à la prévention et aux soins
- Etablissements, services ou organismes mentionnés à l'article L. 5126-10 du code de la santé publique
- Organismes d'assurance maladie
- Organismes d'assurance maladie complémentaire
- Organismes de recherche dans le domaine de la santé et organismes spécialisés dans l'évaluation des pratiques de soins
- Conseil national de l'ordre des pharmaciens au titre de la mise en œuvre du dossier pharmaceutique défini à l'article L. 1111-23 du code de la santé publique, ainsi que l'hébergeur du dossier pharmaceutique
- [2] _____

[1] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre et des durées de conservation que vous avez fixées *(vous pouvez vous référer au point 7 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie et au tableau accessible sur le site de l'Ordre national des pharmaciens)*
2 À compléter si pertinent

Sous-traitants

- Éditeur de logiciel[1] _____ s'il assure une prestation de maintenance informatique ou d'hébergement de données de santé
- [1] _____

Transferts des données hors UE *(Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et 47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD) et les personnes devront être informées. Consultez le site de la CNIL.)*

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

☐ Oui ☒Non[2]

Si oui, vers quel(s) pays ?

Mesures de sécurité *(Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données. Le niveau de sécurité doit être adapté aux risques soulevés par le traitement.)*

Catégories	Mesures[3]	
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel de l'officine accédant aux données	☐
	Pour une officine mutualisant des ressources informatiques, rédiger une charte informatique et lui donner force contraignante	☐
Authentifier les utilisateurs	Définir un identifiant (« login ») propre à chaque utilisateur	☐
	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la CNIL[4]	☐
	Pour les utilisateurs accédant aux données de santé, utiliser une authentification forte basée sur : - les cartes CPx, notamment : o une carte de professionnel de santé (CPS), qui doit rester strictement personnelle, sans communication du code secret aux autres membres du personnel de l'officine ; o une carte de professionnel en formation (CPF pour les étudiants en pharmacie) - ou tout moyen alternatif « à deux facteurs » (par exemple, un mot de passe complété par l'envoi d'un code unique à chaque connexion).	☐
Gérer les habilitations, tracer les accès et gérer les incidents	Attribuer un profil d'habilitation adapté à chaque utilisateur (distinguant notamment les données administratives et les données médicales)	☐
	Supprimer les permissions d'accès obsolètes	☐
	Mettre en place un système de journalisation des accès aux données de santé	☐
	Informer les utilisateurs de la mise en place du système de journalisation	☐
	Prévoir les procédures pour les notifications de violation de données à caractère personnel	☐

1 Indiquer le nom de votre logiciel ou de votre application

2 À adapter si transfert en dehors de l'UE : préciser les Etats concernés et les modalités de transfert en cas de non-adéquation (clauses contractuelles types, mesures supplémentaires, etc.)

3 Mesures décrites au point 10 du Référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des officines de pharmacie. À adapter et compléter en fonction des mesures mises en œuvre au sein de votre officine

4 Authentification par mot de passe : les mesures de sécurité élémentaires

Catégories	Mesures	
Sécuriser les postes de travail et l'informatique mobile	Prévoir une procédure de verrouillage automatique de la session informatique, avec un déclenchement au bout d'un délai d'inactivité de cinq minutes pour les postes situés dans les zones ouvertes au public	☐
	Protéger les postes susceptibles d'être facilement emportés, notamment les ordinateurs portables, à l'aide d'un câble physique de sécurité	☐
	Chiffrer les supports de stockage des équipements informatiques utilisés dans des lieux accessibles au public	☐
	Permettre la mise à jour régulière des antivirus	☐
	Recueillir l'accord de l'utilisateur avant toute intervention sur un poste individuel	☐
	Limiter le stockage de données de santé sur les tablettes et les ordiphones (en raison des conséquences pour les patients/clients en cas de vol ou de perte du matériel). Si ces équipements sont utilisés, leur niveau de sécurisation des données doit être équivalent à celui des autres équipements (chiffrement, codes d'accès, etc.)	☐
	Exiger un secret pour le déverrouillage des ordiphones ou des tablettes	☐
	Protéger les écrans des regards indiscrets (orientation, filtre optique)	☐
	Prévoir une « zone de confidentialité » autour des postes de dispensation, avec un marquage et une information incitant à la respecter	☐
	Limiter l'utilisation de supports de stockage amovibles (clés USB, disques dur externe) et chiffrer systématiquement les données sensibles qui y sont conservées	☐
	Ne pas prêter ou utiliser pour des usages personnels les ordiphones et tablettes à usage professionnel	☐
Protéger le réseau informatique interne	Interdire les connexions d'appareils non professionnels sur le réseau En cas de fourniture d'un accès Wifi public aux clients de l'officine, celui-ci ne doit pas permettre d'accéder au réseau interne de l'officine (cloisonnement)	☐
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
	Permettre l'installation sans délai des mises à jour critiques	☐
Sauvegarder et prévoir la continuité d'activité	Effectuer ou permettre l'exécution des sauvegardes régulières	☐
	Stocker les supports de sauvegarde dans un endroit sûr	☐
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'officine les interventions par des tiers	☐
	Effacer les données de tout matériel avant sa mise au rebut	☐
Gérer la sous-traitance	Prévoir des clauses spécifiques[1] dans les contrats des sous-traitants	☐
	Prévoir des conditions de restitution et de destruction des données	☐
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐

[1] Description précise du traitement (données, localisation, opérations, accès, durée, restitution …), objectifs de sécurité adaptés aux risques, gestion des incidents et notification des violations de données

