

RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNEES A
CARACTERE PERSONNEL DESTINES A LA
GESTION DES OFFICINES DE PHARMACIE

PI

1. A qui s'adresse ce référentiel ?

1.1 Ce référentiel, pris en application des dispositions de l'article 8-I-2-b de la loi « informatique et libertés » du 6 janvier 1978 modifiée (LIL), vise à faciliter la mise en conformité des traitements de données à caractère personnel mis en œuvre au sein des officines de pharmacie dans le cadre de la prise en charge sanitaire et de la gestion administrative de leur patientèle/clientèle.

1.2 Il s'adresse aux officines de pharmacie libérales et à leurs prestataires.

- 1.3 Ne sont pas concernés par ce référentiel en raison de leurs spécificités, les traitements mis en œuvre :
- par les entreprises et établissements pharmaceutiques de fabrication et de distribution de gros ou par les laboratoires d'analyses de biologie médicale ;
 - dans le cadre de l'alimentation du dossier pharmaceutique (DP) prévu par l'article L. 1111-23 du code de la santé publique (CSP) ;
 - au cours du déploiement du télésoin dans les officines ;
 - dans le cadre de la vente en ligne de médicaments ;
 - dans le cadre de la lutte contre l'épidémie de covid (SI-DEP) ;
 - au sein des pharmacies à usage intérieur (PUI).

2. Portée du référentiel

2.1 Les traitements visant à permettre la prise en charge sanitaire et la gestion administrative au sein des officines, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques identifiées ou identifiables (patients, professionnels de santé, etc.). A ce titre, ils sont soumis aux dispositions du règlement général sur la protection des données (RGPD), de la LIL ainsi qu'aux dispositions du CSP.

2.2 Le responsable des traitements mis en œuvre dans le cadre des officines de pharmacie est soit le pharmacien titulaire de l'officine lorsqu'il exerce son activité en tant qu'entrepreneur individuel, soit la société personne morale à travers laquelle il exerce son activité. *A contrario*, un interne en pharmacie ou un pharmacien salarié ne peut être considéré comme étant responsable d'un traitement mis en œuvre dans le cadre de la gestion de l'officine de pharmacie.

2.3 Le responsable de traitement doit mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles dès la conception des traitements et tout au long de la vie de ceux-ci. Il doit, en outre, être en mesure de démontrer cette conformité à tout instant.

2.4 Les traitements mis en œuvre au sein des officines de pharmacie doivent être inscrits dans le registre prévu à l'article 30 du RGPD.

Pour plus d'informations :

- Consulter « [le registre des activités de traitement](#) » sur le site [cnil.fr](#)

2.5 **Ce référentiel n'a pas de valeur contraignante. Il permet en principe d'assurer la conformité des traitements de données mis en œuvre au sein des officines de pharmacie aux principes relatifs à la protection des données et au secret professionnel, dans un contexte d'évolution des pratiques à l'ère numérique.**

2.6 Les pharmacies qui souhaiteraient s'écarter du référentiel au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin, puis prendre toutes les mesures appropriées à même de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

2.7 Le référentiel n'a pas pour objet d'interpréter les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent trouver à s'appliquer.

2.8 Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans le cas où celle-ci est requise.

Pour plus d'informations :

- consulter la page « [Analyse d'impact relative à la protection des données : publication d'une liste de traitements pour lesquels une analyse est requise](#) »

2.9 La CNIL publie régulièrement des guides pratiques afin d'accompagner les professionnels dans la mise en œuvre des obligations prévues par la réglementation sur la protection des données personnelles que ces derniers sont invités à consulter en complément du présent référentiel.

Pour plus d'informations :

- consulter notamment la page « [Les outils de la conformité](#) »

3. Objectifs poursuivis par le traitement (FINALITES)

3.1 Les traitements mis en œuvre doivent répondre à un objectif précis et être justifiés au regard des missions et des activités réalisées au sein de l'officine de pharmacie. Ils permettent notamment :

- la dispensation des médicaments, produits et dispositifs médicaux ;
- le conseil pharmaceutique ;
- la contribution aux soins de premier recours définis à l'article L. 1411-11 du CSP ;
- la coopération entre professionnels de santé ;
- la permanence des soins ;
- la contribution aux actions de veille et de protection sanitaires organisées par les autorités ;
- la participation à l'éducation thérapeutique et aux actions d'accompagnement des patients/clients définies aux articles L. 1151-1 à L. 1161-5 du CSP.

