RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE PAR LE LABORATOIRE TITULAIRE DES DROITS D'EXPLOITATION D'UN MÉDICAMENT BÉNÉFICIANT D'UNE AUTORISATION D'ACCÈS COMPASSIONNEL

Projet soumis à consultation publique

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

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

- mis en œuvre par l'entreprise qui assure l'exploitation du médicament disposant d'une autorisation d'accès compassionnel, ci-après le responsable de traitement ;
- et ayant pour finalité, la mise à disposition du médicament sous autorisation d'accès compassionnel et le suivi d'un patient traité par un médicament dans le cadre d'une telle autorisation.

1.2 Sont visés par le présent référentiel :

- les traitements de données à caractère personnel relatifs au suivi d'un patient traité par un médicament disposant d'une autorisation temporaire d'utilisation nominative en cours ;
- les traitements de données à caractère personnel relatifs au suivi d'un patient traité par un médicament disposant d'une autorisation d'accès compassionnel conformément au deuxième alinéa du II de l'article L. 5121-12-1 du code de la santé publique (CSP), **aussi appelée autorisation d'accès compassionnel très précoce**.

1.3 Sont concernés par le présent référentiel les responsables de traitement mettant en œuvre des traitements de données à caractère personnel relatives à des personnes résidant en France (patient, personne affectée, professionnel de santé), quel que soit leur lieu d'établissement. Dans l'hypothèse où le responsable de traitement ne serait pas établi sur le territoire de l'Union européenne, il est tenu de désigner par un mandat écrit un représentant établi en France conformément à l'article 27 du règlement général sur la protection des données (RGPD).

1.4 Le présent référentiel n'est pas applicable :

- aux traitements de données à caractère personnel relatifs au suivi d'un patient traité par un médicament disposant d'une autorisation d'accès compassionnel conformément au premier alinéa du II de l'article L. 5121-12-1 du CSP (accès compassionnel lorsqu'aucune recherche impliquant la personne humaine n'est en cours) ;
- aux traitements de données à caractère personnel mis en œuvre par les professionnels de santé et les systèmes ou services de soins de santé (p. ex. : établissements de santé, agences sanitaires, etc.) par application des dispositions du 1° de l'article 65 de la loi du 6 janvier 1978 modifiée (dossier médical, dossier patient informatisé) ;
- aux traitements de données à caractère personnel mis en œuvre dans le cadre d'une demande d'autorisation d'accès compassionnel réalisée par un professionnel de santé auprès de l'Agence nationale de sécurité des médicaments et des produits de santé (ANSM) *via* le téléservice « e-saturne » ;
- aux traitements de données à caractère personnel mis en œuvre par les laboratoires pharmaceutiques à des fins de traçabilité des médicaments ;
- aux traitements de données à caractère personnel mis en œuvre au titre d'un cadre de prescription compassionnelle prévu à l'article L. 5121-12-1. V du CSP ;
- aux traitements de données à caractère personnel mis en œuvre dans le cadre d'une autorisation précoce prévue à l'article L. 5121-12 du CSP (voir référentiel sur l'accès précoce).

2. Portée du référentiel

2.1 Ce référentiel précise le cadre juridique, issu du RGPD et des dispositions nationales, applicable aux traitements de données à caractère personnel constitués pour la mise à disposition du médicament concerné par une autorisation d'accès compassionnel, et pour le suivi d'un patient traité par un médicament disposant d'une telle autorisation.

2.2 Les responsables de traitement qui réalisent auprès de la Commission une déclaration de conformité au présent référentiel sont autorisés à mettre en œuvre un traitement de données à caractère personnel à des fins de mise à disposition d'un médicament sous autorisation d'accès compassionnel et de suivi des patients s'il est strictement conforme au référentiel.

2.3 Tout traitement de données à caractère personnel à des fins de mise à disposition d'un médicament sous autorisation d'accès précoce et de suivi des patients qui ne respecte pas l'ensemble des exigences définies par le présent référentiel doit faire l'objet d'une demande d'autorisation spécifique, conformément aux dispositions de l'article 66 III de la loi « Informatique et Libertés ».

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

2.5 Les principes dégagés par la CNIL, dans ce référentiel, constituent une aide à la réalisation de l'analyse d'impact relative à la protection des données que les responsables de traitement concernés doivent mener (voir i*nfra*). Les responsables de traitement pourront ainsi définir les mesures leur permettant d'assurer la proportionnalité et la nécessité de leurs traitements, de garantir les droits des personnes et la maîtrise des risques présentés par leurs traitements.