Catégories	Mesures	
Sécuriser les échanges avec d'autres professionnels de santé et avec les patients/clients	Authentifier les destinataires avant tout envoi de données de santé	☐
	Utiliser une messagerie électronique sécurisée de santé pour les échanges entre professionnels de santé	☐
	Pour les échanges avec d'autres professionnels intervenant dans la prise en charge du patient/client ou avec les patients/clients eux-mêmes : • procéder au chiffrement des documents avant leur envoi sur une messagerie électronique standard[1] et transmettre le secret par un envoi distinct et via un canal différent ;	☐
	• utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ;	☐
	• choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes.	☐
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées	☐
	Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
	Sécuriser le stockage des dossiers au format papier (locaux sécurisés, armoire fermant à clé)	☐
	Récupérer les documents imprimés contenant des données immédiatement après leur impression ou effectuer, lorsque c'est possible, une impression sécurisée	☐
	Détruire les documents papier contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié (certifié au minimum classe 3 de la norme DIN 32757105)	☐
Autres mesures[2]	_____	☐

Information et respect des droits des personnes

Comment les personnes concernées sont-elles informées du traitement ? *(Cochez la ou les cases correspondantes)*

☒ Mention d'information
Précisez sur quel(s) support(s)[3] : _____
☐ Charte informatique
☐ Politique de confidentialité
Précisez sur quel(s) support(s)[2] : _____
☐ Contrat
Précisez les catégories de personnes concernées par le contrat[2] : _____
☐ Autres mesures[2] : _____

Comment sont traitées les demandes d'exercice des droits des personnes ?
Indiquez le délai du traitement de la demande :
8 jours pour les demandes de droits d'accès aux données de santé
1 mois pour les autres demandes

Indiquez la personne chargée de répondre aux demandes[4] : _____

[1] Les messageries instantanées (« *chat* ») doivent être utilisées avec la plus grande précaution, et de manière sécurisée
[2] À préciser, si applicable
[3] À compléter *(exemple : écriteau à l'entrée de la pharmacie ou affichage sur un panneau destiné à diverses informations, affichette ou écran digital disponible au niveau des comptoirs, notice d'information remise au patient)*
[4] À compléter

FICHE N° 2 – Quelles sont vos obligations à l'égard de votre personnel ?

Dans le cadre de la **gestion administrative du personnel,** vous êtes amené à collecter les données personnelles des personnes que vous avez embauchées, lorsque vous accomplissez par exemple les formalités administratives afférentes à leur embauche, mettez à leur disposition des outils informatiques, organisez leur travail, gérez leurs formations et leur carrière, tenez le registre unique du personnel ou encore lorsque vous gérez leur paie.

Le terme « personnel » désigne ici toute personne exerçant de manière permanente ou temporaire dans l'officine, quels que soient son statut, le type ou la durée de son contrat, ou son niveau de rémunération.

Exemples : les pharmaciens adjoints, les préparateurs en pharmacie, les intérimaires ou encore les stagiaires, etc.

Pour en savoir plus :
En matière de gestion du personnel :
Référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel
RGPD en pratique : protéger les données de vos collaborateurs

Pour en savoir plus :
En matière de recrutement : Guide de la CNIL du 30 janvier 2023 relatif au recrutement

☐ Informer votre personnel du traitement de leurs données personnelles

BOITE À OUTILS :

Pour le personnel déjà en poste : vous pouvez utiliser le modèle de note d'information figurant ci-après. Cette information peut se faire par la remise d'une notice d'information par exemple.

Pour les nouveaux arrivants : vous pouvez utiliser le modèle de note d'information figurant ci-après. Il suffit par exemple de l'insérer dans le contrat de travail ou en annexe de celui-ci ou d'envoyer cette note d'information par courriel au moment du recrutement.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

NOTE D'INFORMATION

Vos données personnelles, notamment vos données d'identité, les données relatives au suivi de carrière et de formation, à l'établissement de la fiche de paie, aux outils et matériels informatiques mis à disposition, font l'objet d'un traitement mis en œuvre par la pharmacie[1] _____ , en notre qualité de responsable de traitement. Vos données sont traitées à des fins de gestion du personnel telles que décrites au point 3 du référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel, conformément au Règlement européen général sur la protection des données du 27 avril 2016 et à la loi Informatique et Libertés modifiée.

Les bases juridiques du traitement reposent sur nos obligations légales en matière de gestion du personnel et conformément à votre contrat de travail.[2]

Vos données sont destinées aux personnes habilitées chargées de la gestion du personnel, de la paie, des outils informatiques mis à votre disposition, et aux prestataires en charge de la paie et de la maintenance informatique agissant en qualité de sous-traitant.[3]

Elles sont également transmises aux organismes extérieurs autorisés, tels que les organismes de retraite, de prévoyance, ou autres assurances, diverses autorités réglementaires.

Dans ce contexte, vos données ne font l'objet d'aucun transfert en dehors de l'Union européenne.[4]

Vos données sont conservées pendant la durée de la relation de travail, sauf disposition légale ou réglementaire contraire. Ainsi, par exception[5] :

- Vos bulletins de salaire sont conservés 1 mois, puis archivés :
  - Au format papier : 5 ans (Art. L. 3243-4 du code du travail),
  - Au format électronique : pendant 50 ans ou jusqu'à vos 75 ans (Art. D. 3243-8 du code du travail) ;
- Les ordres de virement pour vos paiements sont conservés le temps nécessaire à l'émission de votre bulletin de salaire, puis archivés 10 ans à compter de la clôture de l'exercice comptable (Art. L. 123-22 du code du commerce) ;
- Les mentions vous concernant figurant sur le registre unique du personnel sont conservées la durée pendant laquelle vous faites partie des effectifs, puis archivées 5 ans à compter de votre départ de l'officine (Art. R. 1221-26 du code du travail).