3.2 Les traitements permettent, **notamment, pour les besoins de la dispensation des médicaments :**

- la tenue du registre de délivrance ;
- la gestion et la tenue des dossiers nécessaires au suivi du patient/client (à l'exclusion du Dossier pharmaceutique (DP)) ;
- la communication et la coordination entre professionnels identifiés participant à la prise en charge de la personne concernée ;
- l'établissement et la télétransmission des documents destinés à la prise en charge des frais de santé par l'assurance maladie (prescriptions, etc.) ;
- la tenue de la comptabilité.

3.3 Les données personnelles doivent être traitées dans le respect de la vie privée des patients/clients et dans le respect du secret des informations les concernant, conformément à l'article L. 1110-4 du CSP.

3.4 Elles peuvent être réutilisées pour des recherches, des études ou des évaluations réalisées par les personnels assurant le suivi du patient/client et destinées à leur usage exclusif (recherche interne), sans nécessiter une autorisation de la CNIL.

3.5 A défaut, cette réutilisation devra faire l'objet de formalités en application des articles 66 et 72 et suivants de la loi « informatique et libertés » portant sur les traitements à des fins de recherches, d'étude ou d'évaluation dans le domaine de la santé.

Pour plus de détails sur la recherche dans le domaine de la santé :

- [Fiche](#) « Recherche médicale : quel est le cadrer légal ? »

4. Base(s) légale(s) du traitement

- 4.1 Chaque finalité du traitement doit reposer sur l'une des bases légales fixées par la réglementation.
- 4.2 Il appartient au responsable de traitement de déterminer ces bases légales avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte. Ayant des conséquences sur l'exercice de certains droits, ces bases légales font partie des informations devant être portées à la connaissance des personnes concernées.
- 4.3 Afin d'aider les responsables de traitement dans cette analyse, le présent référentiel propose, à titre indicatif, un choix de base légale dans le tableau ci-dessous¹.

Finalités	Bases légales envisageables ²
La tenue du registre de délivrance	Obligation légale (notamment R. 5125-45 CSP)
L'établissement et la télétransmission des documents à destination de l'assurance maladie	Obligation légale
La tenue de la comptabilité	Intérêt légitime

Pour plus d'informations :

- Pour plus d'informations consulter la page « [La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD](#) »

5. Données personnelles concernées

- 5.1 Dans un souci de minimisation des données personnelles traitées, le responsable de traitement doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de prise en charge sanitaire et de gestion administrative de l'officine de pharmacie. Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :
- l'identité et coordonnées du patient/client** (telles que le nom, prénom, date de naissance, adresse postale, adresse électronique et numéro de téléphone) ;
 - l'identifiant national de santé (INS)** pour la prise en charge sanitaire d'un patient/client dans le cadre de la délivrance de produits remboursés ;
 - le numéro de sécurité sociale (NIR)** à des fins de facturation et de prise en charge financière des dépenses de santé dans le cadre de la délivrance de produits remboursés ;
 - données relatives à la santé** (telles que le poids, la taille, les antécédents médicaux, les diagnostics médicaux, les traitements prescrits, traitements délivrés, produits vendus, des renseignements propres à influencer la réaction du patient/client à sa prise en charge médicale et tout élément de nature à caractériser la santé du patient/client à la délivrance de conseils, médicaments, produits ou dispositifs médicaux) ;
 - les traces fonctionnelles** (celles qui rendent compte des actions « métier » des utilisateurs ou des machines au sein du système d'information) **et techniques** (celles qui rendent compte de « l'activité » des composants logiciels et matériels utilisés par le système d'information pour assurer la fonctionnalité sollicitée par un utilisateur ou une machine).