3. Responsables de traitement et sous-traitants

3.1 Dans le cadre du présent référentiel, l'organisme au sein duquel la collecte de données à caractère personnel est assurée agit en qualité de sous-traitant en ce qui concerne la collecte et la transmission de données à caractère personnel au laboratoire titulaire des droits d'exploitation du médicament disposant d'une autorisation d'accès compassionnel. Les professionnels intervenant dans la prise en charge du patient et, le cas échéant, ces lieux restent responsables des traitements qu'ils mettent en œuvre notamment à des fins de tenue et de gestion des dossiers médicaux.

3.2 Sont également qualifiés de sous-traitants, les fournisseurs d'une plateforme électronique de saisie des données à caractère personnel relatives au suivi du patient traité par un médicament disposant d'une autorisation d'accès compassionnel.

3.3 En cas de recours à un sous-traitant, qu'il s'agisse d'un établissement de santé ou d'un fournisseur de plateforme électronique, la prestation doit s'effectuer dans les conditions prévues à l'article 28 du RGPD. Un contrat de sous-traitance doit être conclu entre le prestataire et le responsable de traitement. Ce contrat doit notamment :

- spécifier la répartition des responsabilités relatives aux mesures de sécurité et à la gestion des violations de données entre les différents acteurs ;
- prévoir les conditions de restitution et de destruction des données ;
- prévoir les modalités pour le responsable de traitement pour s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.) ;
- préciser les modalités selon lesquelles le sous-traitant aide, dans la mesure du possible, le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

3.4 Le prestataire doit, en sa qualité de sous-traitant, tenir un registre des activités de traitement effectuées pour le compte d'un responsable de traitement dans les conditions de l'article 30.2 du RGPD.

3.5 Seuls les traitements ayant recours à un sous-traitant relevant exclusivement des juridictions de l'Union européenne ou d'un pays considéré comme adéquat au sens de l'article 45 du RGPD sont conformes au présent référentiel.

3.6 Dans le cas où le responsable de traitement a recours aux services d'un sous-traitant pour l'hébergement, le stockage ou la conservation des données de santé, ce sous-traitant doit être un hébergeur de données de santé agréé ou certifié selon les dispositions du CSP.

4. Objectif(s) poursuivi(s) par le traitement (Finalités)

4.1 Un traitement de données à caractère personnel mis en œuvre dans le cadre d'une autorisation d'accès compassionnel a pour finalité de permettre la mise à disposition du médicament au patient, dès l'obtention de l'autorisation, ainsi que leur suivi.

4.2 Pour ce faire, le traitement de données à caractère personnel vise à permettre :

- la collecte, l'enregistrement, l'analyse, le suivi, la documentation, la transmission et la conservation des données relatives à l'accès, à l'initiation, au suivi et à l'arrêt des prescriptions de médicaments dans le cadre défini par l'article L. 5121-12-1 du CSP ;
- la gestion des contacts avec les médecins prescripteurs et les pharmaciens dispensateurs d'un médicament dans le cadre d'une autorisation d'accès compassionnel.

4.3 Les informations à caractère personnel recueillies pour ces finalités pourront être réutilisées uniquement dans les conditions prévues par le RGPD et la loi du 6 janvier 1978 modifiée, notamment par les dispositions relatives aux traitements de données à caractère personnel mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, et sous réserve de l'accomplissement des formalités requises auprès de la Commission.

5. Base(s) légale(s) du traitement

5.1 Dans le cadre du présent référentiel, les obligations légales imposées au responsable de traitement, notamment aux articles L. 5121-12-1 ainsi qu'aux articles R. 5121-74 et suivants du CSP, sont retenues comme bases légales du traitement de données à caractère personnel conformément aux dispositions de l'article 6.1.c du RGPD.

5.2 La collecte de données sensibles pour les finalités mentionnées au point 3 est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ; elle a notamment pour objectif de garantir le respect de normes élevées de qualité et de sécurité des soins de santé et des médicaments conformément aux dispositions de l'article 9.2.i du RGPD et de l'article 66 de la loi du 6 janvier 1978 modifiée.

6. Données à caractère personnel concernées

6.1 Seules peuvent faire l'objet d'un traitement les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement, à savoir la mise à disposition du médicament disposant d'une autorisation d'accès compassionnel, ainsi que le suivi du patient visé par cette autorisation, dans les conditions et selon les spécificités prévues aux articles L. 5121-12-1 ainsi qu'aux articles R. 5121-74 et suivants du CSP.