Conformément au Règlement européen général sur la protection des données et à la loi Informatique et Libertés modifiée, vous disposez d'un droit d'accès et de rectification de vos données à caractère personnel, et sous certaines conditions, d'opposition, d'effacement, de portabilité ou de limitation du traitement. Ces droits peuvent être exercés auprès de[6] _____ en adressant un courrier électronique à l'adresse suivante[6] :
_____ ou par courrier postal à[6] :
_____.

Il est également possible, si vous l'estimez nécessaire, d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

[1] Indiquer le nom de la pharmacie
[2] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre *(vous pouvez vous référer au point 4 du Référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel)*
[3] Conserver uniquement ce qui est applicable
[4] À adapter si transfert en dehors de l'UE
[5] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre et des durées de conservation que vous avez fixées *(vous pouvez vous référer au point 7 du Référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel)*
[6] À compléter

☐ Imposer une obligation de confidentialité auprès de votre personnel

BOITE À OUTILS :
Il convient de vérifier que le contrat qui lie l'officine au personnel prévoit bien une obligation de confidentialité à la charge du personnel. Vous pouvez utiliser le modèle de clause figurant ci-après.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

CLAUSE DE CONFIDENTIALITE

Dans le cadre de ses missions, le[1] collaborateur/employé/stagiaire est susceptible d'accéder, de collecter et d'enregistrer les données personnelles gérées par la pharmacie[2] _____.

À ce titre, il s'engage à respecter le Règlement européen général sur la protection des données du 27 avril 2016 et la loi Informatique et Libertés modifiée et à ne pas divulguer, de quelle que manière que ce soit, les données personnelles à des personnes qui ne sont pas habilitées et de manière générale, à des personnes non autorisées à les recevoir.

☐ Tenir et mettre à jour votre registre RGPD

BOITE À OUTILS :
Pour le traitement relatif à la gestion du personnel, vous pouvez utiliser le modèle de fiche de registre pré-rempli figurant ci-après.

[1] Barrer les mentions inutiles
[2] Indiquer le nom de la pharmacie

FICHE DE REGISTRE DE GESTION DU PERSONNEL

Date de création de la fiche[1]	
Date de dernière mise à jour de la fiche[1]	
Nom du responsable de la mise en œuvre du traitement et fonction occupée[1]	
Nom du logiciel ou de l'application[2] *(si pertinent)*	
Nom et coordonnées du DPO[1] *(si une désignation a eu lieu)*	

Objectifs poursuivis *(Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités)*

- [3]Gestion administrative des personnels ;
- Gestion des rémunérations et accomplissement des formalités administratives afférentes ;
- Mise à disposition du personnel d'outils professionnels ;
- Organisation du travail ;
- Suivi des carrières et de la mobilité ;
- Formation ;
- Tenue des registres obligatoires ;
- Communication interne ;
- Gestion des aides sociales ;
- Réalisation des audits, gestion du contentieux et du précontentieux.

Catégories de personnes concernées *(Listez les différentes catégories de personnes dont vous collectez ou utilisez les données)*

- Personnels
- [4] _____

Catégories de données collectées *(Cochez et listez les différentes données traitées)*

☒ État-civil, identité, données d'identification : nom, prénom, adresse, date de naissance, numéro de sécurité sociale

☒ Vie professionnelle : CV, suivi de carrières et formation

☒ Informations d'ordre économique et financier : rémunérations, taux d'imposition

☒Données de connexion : logs

☐ Données de localisation *(ex. déplacements, données GPS, etc.)*

☐ Autres catégories de données[4] : _____

[1] À compléter
[2] Indiquer le nom de votre logiciel ou de votre application
[3] Conserver uniquement les fonctionnalités mises en place
[4] À compléter si pertinent

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

☒ Oui ☐Non
Si oui, lesquelles ? : numéro de sécurité sociale pour la gestion de la paie

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ? (*Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre)*

[1]Pour les données nécessaires à la gestion de la relation contractuelle (pendant la durée de la relation de travail) :

Pour les bulletins de salaire :
1 ☐Jours ☒Mois ☐Ans
+ archivés :
- Au format papier : 5 ans (Art. L. 3243-4 du code du travail)
- Au format électronique : pendant 50 ans ou jusqu'au 75 ans du[2] collaborateur/employé/stagiaire (Art. D. 3243-8 du code du travail)

Pour les ordres de virement pour les paiements des[2] collaborateurs/employés/stagiaires : Le temps nécessaire à l'émission de son bulletin de salaire.
+ archivés 10 ans à compter de la clôture de l'exercice comptable (Art. L. 123-22 du code du commerce).

Pour les mentions portées sur le registre unique du personnel : La durée pendant laquelle le[2] collaborateur /employé/stagiaire fait partie des effectifs.
+ archivées 5 ans à compter de son départ de l'officine (Art. R. 1221-26 du code du travail).

Autre durée[3] : ☐Jours ☐Mois ☐Ans

Catégories de destinataires des données

Destinataires internes
- Personnes habilitées chargées de la gestion du personnel[4]
- [3] _____

Organismes externes
- Organismes sociaux
- Organismes fiscaux
- [3] _____

Sous-traitants
- Comptable[4]
- [5]Editeur de logiciel[6] _____
- [3] _____

[1] À adapter et compléter en fonction des traitements de données personnelles que vous mettez en œuvre et des durées de conservation que vous avez fixées *(vous pouvez vous référer au point 7 du Référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel)*
[2] Barrer les mentions inutiles
[3] À compléter si pertinent
[4] À conserver si applicable
[5] À conserver si applicable *(par exemple si prestation de maintenance informatique ou d'hébergement de données)*
[6] Indiquer le nom de votre logiciel ou de votre application

Transferts des données hors UE *(Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et 47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD) et les personnes devront être informées. Consultez le site de la CNIL)*

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

☐ Oui ☒ Non[1]

Si oui, vers quel(s) pays ?