Pour plus de détails sur la gestion des traces fonctionnelles :

- [Guide AIPD](#) « Les bases de connaissance »

- 5.2 Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il utilise, le responsable de traitement doit par ailleurs vérifier, tout au long de la durée de vie du traitement, la qualité des données traitées. En pratique, cela signifie que les données doivent être exactes et mises à jour conformément à la réglementation.

¹ D'autres bases légales, telles que le contrat ou l'intérêt public, pourraient également être retenues.

² Sous réserve de choix différents justifiés par un contexte spécifique.

6. Destinataires des données

Les données personnelles ne devraient être rendues accessibles qu'aux seules personnes habilitées à en connaître au regard de leurs attributions. D'une manière générale, les habilitations d'accès devraient être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité.

Peuvent être amenées à accéder aux données des patients/clients pour l'accomplissement de leurs missions et en vertu de dispositions législatives les personnes suivantes :

6.1. Les personnes accédant aux données pour le compte et sous l'autorité du responsable de traitement

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions peuvent accéder aux données à caractère personnel traitées, dans le respect des dispositions sur le secret professionnel et dans la stricte limite de leurs attributions respectives et de l'accomplissement de ces missions et fonctions.

Il peut s'agir, par exemple des personnels de l'officine participant à la délivrance des produits de santé et de conseils.

6.2 Les destinataires des données

Le RGPD définit les destinataires comme « tout organisme qui reçoit la communication des données ».

Avant toute communication des informations, le responsable de traitement doit, d'une part, s'interroger sur la finalité de la transmission pour s'assurer de sa pertinence et de sa légitimité et, d'autre part, vérifier que les données communiquées sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Peuvent notamment être destinataires des données (liste non exhaustive) :

- **les professionnels de santé et les professionnels concourant à la prévention et aux soins**, afin d'assurer la continuité des soins dans le respect des dispositions des articles L. 1110-4 et L. 1110-12 du code de la santé publique ;
- afin de permettre le remboursement des actes, des prestations et leur contrôle, **les personnels des organismes d'assurance maladie obligatoire**, qui ont connaissance, dans le cadre de leurs fonctions et pour la durée nécessaire à l'accomplissement de celles-ci, de l'identité de leurs assurés et ayants droits, de leur numéro de sécurité sociale et des numéros de code des actes exécutés et prestations servies dans les conditions définies à l'article L. 161-29 du code de la sécurité sociale ;
- **les organismes menant des études, recherche et évaluations dans le domaine de la santé**, qui peuvent être destinataires de données personnelles de santé dans les conditions définies par le RGPD et la loi « informatique et libertés » (notamment dans le respect du principe de la minimisation des données).

6.3 Les sous-traitants

Le RGPD définit le sous-traitant comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Il peut s'agir, par exemple, des prestataires de services informatiques (ex : maintenance du logiciel et des postes de travail utilisés dans l'officine de pharmacie, etc.) ou encore de tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme (ex. : la gestion de la paie des salariés, etc.).

Le responsable de traitement qui souhaite avoir recours à un prestataire de services pour traiter des données personnelles pour son compte (société de maintenance, plateforme en ligne, hébergeur de données de santé agréé ou certifié), doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Ce contrat **devra mentionner que le prestataire, en tant que sous-traitant :**

- ne traite les données à caractère personnel **que sur instruction du responsable de traitement** ;

- veille à la **signature d'engagements de confidentialité par le personnel** ;
- **prend toutes les mesures de sécurité requises au regard des objectifs de sécurité qui lui sont fixés par le responsable de traitement** ;
- **ne recrute pas de sous-traitant sans autorisation écrite préalable du responsable de traitement** ;
- **coopère avec le responsable de traitement** pour le respect de ses obligations, notamment lorsque des patients/clients ont des demandes concernant leurs données ;
- **supprime ou renvoie** au responsable de traitement l'ensemble des données à caractère personnel à l'issue des prestations ;
- **met à la disposition du responsable du traitement toutes les informations** nécessaires pour démontrer le respect des obligations pour permettre la réalisation d'audits.

Le prestataire doit, en sa qualité de sous-traitant, tenir un registre des activités de traitement dans les conditions de l'article 30.2 du RGPD.