6.2 À ce titre, en fonction de l'objectif poursuivi par le traitement de données à caractère personnel, du médicament concerné et des situations, conformément au protocole d'utilisation thérapeutique de suivi des patients (PUT-SP) défini par l'ANSM, le responsable de traitement peut collecter et traiter :

a) les données relatives au patient:

- données d'identification du patient : numéro, code alphanumérique ou code alphabétique, informations signalétiques (sexe, poids, taille, âge ou année et mois de naissance ou date de naissance complète si nécessaire dans un contexte pédiatrique), à l'exclusion du numéro d'inscription au répertoire national d'identification des personnes physiques et de l'identifiant national de santé ;
- données relatives à la santé du patient notamment l'histoire de la maladie, les antécédents personnels ou familiaux, les pathologies ou événements associés ;
- données relatives aux conditions d'utilisation du médicament impliquant notamment les traitements concomitants, les informations relatives au mode de prescription, de dispensation ;
- données portant sur l'efficacité du médicament ;
- données portant sur la sécurité du médicament : nature et fréquence des effets indésirables ;

En complément de ces données, le responsable de traitement peut également collecter et traiter les données suivantes sous réserve qu'elles soient strictement nécessaires au regard du produit prescrit et de la pathologie en cause :

- l'origine ethnique ;
- les données génétiques, à l'exclusion du génome complet ;
- la vie sexuelle ;
- la consommation de tabac, d'alcool et de drogues ;

b) le cas échéant, les données collectées concernant les personnes en lien avec le patient, uniquement si la prise du médicament les a affectées (partenaire, descendance), notamment les données d'identification dont le lien avec le patient, les données d'efficacité et les données portant sur des effets indésirables telles que décrites au point 5.a) ;

c) les données relatives aux professionnels de santé (médecins prescripteurs et pharmaciens dispensateurs) : nom, prénom, spécialité, numéro d'inscription au répertoire partagé des professionnels de santé (RPPS), coordonnées professionnelles.

6.3 Les supports permettant la collecte des données susmentionnées devront limiter le recours à des zones de saisie libre sous forme de « bloc-notes ».

7. Destinataires des informations

7.1 Peuvent être destinataires des données, sous la responsabilité du responsable de traitement, notamment :

- les sous-traitants intervenant pour le compte du responsable de traitement, dans la limite de leurs fonctions, leurs attributions respectives et dans les conditions définies par le contrat de sous-traitance ;
- le personnel habilité des autres sociétés du groupe auquel appartient le responsable de traitement qui participent à la mise en œuvre de l'autorisation d'accès compassionnel, notamment par la mise à disposition du médicament, dans la limite de leurs attributions respectives ;
- les organismes publics nationaux ou étrangers en charge de la surveillance des médicaments bénéficiant d'une autorisation d'accès compassionnel, dans le cadre de l'exercice de leurs missions telles que définies par les textes, notamment l'ANSM, les centres régionaux de pharmacovigilance et les centres antipoison, ou les organismes en charge de la surveillance des médicaments bénéficiant d'une autorisation d'accès précoce, notamment la Haute Autorité de santé (HAS).

8. Durées de conservation

8.1 Les données traitées sont conservées en base active dans la limite de deux ans suivant l'approbation par l'ANSM, du résumé du dernier rapport de synthèse prévu à l'article R. 5121-74-6 ou, en l'absence de protocole d'utilisation thérapeutique et de suivi des patients (PUT-SP), suivant l'expiration de la décision de l'ANSM octroyant l'autorisation d'accès compassionnel.

8.2 Les données sont ensuite archivées en base intermédiaire pendant la durée de l'autorisation d'accès compassionnel très précoce et ne peuvent pas être conservées, en fonction du médicament concerné, de l'indication thérapeutique visée et des dispositions législatives et règlementaires en vigueur, au-delà d'une période de soixante-dix ans à compter de la date d'expiration de l'autorisation d'accès précoce.

8.3 Si aucune autorisation d'accès précoce n'est accordée à la spécialité pharmaceutique concernée ou si l'autorisation d'accès compassionnel est suspendue ou retirée, les données ne pourront pas être archivées en base intermédiaire au-delà d'une période de soixante-dix ans à compter de :

- l'expiration de la décision de l'ANSM octroyant l'autorisation d'accès compassionnel ;
- la date de la décision de l'ANSM prononçant la suspension ou le retrait de l'autorisation d'accès compassionnel.