Mesures de sécurité *(Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données. Le niveau de sécurité doit être adapté aux risques soulevés par le traitement.)*

Catégories	Mesures[2]	
Sensibiliser 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	☐
	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	☐
	Utiliser des antivirus régulièrement mis à jour	☐
	Installer un « pare-feu » (*firewall*) logiciel	☐
	Recueillir l'accord de l'utilisateur avant toute intervention 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 *smartphones*	☐
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 cookies non nécessaires au service	☐

[1] À adapter si transfert en dehors de l'UE

[2] Mesures décrites au point 10 du *Référentiel de la CNIL du 21 novembre 2019 relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel*. À adapter et compléter en fonction des mesures mises en œuvre au sein de votre officine

Catégories	Mesures	
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières	☐
	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'officine les interventions par des tiers	☐
	Effacer les données de tout matériel avant sa mise au rebut	☐
Gérer la sous-traitance	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.). Pour plus de précisions, vous pouvez vous reporter au guide de la sous-traitance et aux exemples des clauses de sous-traitance.	☐
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi	☐
	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	☐
	Installer des alarmes anti-intrusion et les vérifier périodiquement	☐
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
	Encadrer de manière stricte les zones de commentaires libres	☐
	Tester sur des données fictives ou anonymisées	☐
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus	☐
	Conserver les secrets et les clés cryptographiques de manière sécurisée	☐
Autres mesures[1]	_____	☐

Information et respect des droits des personnes

Comment les personnes concernées sont-elles informées du traitement ? *(Cochez la ou les cases correspondantes)*

☒ Mention d'information

Précisez sur quel(s) support(s) : notice d'information communiquée au personnel déjà en poste et aux nouveaux arrivants

☐ Charte informatique

☐ Politique de confidentialité

Précisez sur quel(s) support(s)[1] : *(ex. : site internet de l'officine)*

☐ Contrat

Précisez les catégories de personnes concernées par le contrat[1] : _____

☐ Autres mesures[1] : _____

[1] À préciser, si applicable

Comment sont traitées les demandes d'exercice des droits des personnes ?
Indiquez le délai du traitement de la demande : 1 mois

Indiquez la personne chargée de répondre aux demandes[1] : _____

[1] À compléter

FICHE N° 3 – Comment gérer les relations avec vos sous-traitants ?

Lorsque vous confiez des traitements de données personnelles à vos sous-traitants, vous devez encadrer vos relations par un contrat de sous-traitance conforme au RGPD.

Pour en savoir plus :
Travailler avec un sous-traitant

☐ Encadrer vos relations avec vos sous-traitants

BOITE À OUTILS :
Pour encadrer vos relations avec vos sous-traitants conformément au RGPD, vous pouvez utiliser le modèle d'annexe figurant ci-après.

BONNES PRATIQUES :

Pour tout nouveau contrat : compléter et intégrer le modèle en annexe du contrat.

Pour les contrats en cours : s'assurer que les contrats comportent déjà les mentions obligatoires prévues par l'article 28 du RGPD et figurant dans le modèle ci-après. Dans le cas contraire, pensez à mettre à jour vos contrats en signant un avenant reprenant le modèle proposé et complété.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

ANNEXE AU CONTRAT DE SOUS-TRAITANCE

La présente annexe « Protection des Données personnelles » est partie intégrante du contrat.

Les Parties acceptent de se conformer à la réglementation applicable à la protection des données personnelles et en particulier le Règlement européen sur la protection des données du 27 avril 2016 (le « RGPD ») et la loi Informatique et Libertés du 6 janvier 1978 modifiée.

Préambule[1]

Pour les besoins de gestion de son officine, la pharmacie[2] _____ a souhaité se doter d'un logiciel de gestion d'officine. Pour ce faire, elle s'est rapprochée de la société[3] _____, éditeur de logiciel de gestion pour les pharmacies, qui propose des outils à cet effet.

Dans ce cadre, la société[3] _____ (ci-après le « Sous-traitant ») pourra être amenée à traiter des données personnelles pour le compte de la pharmacie[2] _____ (ci-après le « Responsable du traitement »).

Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable du traitement les opérations de traitement de données personnelles définies ci-après.

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

Dans le cadre du présent contrat, le Sous-traitant traite les données personnelles suivantes des[4] _____ _____ (ci-après les « **Personnes concernées** ») :

[5] _____ _____ (ci-après les « **Données personnelles** »)

pour répondre à la ou les finalité(s) du traitement suivante(s)[6] : _____ _____.

<u>À LA SUITE DE QUOI, IL A ETE DECIDE CE QUI SUIT :</u>

ARTICLE 1 : OBLIGATIONS DE CONFIDENTIALITE

Chaque partie s'engage à garder strictement confidentielles et à ne pas divulguer à des tiers, par quelque moyen que ce soit, les informations qui lui seront transmises ou auxquelles elle aura accès à l'occasion de l'exécution du présent contrat.

ARTICLE 2 : OBLIGATIONS DU SOUS-TRAITANT

Le Sous-traitant s'engage à :

- Ne traiter les données que pour les finalités définies par le Responsable du traitement et conformément à ses instructions. Il informera le Responsable du traitement en cas d'instruction qui apparaîtrait contraire à la Réglementation applicable à la protection des données personnelles.
- Prendre toutes mesures techniques et organisationnelles appropriées afin de garantir la confidentialité des Données personnelles traitées et un niveau de sécurité conforme à la réglementation applicable à la protection