Le prestataire doit, en cas d'incident lié aux données qu'il gère pour le compte du responsable de traitement (faible de sécurité, piratage, perte, etc.) l'en informer dans les meilleurs délais, afin que ce dernier puisse respecter ses propres obligations de gestion et de notification de l'incident. Le contrat signé entre le responsable de traitement et son sous-traitant devrait prévoir les modalités de notification du sous-traitant au responsable de traitement.

Pour plus de détails sur la sous-traitance :

- Rubrique « [Travailler avec un sous-traitant](#) »
- [Guide](#) d'accompagnement des sous-traitants

- **Exemple : la maintenance du logiciel et des postes de travail utilisés dans l'officine de pharmacie**

En cas de recours à un prestataire de service pour assurer la maintenance du logiciel et des postes de travail utilisés dans l'officine de pharmacie, celui-ci accède aux données personnelles dans le respect du secret professionnel. La sécurité des données doit être garantie et leur confidentialité préservée. À ce titre, des mesures physiques et logiques doivent être mises en œuvre, telles que le chiffrement, afin de permettre au technicien d'assurer ses missions sans pouvoir lire ces données.

7. Durées de conservation

7.1. La conservation des données à caractère personnel

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité : ces données ne peuvent en effet pas être conservées pour une durée indéfinie.

La durée de conservation des données ou, lorsqu'il est impossible de la fixer, les critères utilisés pour déterminer cette durée, font partie des informations qui doivent être communiquées aux personnes concernées. Dans ces conditions, il incombe au responsable du traitement de déterminer cette durée en amont de la réalisation du traitement.

Au regard des finalités de gestion de l'officine de pharmacie, les données relatives à la délivrance doivent être conservées à la fois en base active pour consultation habituelle et dans un registre conservé en réserve. Conformément à l'article R. 5125-45 du code de la santé publique, les données du registre doivent être archivées pendant une durée de dix ans.

Dans le cadre de la délivrance de produits particuliers, certaines durées de conservation particulières doivent en outre être appliquées (ex : les registres ou enregistrements liés aux médicaments dérivés du sang doivent être conservés pendant une durée de 40 ans, conformément à l'article R. 5121-195 du CSP).

Les doubles des feuilles de soins électroniques doivent être conservés trois mois, conformément à l'article R.161-47 du code de la sécurité sociale.

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

Il revient aux prestataires fournissant des solutions logicielles d'intégrer des fonctionnalités d'archivage automatique à date d'échéance. À défaut, le responsable de traitement devrait y procéder manuellement.

De même, les traces (techniques et fonctionnelles) des solutions logicielles devraient être conservées pendant une durée de six mois minimum ; cette durée peut être étendue si cela s'avère nécessaire pour traiter certains risques pesant sur les personnes.

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

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

- [« Sécurité : Archiver de manière sécurisée »](#)
- [« Limiter la conservation des données »](#)
- [Guide pratique sur les durées de conservation](#)
- [Référentiel sur les durées de conservation en santé](#) (hors recherche)

7.2. La conservation des données anonymisées

La réglementation relative à la protection des données à caractère personnel ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux **données anonymisées**. Il s'agit des données qui ne peuvent plus, par quiconque, être mises en relation avec la personne physique identifiée à laquelle elles se rapportaient initialement (ex : statistiques).

L'anonymisation doit être distinguée de la pseudonymisation, pour laquelle il est techniquement possible de retrouver l'identité de la personne concernée grâce à des données tierces. En effet, l'opération de pseudonymisation est réversible, contrairement à l'anonymisation.

Ainsi, le responsable du traitement peut conserver sans limitation de durée les données anonymisées. Dans ce cas, le responsable de traitement doit garantir le caractère anonymisé des données de façon pérenne.

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. Aussi, une fois anonymisées, les données ne peuvent plus être reliées à une personne (pour en savoir plus, vous pouvez vous référer aux lignes directrices du Comité européen de la protection des données (CEPD, anciennement G29) sur l'anonymisation).