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

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

9. Information des personnes

9.1 Un traitement de données à caractère personnel doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées et/ou leurs représentants légaux (patient faisant l'objet d'un traitement par un médicament sous autorisation d'accès compassionnel, professionnels de santé intervenant dans la prise en charge des patients, personnes, en lien avec le patient, affectées par la prise du médicament). Le responsable de traitement prend les mesures appropriées pour fournir aux personnes concernées et/ou leurs représentants légaux une information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

9.2 S'agissant des patients et/ou de leurs représentants légaux, les modalités d'information sont les suivantes :

- conformément à l'article L. 5121-12-1.VI du CSP, le médecin prescripteur doit informer le patient et/ou ses représentants légaux que la prescription du médicament ne s'effectue pas dans le cadre d'un AMM mais dans le cadre d'une autorisation d'accès compassionnel, des risques encourus, des contraintes et des bénéfices susceptibles d'être apportés par le médicament ;
- dès l'initiation du traitement, le médecin prescripteur remet au patient et/ou à ses représentants légaux une note d'information, établie dans les conditions prévues par les articles 13 et, le cas échéant, 14 du RGPD, ainsi que par les articles 69 et 70 de la loi « Informatique et Libertés » ;
- il est rappelé que le patient et/ou ses représentants légaux sont libres d'accepter ou de refuser le traitement par un médicament prescrit sous autorisation d'accès compassionnel. En cas d'acceptation des soins, les articles L. 5121-12 -1 et suivants et R. 5121-74 et suivants du CSP imposent le recueil de données à caractère personnel relatives au suivi du patient ;
- le patient peut être assisté par la personne confiance qu'il a désignée en application de l'article L. 1111-6 du CSP.

9.3 S'agissant des personnes en lien avec le patient et qui sont affectées par la prise du médicament, les modalités d'information sont les suivantes :

- si le professionnel a collecté ces données directement auprès de la personne, il lui remet, dans le respect du secret médical, une note d'information établie dans les conditions prévues par l'article 13 du RGPD ainsi que par les articles 69 et 70 de la loi « Informatique et Libertés » ;
- si le professionnel a collecté indirectement ces données, il remet au patient une note d'information destinée à la personne affectée par la prise du médicament, établie dans les conditions prévues par l'article 14 du RGPD ainsi que par les articles 69 et 70 de la loi « Informatique et Libertés ». À cette occasion, le professionnel informe le patient et/ou ses représentants légaux des conséquences que cette information aura vis-vis du secret des informations le concernant.

9.4 En outre, le responsable de traitement est tenu de mettre à disposition sur son site web les notices d'information relatives au traitement mis en œuvre.

9.5 S'agissant des professionnels de santé intervenant pour la prise en charge du patient, le responsable de traitement informe, dans un délai raisonnable, ces derniers du traitement de leurs données à caractère personnel dans le courrier qui leur est adressé au moment de l'initiation de l'autorisation d'accès compassionnel. Cette information reprend les mentions prévues aux articles 13, le cas échéant, 14 du RGPD.

9.6 Si une plateforme électronique est utilisée pour recueillir les données à caractère personnel mentionnées au point 5, les professionnels de santé doivent être informés lors de leur connexion à cette plateforme.

9.7 Dans le cas où des données à caractère personnel collectées conformément au présent référentiel font l'objet d'une réutilisation à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, une nouvelle information individuelle des personnes concernées est requise, sauf si :

- la personne concernée dispose déjà des informations prévues aux articles 13 ou 14 du RGPD concernant ce traitement ultérieur ;
- l'information délivrée lors de la collecte des données dans le cadre d'une autorisation d'accès compassionnel prévoit la possibilité de réutiliser les données, et renvoie à un dispositif spécifique d'information auquel les personnes concernées pourront se reporter préalablement à la mise en œuvre de chaque nouveau traitement de données.

10. Droits des personnes

10.1 Les personnes concernées par le traitement et/ou leurs représentants légaux (patients et professionnels de santé) disposent des droits suivants :

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

10.2 Conformément à l'article L. 1111-6 du CSP, le patient peut être accompagné dans ses démarches par la personne de confiance qu'il a désigné.

10.3 Dans la mesure où le traitement de données à caractère personnel est fondé sur le respect d'une obligation légale et poursuit un objectif d'intérêt public dans le domaine de la santé publique, les personnes concernées ne disposent ni du droit d'opposition, ni du droit à l'effacement, ni du droit à la portabilité des données. Les personnes concernées en sont informées préalablement.

10.4 S'agissant des personnes en lien avec le patient et qui sont affectée par la prise du médicament, ces droits s'exercent dans des conditions compatibles avec les dispositions relatives au secret médical et professionnel. Plus précisément, l'exercice des droits de ces personnes ne doit pas conduire le laboratoire à communiquer des informations couvertes par le secret médical. Si l'identification de la personne en lien avec le patient et qui est affectée par la prise du médicament nécessite que le responsable de traitement relève des informations confidentielles concernant le patient, le responsable de traitement devra en informer la personne en lien avec le patient et pourra ne pas donner suite à sa demande d'exercice des droits.