[1] Exemple de préambule pour un éditeur de LGO : à adapter en fonction du prestataire concerné
[2] Indiquer le nom de la pharmacie
[3] Indiquer le nom du prestataire
[4] Indiquer les catégories de personnes *(exemple : employés, patients, professionnels de santé, contacts, etc.)*
[5] Lister les différentes données qui seront traitées par votre sous-traitant *(exemple : nom, prénom, etc.)*
[6] À compléter *(exemple : maintenance, hébergement des données des patients du Responsable du traitement)*

des Données personnelles. À ce titre, il s'engage à ce que les personnes autorisées à traiter les Données personnelles pour le compte du Responsable du traitement soient soumises à une obligation de confidentialité.
- Ne pas transférer les Données personnelles hors de l'Union européenne.
- Informer le Responsable du traitement de toute violation de données à caractère personnelles dans les meilleurs délais et au plus tard dans les 48 heures après en avoir eu connaissance.
- Informer le Responsable du traitement, dans le cas où il ferait appel à un sous-traitant ultérieur pour traiter les Données personnelles confiées par le Responsable du traitement. À ce titre, il s'engage à ce que ce sous-traitant ultérieur soit soumis à des obligations au moins équivalentes à celles fixées par le présent contrat et demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution par ce sous-traitant ultérieur de ses obligations.
- Mettre à la disposition du Responsable du traitement toute information nécessaire pour démontrer le respect des obligations décrites dans le présent contrat et pour permettre la réalisation d'audits de conformité.
- Assister le Responsable du traitement dans la mise en œuvre de l'exercice des droits des personnes concernées.

Les Parties s'engagent à coopérer avec l'autorité de contrôle en matière de protection des Données personnelles en cas de demande d'information qui pourrait être adressée ou en cas de contrôle effectué.

ARTICLE 3 : DUREE DE CONSERVATION ET RESTITUTION DES DONNEES

Le Sous-traitant s'engage à retourner au Responsable du traitement l'intégralité des Données personnelles des personnes concernées collectées pour le compte du Responsable du traitement et à supprimer définitivement toute copie restante de ces Données personnelles dans les quinze jours au terme du contrat. Il s'engage à communiquer, sur simple demande du Responsable du traitement, toute attestation de destruction de ces données.

ARTICLE 4 : RESPONSABILITE

Le Sous-traitant s'engage à indemniser le Responsable du traitement de tous dommages liés (i) à l'atteinte à la sécurité, l'intégrité ou la confidentialité des Données personnelles résultant du manquement de ses obligations au titre du présent contrat, (ii) à toute violation de la réglementation applicable à la protection des données personnelles et (iii) à tout préjudice d'image ou de réputation lié à un manquement du Sous-traitant à ses obligations au titre du présent contrat.

ARTICLE 5 : JURIDICTION COMPETENTE ET LOI APPLICABLE

Le présent contrat est soumis à la loi française et tout litige né de ce contrat relève de la compétence des juridictions de[1] _____.

Fait à[1] _____
Le[1] _____

En[2] _____ exemplaires originaux.

[1] À compléter
[2] À compléter par le nombre de parties au contrat

☐ Respect de ses obligations par votre sous-traitant

☐ Utilisation des données conformément à ce qui est défini dans le contrat

Le sous-traitant ne peut pas utiliser les données pour d'autres raisons que celles définies dans le contrat.

☐ Recours à son propre sous-traitant

Conditions requises pour que votre sous-traitant recourt à son propre sous-traitant :

- Vérifier que son sous-traitant respecte le RGPD
- Obtenir votre autorisation spécifique ou générale écrite au préalable
- Vous informer de tout changement

> **IMPORTANT :**
> Votre sous-traitant reste responsable des manquements de son sous-traitant.

Pour en savoir plus :
Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles

☐ En cas de demandes d'exercice de droit

Votre sous-traitant doit vous aider à répondre à toute demande d'exercice des droits, soit en y répondant directement, soit en vous en informant sans délai.

☐ En cas de violation des données personnelles

Votre sous-traitant doit vous signaler toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance.

BONNES PRATIQUES :

Indiquer dans le contrat un délai compris entre 24h et 48h pour vous permettre le cas échéant de notifier ladite violation à la CNIL dans le délai imparti, soit 72h après en avoir pris connaissance.

☐ En cas de contrôle de la CNIL

Votre sous-traitant doit vous aider pour démontrer le respect de vos obligations.

> **IMPORTANT :**
> En cas de manquements, la CNIL peut sanctionner tant le responsable du traitement que le sous-traitant.

☐ Tenir un registre pour votre compte

Votre sous-traitant doit recenser les traitements que vous lui confiez dans un registre qu'il tient pour votre compte.

Pour en savoir plus :
Le registre des activités de traitement

> **IMPORTANT :**
> N'oubliez pas de votre côté de compléter une fiche de registre pour le traitement de la gestion de vos fournisseurs.

☐ **En cas de nécessité de réaliser une analyse d'impact**

Dans ce cas, votre sous-traitant doit vous aider dans la réalisation de votre analyse d'impact.

BONNES PRATIQUES :

Demandez à votre sous-traitant s'il n'en a pas déjà réalisé une pour ce traitement, qui pourra ensuite être adaptée si nécessaire.

☐ **Fin du contrat**

À la fin du contrat ou en cas de résiliation de celui-ci, votre sous-traitant devra supprimer les données ou vous les restituer en fonction de ce que vous aurez défini dans le contrat.

BONNES PRATIQUES :

Dans le cas où vous optez pour la suppression des données, pensez à demander à votre sous-traitant un document justifiant de leur destruction par un moyen sécurisé.

FICHE N° 4 – Quelles sont vos obligations en cas d'installation d'un dispositif vidéo ?

Pour assurer la sécurité des biens et des personnes dans votre officine contre les risques de vols, de dégradations et d'agressions par exemple, vous pouvez décider d'installer un dispositif vidéo. Peu importe que celui-ci soit accessible depuis votre officine ou à partir d'un appareil connecté, les règles ci-dessous sont applicables.