Pour en savoir plus :

- [Voir les lignes directrices du G29 sur l'anonymisation](#)

8. Information des personnes

8.1 Un traitement de données personnelles doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

8.2 Ainsi, dès **le stade de la collecte des données personnelles**, les personnes doivent être informées des modalités de traitement de leurs données dans les conditions prévues par les articles 12, 13 et 14 du RGPD ainsi que les articles 69 et 70 de la LIL.

Pour en savoir plus, vous pouvez :

- [Voir Guide pratique sur la protection des données](#)
- voir annexe 1 du présent Référentiel

8.3 Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs [droits](#).

8.4 Les personnes dont les données sont enregistrées et conservées dans les traitements de données à caractère personnel du responsable de traitement **sont informées par voie d'affichage dans l'officine de**

pharmacie ou par la remise d'un document spécifique, notamment dans le cadre des visites à domicile (tel qu'un dépliant remis au patient/client ou mis à sa disposition au comptoir).

9. Droits des personnes

9.1 Les personnes concernées disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD (voir la rubrique dédiée aux [droits](#)) :

- droit de **s'opposer au traitement** de leurs données, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD : ainsi par exemple, le droit d'opposition ne trouvera pas à s'appliquer aux registres de dispensation ou à la transmission de leur ordonnance pour la délivrance de médicaments soumis à prescription ;
- droit **d'accès** à toutes les données les concernant de manière générale ;
- droit **de rectification** des données les concernant, si elles sont inexactes ;
- droit **d'effacement** des données qui les concernent sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 17 du RGPD ;
- droit à la **limitation** du traitement. Par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander au professionnel de santé, le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires concernant sa demande.

8.1 Il est à noter que le choix d'une base légale du traitement conditionne l'existence de certains droits (<https://www.cnil.fr/fr/la-licite-du-traitement-essentiel-sur-les-bases-legales-prevues-par-le-rgpd>). Ainsi, la tenue d'un registre de dispensation répond à une obligation légale. Le patient/client ne peut dès lors s'opposer par principe au traitement de ses données personnelles, conformément aux dispositions de l'article 21 du RGPD.

10. Sécurité

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

10.1. Les obligations de sécurité imposées par le RGPD

Afin de satisfaire ses obligations en matière de sécurité, le responsable de traitement pourra utilement se référer au [Guide de la sécurité des données personnelles](#).

En particulier, dans le contexte spécifique du présent référentiel, **le pharmacien est invité à adopter les mesures suivantes, à justifier de leur équivalence ou du fait que leur mise en œuvre n'est pas nécessaire** :

Catégories	Mesures
Sensibiliser les utilisateurs	Informier 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 ³

³ <https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>

Catégories	Mesures
	<p>Pour les utilisateurs accédant aux données de santé, utiliser une authentification forte basée sur :</p> <ul style="list-style-type: none"> - 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 ; - une carte de personnel d'établissement (CPE, à demander à l'Agence du numérique en santé, pour le personnel de l'officine) ; - 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
	<p>Informers les utilisateurs de la mise en place du système de journalisation</p> <p>Prévoir les procédures pour les notifications de violation de données à caractère personnel</p>
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 5 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
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

Catégories	Mesures
Gérer la sous-traitance	Prévoir des clauses spécifiques ⁴ 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.)
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 : <ul style="list-style-type: none"> procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard⁵ 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)

Les prestataires de service chargés de développer, d'assurer la maintenance du logiciel et des postes de travail gérant les « dossiers patients/clients » ou proposant une plateforme de rendez-vous sont invités à mettre en œuvre les mesures suivantes, ou être en mesure de justifier de la mise en place de mesures équivalentes ou de leur absence de nécessité ou de possibilité, sous le contrôle du responsable de traitement :

Catégories	Mesures
Sensibiliser les utilisateurs	Informier et sensibiliser leur personnel ayant accès à des données de santé ou bien participant au développement ou à la maintenance des outils informatiques manipulant des données de santé
Authentifier les utilisateurs	Définir un identifiant (« <i>login</i> ») propre à chaque utilisateur
	Intégrer une politique de mots de passe utilisateur conforme aux recommandations de la CNIL ⁶
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
	Pour les utilisateurs accédant aux données de santé, exiger une authentification forte via leur carte de professionnel de santé (CPS) ou d'établissement (CPE) ou

⁴ 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.