10.5 S'agissant du patient, ses droits s'exercent à tout moment auprès du professionnel de santé intervenant dans sa prise en charge ou par l'intermédiaire du médecin de son choix. Il peut également exercer ses droits directement auprès du responsable de traitement. Dans cette hypothèse, le patient est informé des conséquences sur la confidentialité de ses données.

10.6 S'agissant des professionnels de santé intervenant dans la prise en charge du patient, leurs droits s'exercent directement auprès du responsable de traitement.

11. Transfert des données en dehors de l'Union européenne

11.1 Les données indirectement identifiantes des patients et les données directement identifiantes des professionnels de santé peuvent faire l'objet d'un transfert hors de l'Union européenne si les conditions suivantes sont réunies :

- les dispositions du point 7. relatives aux destinataires des données sont respectées ;
- le transfert est strictement nécessaire à la mise à disposition du médicament sous autorisation d'accès compassionnel et le suivi des patients traités par un médicament faisant l'objet d'une telle autorisation.

11.2 En outre, le transfert peut être effectué dans le cadre de la déclaration de conformité au présent référentiel lorsque l'une des conditions suivantes, prévues au chapitre V du RGPD, est remplie :

- le transfert s'effectue à destination d'un pays ou d'une organisation internationale reconnu par la Commission européenne comme assurant un niveau de protection adéquat, conformément à l'article 45 du RGPD (décision d'adéquation) ;
- le transfert s'effectue moyennant des garanties appropriées, listées à l'article 46.2, du RGPD (notamment : clauses contractuelles types approuvées par la Commission européenne, règles d'entreprise contraignantes, code de conduite, mécanisme de certification), et, le cas échéant, de mesures supplémentaires si la législation du pays dans lequel les données sont exportées fait obstacle au respect des garanties contractuelles ;

- en l'absence d'une décision d'adéquation ou de garanties appropriées, le transfert peut être fondé sur l'une des exceptions prévues à l'article 49 du RGPD sous réserve que les conditions particulières, d'interprétation stricte, énoncées dans cet article s'appliquent[1].

11.3 Le responsable de traitement doit avoir préalablement informé les personnes concernées du transfert de leurs données à caractère personnel vers des pays tiers à l'Union européenne, de l'existence ou de l'absence d'une décision d'adéquation ou de garantie appropriée, et enfin des moyens d'en obtenir une copie conformément aux articles 13.1.f), et 14.1.f) du RGPD.

11.4 Est considéré comme un transfert tout accès distant aux données depuis l'extérieur du territoire de l'Union européenne.

12. Sécurité

12.1 De manière générale, le responsable de traitement ainsi que son ou ses sous-traitant, y compris le lieu au sein duquel la collecte de données est assurée, doivent prendre toutes les précautions utiles au regard des risques présentés par le 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 ne soient déformées, endommagées, perdues ou que des tiers non autorisés y aient accès.

12.2 Le responsable du traitement définit, met en œuvre et contrôle l'application d'une politique de sécurité qui doit notamment décrire les mesures répondant à l'exigence de sécurité du traitement prévu par l'article 32 du RGPD.

12.3 En particulier, dans le contexte du présent référentiel, le responsable de traitement et ses sous-traitants, doivent adopter les mesures techniques et organisationnelles suivantes :

Numéros d'exigence	Exigences de sécurité
Sensibiliser les utilisateurs	
SEC-SEN-1	**Informer et sensibiliser les personnes manipulant les données** Chaque personne habilitée à accéder aux données concernées par le présent référentiel doit être formée au respect du secret médical et régulièrement sensibilisée aux risques et obligations inhérents au traitement de données à caractère personnel, et en particulier aux données de santé et aux catégories particulières de données à caractère personnel (comme les données génétiques ou celles révélant l'origine ethnique du patient).
SEC-SEN-2	**Rédiger une charte informatique et lui donner une force contraignante** Chaque personne habilitée à accéder aux données traitées dans le cadre d'un traitement encadré par le présent référentiel doit s'engager à respecter une charte de confidentialité précisant notamment les sanctions en cas de non-respect.
Authentifier les utilisateurs	
SEC-AUT-1	**Définir un identifiant (*login*) unique à chaque utilisateur** Chaque personne habilitée à accéder aux données traitées dans le cadre d'un traitement encadré par le présent référentiel doit disposer d'un identifiant unique et individuel. Les comptes partagés entre plusieurs utilisateurs sont à proscrire.