Ce que vous pouvez faire

- Filmer les zones de circulation des patients dans l'officine à des fins de sécurité et dans le respect de leur vie privée
- Filmer les collaborateurs qui manipulent de l'argent ou des médicaments stupéfiants, qui sont impérativement conservés dans une armoire fermée à clé
- Filmer les lieux de stocks et les réserves

Ce que vous ne devez pas faire

- Placer vos collaborateurs sous une surveillance constante et permanente
- Filmer les zones de repos des collaborateurs ou les toilettes

Pour en savoir plus :
Vous pouvez consulter notamment les pages du site de la CNIL relatives au dispositif vidéo au travail, dans les commerces et sur la voie publique.

☐ Informer les personnes filmées

BONNES PRATIQUES :

La CNIL recommande de prévoir deux niveaux d'information (voir ci-dessous).

BOITE À OUTILS :
Pour informer les personnes filmées, vous pouvez utiliser les modèles de mentions d'information figurant ci-après.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

NIVEAU 1 DE L'INFORMATION :

PANNEAU D'INFORMATION AFFICHÉ DANS LES LOCAUX DE LA PHARMACIE

ETABLISSEMENT SOUS SURVEILLANCE VIDEO

Etablissement placé sous vidéosurveillance par la pharmacie [1] _____ pour la sécurité des personnes et des biens.

Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de la pharmacie[1] _____ et par les forces de l'ordre.

Conformément à la réglementation applicable à la protection des données, vous pouvez exercer votre droit d'accès aux images qui vous concernent ou demander toute information sur ce dispositif en écrivant à la pharmacie à l'adresse e-mail suivante[2] : _____ ou à l'adresse postale suivante[2] : _____.

Vous pouvez également, si vous l'estimez nécessaire, introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Pour plus d'informations, nous vous invitons à consulter notre note d'information disponible[3] _____.

IMPORTANT :
Ce panneau doit être placé à une distance raisonnable des lieux surveillés de manière à ce que la personne puisse facilement reconnaître la zone surveillée.

[1] Indiquer le nom de la pharmacie
[2] À compléter
[3] À adapter *(exemple : au niveau du comptoir)*

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

NIVEAU 2 DE L'INFORMATION :

NOTE D'INFORMATION DESTINEE À VOS PATIENTS ET À VOTRE PERSONNEL

La pharmacie [1] _____ située à [2] _____ a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité des personnes et de ses biens et lutter, ainsi, contre les vols et les agressions.

En tant que responsable du traitement, la pharmacie[1] _____ collecte des images de son personnel, des patients et des visiteurs. Ces images ne sont pas utilisées à des fins de surveillance du personnel, ni de contrôle des horaires.

*Les images peuvent être visionnées, **en cas d'incident**, par le personnel habilité de la pharmacie[1] _____ et par les forces de l'ordre, ainsi que le personnel de la société en charge de la maintenance du matériel agissant en qualité de sous-traitant[3].*

Ces images sont conservées pendant un mois à compter de leur enregistrement. En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif.

Elles sont alors conservées sur un support distinct le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition et d'un droit à la limitation du traitement de vos données. Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez nous contacter par voie électronique[4] :
_____ ou à l'adresse postale suivante[4] : _____
_____.

Vous pouvez également, si vous l'estimez nécessaire, introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

BONNES PRATIQUES :

Pour vos patients : vous pouvez mettre cette note d'information à leur disposition au niveau des comptoirs par exemple.

Pour votre personnel : vous pouvez leur remettre en main propre.

[1] Indiquer le nom de la pharmacie
[2] Indiquer l'adresse de la pharmacie
[3] Conserver si applicable
[4] À compléter

☐ Formalités à accomplir

☐ Pour les lieux non ouverts au public *(exemples : réserves, lieux de stocks, …)*

Pas de formalité particulière à accomplir.

Pensez seulement à compléter une fiche de registre relative à ce traitement et à associer votre DPO à l'installation de ce dispositif, le cas échéant.

☐ Pour les lieux ouverts au public *(exemples : comptoirs, devantures, …)*

Le dispositif mis en place doit être autorisé préalablement par le préfet du département.

Pour cela, vous pouvez compléter le formulaire de déclaration accessible sur le site du ministère de l'Intérieur ou procéder à une déclaration en ligne.

Comme pour les lieux non ouverts au public, vous devez également compléter une fiche de registre relative à ce traitement.

> **!** **IMPORTANT :**
> Dès lors que la mise en œuvre d'un dispositif de vidéo dans un lieu ouvert au public est susceptible de conduire à la « surveillance systématique à grande échelle d'une zone accessible au public », il est recommandé de s'interroger sur la nécessité d'effectuer une analyse d'impact.

FICHE N° 5 – Comment réagir en cas de violation de données ?

Malgré les mesures de sécurité mises en place dans votre officine, il se peut que vous constatiez une violation des données personnelles que vous traitez. Dans ce cas, le RGPD vous impose certaines obligations.

Pour en savoir plus :
Les violations de données personnelles

☐ Identifier la violation de données personnelles

Constitue une violation de données personnelles tout incident de sécurité ayant comme conséquence de compromettre :

- L'intégrité des données personnelles (altération des données) ;
- La confidentialité des données (divulgation ou accès non autorisés aux données) ;
- La disponibilité des données (destruction ou perte des données rendant impossible leur consultation pour les personnes autorisées).

Peu importe que cet incident soit d'origine accidentelle ou non, ou encore qu'il se produise dans les locaux de votre officine ou chez votre prestataire.