⁵ Les messageries instantanées (« *chat* ») doivent être utilisées avec la plus grande précaution, et de manière sécurisée.

⁶ <https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>

Catégories	Mesures
	tout moyen alternatif à deux facteurs (par ex. envoi d'un code à usage unique)
Gérer les habilitations	Intégrer des profils d'habilitation distinguant notamment les données administratives et les données médicales
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
	Limiter la diffusion des documents papier contenant des données de santé aux personnes ayant besoin d'en disposer dans le cadre de leur activité
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informers 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 la session informatique, avec un déclenchement au bout d'un délai d'inactivité de 5 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
	Mettre en œuvre des antivirus régulièrement mis à jour
	Installer un « pare-feu » (« firewall ») logiciel
	Chiffrer les données stockées
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Pour l'accès à distance aux dossiers patients/clients, respecter les référentiels d'interopérabilité et de sécurité prévus à l'article L. 1110-4-1 du code de la santé publique
	Protéger les écrans des regards indiscrets
	Limiter l'utilisation de supports de stockage amovibles (clés USB, disques dur externe) et chiffrer systématiquement les données sensibles qui y sont conservées
	Prévoir des mesures de sauvegarde et de synchronisation régulière des données
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire (bloquer les protocoles et ports qui ne sont pas utilisés)
	Limiter les connexions d'appareils non professionnels sur le réseau
	Sécuriser les accès distants des appareils informatiques nomades par un 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
	Chiffrer les données stockées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS conformément aux recommandations de l'ANSSI et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant de ressources contenant des données personnelles n'est incorporé aux URL
Sauvegarder et prévoir la continuité d'activité	Prévoir des sauvegardes régulières stockées dans un site distinct
	Prévoir le stockage des supports de sauvegarde dans un endroit sûr et suffisamment distant du système principal
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes le cas échéant
	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
	Enregistrer les interventions de maintenance dans une main courante

Catégories	Mesures
Encadrer la maintenance et la destruction des données	Effacer physiquement les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques ⁷ dans le contrat avec le responsable de traitement
	Prévoir des conditions de restitution et de destruction des données
	Permettre au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
Sécuriser les échanges avec d'autres organismes	Faciliter l'utilisation exclusive d'une messagerie électronique sécurisée de santé pour les échanges entre professionnels de santé
	<p>Pour les échanges avec d'autres professionnels intervenant dans la prise en charge du patient/client ou avec les patients/clients eux-mêmes :</p> <ul style="list-style-type: none"> • intégrer le chiffrement des données avant leur envoi sur une messagerie électronique standard⁸ et prévoir la transmission du code 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 ; • permettre et faciliter l'utilisation d'une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes
Encadrer les développements informatiques	Proposer par défaut des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires libres ou les encadrer strictement
	Tester sur des données fictives ou anonymisées (et non pas seulement pseudonymisées)
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques à l'état de l'art et conformes aux préconisations du référentiel général de sécurité de l'ANSSI
	Conserver les secrets et les clés cryptographiques de manière sécurisée

⁷ 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.

10.2. Les obligations de sécurité imposées par le CSP

Outre les obligations générales issues du RGPD (article 32) et de la loi Informatique et libertés, les traitements des données de santé dans le cadre de la prise en charge sanitaire sont soumises à des obligations de sécurité spécifiques, les articles L. 1470-1 et suivants du code de la santé publique prévoient que le responsable de traitement doit s'assurer que les systèmes d'information, services ou outils numériques qu'il utilise sont conformes aux référentiels de sécurité⁹ et d'interopérabilité¹⁰ élaborés par l'ANS¹¹. Il devra également respecter les consignes de sécurité le concernant prévues par ces derniers qui correspondent à l'état de l'art.