[1] Voir les lignes directrices 2/2018 du CEPD sur les dérogations à l'article 49 en vertu du règlement 2016/679, adoptées le 25 mai 2018 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf.

SEC-AUT-2	**Mettre en place une authentification forte et multi-facteurs** Le responsable de traitement prévoit la mise en place d'une authentification multi-facteurs forte faisant intervenir *a minima* deux facteurs d'authentification distincts pour l'ensemble des utilisateurs et administrateurs, par exemple en utilisant un identifiant couplé à un mot de passe et à un mot de passe à usage unique généré *via* un protocole cryptographique. Pour l'authentification des professionnels de santé, le responsable de traitement peut imposer une authentification forte par l'utilisation d'une carte de professionnel de santé (CPS) ou un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS pour toute transmission ou tout accès aux données de santé. Lorsque les seules opérations effectuées consistent en des opérations de saisie de données, excluant de fait les opérations de consultation de données, ces modalités d'authentification ne sont pas exigées
SEC-AUT-3	**Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL** Si l'un des facteurs d'authentification est un mot de passe, celui-ci doit être conforme à la délibération n° 2017-012 du 19 janvier 2017 de la CNIL portant adoption d'une recommandation relative aux mots de passe et modifiée par la délibération n° 2017-190 du 22 juin 2017, ou toute autre mise à jour ultérieure de cette recommandation.
SEC-AUT-4	**Obliger l'utilisateur à changer son mot de passe après réinitialisation** L'utilisateur doit changer tout mot de passe attribué par un administrateur ou automatiquement par le système lors de la création du compte ou d'une réinitialisation.
SEC-AUT-5	**Limiter le nombre de tentatives d'accès à un compte** Le responsable de traitement doit prévoir une limite du nombre de tentatives d'accès à toute plateforme électronique utilisée pour recueillir les données traitées dans le cadre d'un traitement encadré par le présent référentiel et mettre en place un blocage temporaire de l'accès lorsque la limite est atteinte.
Gérer les habilitations	
SEC-HAB-1	**Définir des profils d'habilitation** Différents profils d'habilitation doivent être prévus afin de gérer les accès aux données en tant que besoin et de façon exclusive, d'une durée déterminée et limitée. Une granularité des accès aux données doit être prévue pour chaque type de profil, par exemple un accès uniquement à des données agrégées, un accès à des données pseudonymisées ou un accès à des données directement identifiantes. Les accès privilégiés disposant de droits étendus, notamment pour l'administration et la maintenance doivent être réservés à une équipe restreinte et être limités au strict nécessaire. En particulier, seul le personnel habilité du responsable de traitement peut, sous la responsabilité de ce dernier, accéder aux données à caractère personnel traitées, dans la limite de leurs attributions respectives et pour ce qui les concerne, notamment : • le pharmacien responsable ou son représentant ainsi que toute personne dûment habilitée et placée sous sa responsabilité ; • le responsable de la pharmacovigilance ainsi que les collaborateurs placés sous sa responsabilité ; • les membres des services en charge des affaires médicales, de la recherche et du développement, des affaires réglementaires, de l'accès au marché ; • les membres du service en charge de la gestion des commandes, de l'approvisionnement et de la distribution des médicaments ; • les membres du service des audits peuvent, de façon ponctuelle et motivée, avoir accès à ces données pour vérifier le respect des exigences réglementaires et des