Exemples :

- *La modification accidentelle des données de santé d'un patient dans votre LGO ;*
- *Laisser à la vue de tous les résultats d'un test antigénique d'un patient ;*
- *Attaque par un logiciel malveillant vous empêchant d'accéder aux données figurant dans votre LGO tant que vous n'avez pas versé une rançon ;*
- *Vol ou perte de l'ordonnancier de votre officine.*

☐ Tenir un registre des violations

Toute violation de données personnelles doit être documentée en interne. Cela peut prendre la forme d'un registre comportant au minimum les informations suivantes :

- **La nature de la violation** *(exemples : atteinte à l'intégrité, la disponibilité ou la confidentialité des données)* ;
- **Les catégories et le nombre approximatif des personnes concernées** *(exemples : 200 patients, 5 employés, etc.)* ;
- **Les catégories et le nombre approximatif d'enregistrements de données personnelles concernées** *(exemples : 200 pages de l'ordonnancier, 120 minutes d'images vidéo du mois de septembre, etc.)* ;
- **Les conséquences probables de la violation** *(exemples : risque d'usurpation d'identité, risque d'interactions médicamenteuses ou de redondances de traitements, etc.)* ;
- **Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation** *(exemples : modifications des droits d'accès, chiffrement des données, etc.)* ;
- **Le nom et les coordonnées de la personne à contacter**.

BONNES PRATIQUES :

Vous pouvez vous aider du document préparatoire pour le formulaire de notification mis en ligne par la CNIL.
Il vous servira de canevas pour la documentation interne et peut constituer un outil utile de gestion de la conformité en matière de violations de données personnelles.

☐ Notifier la violation à la CNIL

Dans quels cas notifier à la CNIL ?

Lorsque cette violation fait peser un risque sur les droits et libertés des personnes dont les données ont été impactées.

Exemples :

- *La perte définitive des données des patients suite à un incendie ;*
- *La publication sur internet ou la perte définitive des données de santé de vos patients ;*
- *La divulgation d'une maladie au conjoint d'un patient sans y être autorisé ;*
- *Le piratage du système informatique de l'officine contre une rançon ;*
- *La panne de courant dans l'officine pendant plusieurs heures rendant les dossiers patients indisponibles.*

En revanche, lorsque vous perdez un appareil mobile chiffré de façon sécurisée et utilisé par vous et votre personnel, vous n'aurez pas besoin de notifier la violation à la CNIL :

- si la clé de chiffrement reste en votre possession,
- et les données personnelles affectées ne constituent pas une copie unique.

Comment notifier à la CNIL ?

Il suffit de compléter le formulaire de téléservice mis à votre disposition sur le site internet de la CNIL, en y indiquant les informations que vous avez consignées à ce titre dans votre registre.

La CNIL pourra vous demander des informations complémentaires si besoin.

Dans quel délai notifier ?

Dans les meilleurs délais et au plus tard 72h après en avoir pris connaissance.

Si vous ne disposez pas de toutes les informations lors de votre notification initiale, vous pouvez la compléter par la suite à l'aide d'une notification complémentaire. Cette notification complémentaire doit intervenir si possible dans un délai maximal de 72h. Si le délai de 72h est dépassé, les raisons de ce retard seront à justifier auprès de la CNIL.

☐ Communiquer la violation aux personnes concernées

Dans quels cas informer les personnes concernées ?

Lorsque le risque sur les droits et les libertés de ces personnes est élevé.

Comment communiquer auprès des personnes ?

La communication doit se faire directement auprès de la personne et peut se faire par tout moyen permettant de s'assurer que la personne a bien été informée (email, SMS …). Si cette information individuelle exige des efforts disproportionnés, il sera alors procédé à une communication plus générale (message sur site web …).

La communication doit se faire en des termes clairs et précis et contenir au minimum les informations suivantes :

- La nature de la violation ;
- Les conséquences probables de la violation ;
- Les coordonnées de la personne à contacter ;
- Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

Dans quel délai communiquer ?

« Dans les meilleurs délais », en d'autres termes aussi vite que possible afin de permettre aux personnes concernées de prendre des mesures pour se protéger contre toute conséquence négative de la violation.

BONNES PRATIQUES :

Pensez à mettre en place une procédure interne de violation de données personnelles, afin de sensibiliser votre personnel et leur permettre d'adopter, le cas échéant, les bons réflexes pour être en mesure de réagir dans les délais impartis.

FICHE N° 6 – Comment réagir en cas de contrôle de la CNIL ?

Qui est la CNIL ? La Commission nationale de l'informatique et des libertés (CNIL) est le régulateur français des données personnelles. La CNIL accompagne les acteurs privés et publics dans la mise en œuvre de leur conformité en matière de protection des données personnelles.

Dans le cadre de ses missions, elle dispose également de pouvoirs de contrôle sur les organismes. Ces contrôles peuvent faire suite à une réclamation ou au signalement d'un particulier, lorsqu'un organisme ne répond pas à une demande d'exercice des droits, par exemple.

Pour en savoir plus :
Comment se passe un contrôle de la CNIL ?
Contrôles de la CNIL : une charte pour tout comprendre

☐ Déroulement d'un contrôle de la CNIL

La CNIL peut procéder à différents types de contrôles :

- **Contrôle sur place** : les agents de la CNIL se rendent directement dans l'officine. Ils peuvent prendre copie de tout document papier ou numérique (contenu d'un ordinateur ou d'un serveur, contenu d'une messagerie, extraction d'enregistrements de caméras de vidéosurveillance, copie des notes d'information, copie des contrats, …) et s'entretenir avec tout membre du personnel.

> ! **IMPORTANT :**
> Au titre de la loi Informatique et Libertés, l'accès aux données médicales individuelles couvertes par le secret médical ne peut se faire « *que sous l'autorité et en présence d'un médecin* ».[1]

- **Audition du responsable de traitement** : le titulaire de l'officine est convoqué dans les locaux de la CNIL à la date indiquée sur la convocation pour répondre aux questions de la CNIL.