En cas d'externalisation de l'hébergement des données de santé, les prestataires informatiques doivent être agréés ou certifiés pour l'hébergement, le stockage, la conservation de données de santé conformément aux dispositions de l'article L. 1111-8 du code de la santé publique (certification dite « HDS », hébergement de données de santé).

Pour en savoir plus :

- [Liste de l'ANS des hébergeurs certifiés](#)
- [Liste de l'ANS des hébergeurs agréés](#)

• Exemple d'externalisation de l'hébergement des données :

Lorsque le logiciel de gestion de l'officine (LGO) est accessible à distance et est hébergé par un prestataire (en général l'éditeur de logiciel, une plateforme de prise de rendez-vous en ligne) ou si le stockage des données de santé de patients/clients est confié à un prestataire chargé d'en assurer la conservation dans des serveurs à distance (par exemple, un prestataire de sauvegarde), **ce prestataire doit être HDS.**

11. Mesures complémentaires : Analyse d'impact et délégué à la protection des données

11.1 La CNIL estime que la réalisation d'une AIPD et la désignation d'un délégué à la protection des données (DPD/DPO) devraient être nécessaires pour les officines de pharmacie qui recensent dans leur système d'information les données d'au moins 10 000 patients/clients annuellement.

11.2 Pour réaliser une étude d'impact, le responsable de traitement pourra se reporter :

- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web¹².

11.3 Conformément à l'article 28 du RGPD, **le sous-traitant doit fournir au responsable de traitement toute information nécessaire à la réalisation de cette analyse.**

⁹ <https://esante.gouv.fr/securite>

¹⁰ <https://esante.gouv.fr/interopabilite>

¹¹ Voir les référentiels PGSSI-S : <https://esante.gouv.fr/securite/pgssi-s/espace-de-publication>

¹² <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>

Annexe 1 : exemple de notice d'information pour la gestion d'une officine de pharmacie

Pourquoi votre pharmacien/le responsable de traitement tient-il un registre contenant des données vous concernant ?

La tenue du registre est obligatoire. Ce registre a pour finalité de conserver une trace de la délivrance de médicaments.

Quelle est sa durée de conservation ?

Les données vous concernant sont conservées pendant dix ans, en application de l'article R. 5125-45 du code de la santé publique.

[Dans le cas d'un logiciel hébergé par un prestataire]

Le registre est hébergé sur les serveurs de XXX, qui dispose d'un agrément / d'une certification délivrée en application des dispositions de l'article L.1111-8 du code de la santé publique.

Dr. XX, [adresse], présent chez l'hébergeur est garant de la confidentialité des données de santé. Vous pouvez vous opposer à l'externalisation de vos données soit en contactant directement votre pharmacien/le responsable de traitement soit en contactant directement l'hébergeur de données de santé par courrier postal ou à l'adresse électronique xxxx@xxx.com.

Quels sont les destinataires des informations figurant dans le registre ?

Seuls ont accès aux informations figurant dans le registre votre pharmacien/du responsable de traitement et, dans une certaine mesure, au regard de la nature des missions qu'il exerce, son personnel ou les autorités de contrôle.

Enfin, afin de permettre le remboursement et la prise en charge des médicaments, produits et dispositifs délivrés, votre pharmacien/le responsable de traitement est amené à télétransmettre des feuilles de soins à votre caisse de sécurité sociale.

Quels sont vos droits et comment les exercer ?

Vous pouvez accéder aux informations figurant dans le registre.

Vous disposez, par ailleurs, sous certaines conditions, d'un droit de rectification, d'effacement de ces informations, ou du droit de vous opposer ou de limiter leur utilisation.

Pour toute question relative à la protection de vos données ou pour exercer vos droits, vous pouvez vous adresser directement à votre pharmacien/au responsable de traitement. En cas de difficultés, vous pouvez également saisir la Commission nationale de l'informatique et des libertés (CNIL) d'une réclamation.

Cette notice d'information doit naturellement être adaptée à votre situation particulière. Elle ne vise que la gestion du registre. Si d'autres traitements sont mis en place (ex : recherche, télésoin), vous devrez réaliser une information spécifique concernant ces traitements portant notamment sur la finalité de ces traitements, le fondement légal, la durée de conservation des données.