	procédures internes.
SEC-HAB-2	**Supprimer les permissions d'accès obsolètes** Les permissions d'accès doivent être retirées dès le retrait des habilitations, par exemple après le départ d'un collaborateur.
SEC-HAB-3	**Réaliser une revue annuelle des habilitations** Une revue des habilitations doit être réalisée régulièrement et *a minima* annuellement.
Sécuriser les échanges avec d'autres organismes	
SEC-ÉCH-1	**Sécuriser le recueil d'informations via une plateforme électronique** Si le recueil de données à caractère personnel se fait au format électronique à l'aide d'une plateforme dédiée, le responsable de traitement prévoit que les données soient envoyées de façon chiffrée : • soit en chiffrant directement les données ; • soit en utilisant un canal de communication chiffré (via des protocoles du type HTTPS, SFTP). Dans tous les cas, les algorithmes de chiffrement employés devront satisfaire les exigences SEC-CRY-1. La confidentialité des secrets (clé de chiffrement, mot de passe, etc.) devra être assurée en les transmettant via un canal de communication distinct (par exemple, dépôt du fichier chiffré sur la plateforme et communication du mot de passe par téléphone ou SMS).
SEC-ÉCH-2	**Sécuriser les envois par courriel** S'agissant des transmissions de données par courriel, celles-ci devront être sécurisées par exemple en chiffrant les données à caractère personnel par un algorithme de chiffrement asymétrique avec une clé privée détenue uniquement par le destinataire des données. La confidentialité des secrets (clé de chiffrement, mot de passe, etc.) devra être assurée en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par courriel et communication du mot de passe par téléphone ou SMS). Lors de la transmission par courriel, l'expéditeur devra s'assurer qu'il s'agit du bon destinataire, afin d'éviter que des données à caractère personnel ne soient accidentellement divulguées à un tiers non autorisé.
SEC-ÉCH-3	**Sécuriser les envois par fax** Si le format papier est utilisé et que les transmissions sont effectuées par fax, les mesures de sécurité suivantes doivent être mises en œuvre : • Le fax doit être situé dans un local physiquement contrôlé et accessible uniquement au personnel habilité ; • L'impression des messages doit être subordonnée à l'introduction d'un code d'accès personnel ; • Lors de l'émission des messages, le fax doit afficher l'identité du fax destinataire afin d'être assuré de l'identité du destinataire ; • Le carnet d'adresses des fax doit pré-enregistrer, dans la mesure du possible, les destinataires potentiels afin d'éviter toute erreur de destinataire.
SEC-ÉCH-4	**Envoyer de manière sécurisée les rapports de synthèse aux autorités** Le responsable de traitement doit prendre les mesures de sécurité adéquates, y compris celles listées dans les exigences SEC-ÉCH-1, SEC-ÉCH-2 et SEC-ÉCH-3, afin de transmettre aux autorités compétentes les rapports de synthèse. L'usage d'une plateforme électronique d'échange de documents sécurisée est à privilégier.

Utiliser des fonctions cryptographiques	
SEC-CRY-1	**Utiliser des algorithmes, des logiciels et des bibliothèques reconnues** Les données à caractère personnel doivent être chiffrées au repos par des algorithmes et tailles de clé conformes à l'annexe B1 du référentiel général de sécurité (« RGS »). Une procédure opérationnelle de gestion des clés doit être formalisée. Les sauvegardes de ces données doivent également faire l'objet d'un chiffrement conforme à l'annexe B1 du RGS. Toutes les transmissions de données sont réalisées via des canaux de communication chiffrés et assurant l'authentification de la source et du destinataire (type HTTPS, avec une version de TLS la plus à jour possible).
SEC-CRY-2	**Conserver les secrets et les clés cryptographiques de manière sécurisée** Ces secrets doivent être protégés, *a minima* par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr.
Tracer les accès	
SEC-JOU-1	**Prévoir un système de journalisation (*logs*)** Les actions des utilisateurs doivent faire l'objet de mesures de journalisation notamment, a minima, les accès des utilisateurs, l'horodatage de leurs accès ainsi que les détails des actions effectuées (comme des opérations de lecture ou d'écriture) ainsi que la référence de l'enregistrement concerné. Les traces de journalisation doivent être conservées pendant une durée comprise entre six mois et un an.
SEC-JOU-2	**Informer les utilisateurs de la mise en place du système de journalisation** Les utilisateurs participant aux traitements encadrés par le présent référentiel doivent être informés de la mise en place du dispositif de journalisation, de la nature des données collectées et de la durée de conservation de ces traces.
SEC-JOU-3	**Protéger les équipements de journalisation et les informations journalisées** L'architecture de journalisation doit être centralisée et les journaux doivent faire l'objet de mesures de protection particulières. L'accès aux journaux est restreint aux seules personnes ayant obtenu une autorisation spécifique basée sur la stricte nécessité.
SEC-JOU-4	**Contrôler les traces** Un contrôle automatique ou semi-automatique des traces doit être réalisé régulièrement et *a minima* tous les deux mois, afin de détecter d'éventuelles anomalies.
Gérer les incidents et les violations de données	
SEC-VIO-1	**Prévoir les procédures pour les incidents de sécurité** Une politique de gestion des incidents de sécurité est mise en œuvre afin de répondre immédiatement à tout éventuel incident de sécurité et d'identifier si l'incident entraîne une violation des données à caractère personnel traitées par le responsable de traitement. La politique prévoit notamment une procédure visant à mettre en œuvre des actions de remédiation afin de réduire la gravité du préjudice pour une personne concernée par la violation de données et de corriger les vulnérabilités engendrées par les incidents de sécurité.
SEC-VIO-2	**Prévoir les procédures pour les notifications de violation de données à caractère personnel**