- **Contrôle en ligne** : les agents de la CNIL effectuent des vérifications en consultant toute donnée librement accessible (par exemple : le site internet de l'officine), y compris par négligence ou du fait d'un tiers.

- **Contrôle sur pièces** : la CNIL peut adresser un courrier au titulaire de l'officine pour lui demander de répondre à des questions par écrit, et d'y joindre tout document utile.

> ! **IMPORTANT**
> Conformément à l'article 226-22-2 du code pénal, l'entrave à l'action de la CNIL est punie d'un an d'emprisonnement et de 15 000 € d'amende. C'est le cas par exemple de la personne qui dissimulerait ou détruirait des renseignements ou documents utiles à la mission de contrôle des agents de la CNIL.

[1] L'article 36 du décret du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés précise que « *Lorsque les opérations de vérification nécessitent l'accès à des données médicales individuelles, dans les cas prévus au III de l'article 19 de la loi du 6 janvier 1978 susvisée, le préfet ou, selon le cas, le directeur général de l'agence régionale de santé dans le ressort territorial duquel doit avoir lieu le contrôle désigne, à la demande du président de la commission, un médecin inspecteur du travail ou un médecin chargé de requérir la communication de ces données ; le président de la commission peut également désigner un médecin inscrit sur une liste d'experts judiciaires.* »

☐ Issue d'un contrôle de la CNIL

La présidente de la CNIL peut notamment décider de :

- **Clore la procédure de contrôle avec ou sans observation ;**
- **Mettre en demeure le responsable du traitement** d'adopter des mesures nécessaires pour remédier aux manquements constatés dans un délai imparti et, éventuellement, de justifier des mesures prises et décider de rendre publique cette mise en demeure ;
- **Prononcer un rappel aux obligations légales** à l'encontre du responsable de traitement ;
- **Transmettre le dossier à la formation restreinte de la CNIL qui pourra prononcer des sanctions à l'encontre du responsable du traitement** (allant du rappel à l'ordre au paiement d'une amende administrative pouvant atteindre jusqu'à 20 000 000 € ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent) et qui pourra **rendre publique sa décision** en la publiant sur son site internet.

> ! **IMPORTANT :**
> En plus des sanctions administratives prononcées par la CNIL, des sanctions pénales peuvent être prononcées par les juridictions répressives pouvant aller jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende pour une personne physique (articles 226-16 et suivants du code pénal) et 1 500 000 € d'amende pour une personne morale (articles 131-38 et 226-24 du code pénal).

Quelques illustrations de sanctions prononcées :

- En 2023 la CNIL a rappelé à deux organismes procédant à des recherches médicales leurs obligations de réaliser une AIPD et d'informer correctement les personnes.
- En 2022, la CNIL a sanctionné la société Dedalus Biologie d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500 000 personnes.
- En 2021, la CNIL a mis en demeure la société privée Francetest de sécuriser les données de santé qu'elle collecte pour le compte des pharmacies à l'occasion de tests de dépistage à la COVID-19. Elle s'est également rapprochée de plus de 300 pharmacies afin qu'elles vérifient leur conformité au RGPD et à l'obligation de sécurité.
- En 2020, la CNIL a prononcé deux amendes de 3 000 € et 6 000 € à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL.
- En 2019, la CNIL a mis en demeure un organisme de mettre en conformité son dispositif de vidéosurveillance considéré comme contraire au RGPD, dans la mesure où il plaçait ses collaborateurs sous surveillance constante.
- En 2019, l'autorité britannique de protection des données (l'*Information Commissioner's Office*, soit l'équivalent de la CNIL) a infligé une amende de 275 000 £ à une pharmacie pour avoir enfreint les règles du RGPD. Il est reproché à cette pharmacie, qui fournit des médicaments à des milliers de résidents de maisons de retraite, d'avoir jeté 500 000 documents médicaux contenant des informations sensibles à l'extérieur dans des conteneurs déverrouillés.

☐ Préparation à un contrôle de la CNIL

BONNES PRATIQUES :

Tenir et mettre à jour l'ensemble des documents que la CNIL pourrait vous demander en cas de contrôle.

Modèle à compléter et à adapter en fonction des traitements de données personnelles mis en œuvre dans votre officine

CHECK-LIST DE LA DOCUMENTATION RGPD :

CHECK-LIST DE LA DOCUMENTATION RGPD

La documentation portant sur vos traitements de données personnelles

- ☐ Le registre des traitements de données à caractère personnel de votre pharmacie
- ☐ Si cela est requis : les analyses d'impact réalisées
- ☐ Si transfert de données hors de l'Union européenne : les garanties apportées pour encadrer ces transferts *(exemples : clauses contractuelles types)*

La documentation relative à l'information et aux droits des personnes concernées

- ☐ Les mentions d'information
- ☐ Les modèles de recueil du consentement des personnes concernées, le cas échéant
- ☐ La procédure mise en place pour l'exercice des droits des personnes concernées, ou à défaut un document démontrant la sensibilisation de votre personnel sur cette thématique

La documentation relative aux contrats conclus avec vos sous-traitants

- ☐ Les contrats conclus avec vos sous-traitants conformes au RGPD
- ☐ La documentation démontrant la conformité de vos sous-traitants *(exemples : documentation relative à leurs mesures de sécurité, certificat pour un hébergeur de données de santé, etc.)*

La documentation relative à la sécurité de vos traitements

- ☐ La procédure de violation de données personnelles, ou à défaut un document démontrant la sensibilisation de votre personnel sur cette thématique
- ☐ Le registre des violations de données personnelles

ORDRE NATIONAL DES PHARMACIENS
4 avenue Ruysdaël – 75379 Paris Cedex 08
Tél. 01 56 21 34 34
www.ordre.pharmacien.fr

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES
3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07
Tél. 01 53 73 22 22
www.cnil.fr