	Le responsable de traitement prévoit une procédure pour déterminer la gravité d'une violation de données (c'est-à-dire toute atteinte, même temporaire, à la confidentialité, à la disponibilité ou à l'intégrité des données) pour les personnes concernées. Le cas échéant, s'il existe un risque pour les personnes concernées, le responsable de traitement devra procéder à la notification de la violation auprès de l'autorité en charge de la protection des données à caractère personnel compétente sur le territoire dans lequel le responsable de traitement a son établissement principal et, dans l'hypothèse où le responsable de traitement n'est pas établi sur le territoire de l'Union européenne, à la CNIL dans les conditions prévues à l'article 33 du RGPD. Si ce risque est estimé élevé, le responsable de traitement devra communiquer la violation aux personnes concernées dans les conditions prévues à l'article 34 du RGPD. Le responsable de traitement doit documenter en interne toute violation de données quel que soit son niveau de gravité.
Sauvegarder et prévoir la continuité d'activité	
SEC-SAU-1	**Effectuer des sauvegardes fréquentes des données** Que les données soient sous forme papier ou électronique, des sauvegardes complètes doivent être prévues à intervalles réguliers. Le processus de restauration des données à partir des sauvegardes doit également faire l'objet de tests réguliers.
SEC-SAU-2	**Stocker les supports de sauvegarde dans un endroit sûr** Les supports de sauvegardes (disque dure externe, clé USB, etc.) doivent être conservées dans un lieu sûr et différent de ces données. Les supports à privilégier sont ceux ayant une longévité suffisante.
SEC-SAU-3	**Prévoir des moyens de sécurité pour le convoyage des sauvegardes** Lorsque les sauvegardes sont transmises par le réseau, il convient de chiffrer le canal de transmission des sauvegardes lorsqu'elles sont transmises *via* un réseau public.
SEC-SAU-4	**Prévoir et tester régulièrement la continuité d'activité** Le responsable de traitement prévoit un plan de reprise et de continuité d'activité informatique, même sommaire. Il doit s'assurer que les utilisateurs et les sous-traitants savent qui contacter en cas d'incident. Ce plan de continuité ou de reprise d'activité ainsi que la restauration des sauvegardes doivent être régulièrement testées.
Archiver de manière sécurisée	
SEC-ARC-1	**Mettre en œuvre des modalités d'accès spécifiques aux données archivées** Le responsable de traitement définit un processus d'archivage et de gestion des archives, qui inclut les modalités d'accès spécifiques aux données archivées, du fait que l'utilisation des données archivées doit intervenir de manière ponctuelle et exceptionnelle.
SEC-ARC-2	**Détruire les archives obsolètes de manière sécurisée** Le responsable de traitement met en œuvre un mode opératoire garantissant que l'intégralité d'une archive a été détruite.

12.4 De façon plus générale, le responsable de traitement ou son sous-traitant, si le responsable de traitement a recours à des prestataires informatiques dans le cadre des traitements visés par le référentiel, doivent mettre en œuvre et documenter les mesures suivantes :

Catégories	Mesures
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser un antivirus régulièrement mis à jour
	Installer un « pare-feu » (« *firewall* ») logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention de maintenance à distance sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des supports de stockage des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Définir et implémenter une politique de mise à jour des outils logiciels et installer sans délai les mises à jour critiques
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est transmis *via* des URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les traceurs (cookies) non nécessaires au service
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions de maintenances réalisées par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Réaliser les tests et recettes sur des données fictives ou anonymisées

12.5 Ces mesures ne sont pas exhaustives et devront être complétées par les éventuelles mesures qui auront été jugées nécessaires lors de la réalisation de l'analyse d'impact sur la protection des données menée, tel que détaillé au point 13 du présent référentiel.

12.6 Le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles[2] publié par la CNIL.

12.7 Les articles 5-1-f et 32 du RGPD nécessitent la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques, afin que celles-ci soient conformes à l'état de l'art.

13. Analyse d'impact relative à la protection des données

13.1 Le responsable de traitement doit réaliser et documenter une analyse d'impact relative à la protection des données (AIPD).

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

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

13.3 Le cas échéant, le responsable de traitement pourra élaborer une procédure relative à l'AIPD permettant d'impliquer les acteurs et les personnes pertinentes pour sa réalisation, notamment le délégué à la protection des données (DPD/DPO), qui devra être consulté.

13.4 L'AIPD devra être réexaminée et mise à jour régulièrement, notamment si des changements importants sont prévus dans le traitement ou si les risques pour les personnes concernées ont évolué (comme la poursuite d'une finalité supplémentaire, le recours à un nouveau sous-traitant, de nouvelles données collectées, une fuite de données permettant la réidentification, etc.).

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

[2] https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf