Commission nationale de l'informatique et des libertés

Délibération n° 2020-081 du 18 juin 2020 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux

NOR : *CNIL2019851X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le code de la santé publique ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Valérie PEUGEOT, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Adopte le référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux, qui sera publié au *Journal officiel* de la République française.

La présidente,
M.-L. Denis

RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL
DESTINÉS À LA GESTION DES CABINETS MÉDICAUX ET PARAMÉDICAUX

Table des matières

1. **A qui s'adresse ce référentiel ?**

Ce référentiel, pris en application des dispositions de l'article 8-I-2-*b* de la loi du 6 janvier 1978 modifiée, encadre la mise en œuvre des traitements de données à caractère personnel par les professions médicales et paramédicales dans le cadre de la gestion médicale et administrative de leur patientèle.

Il s'adresse aux professionnels de santé exerçant à titre libéral.

Il ne s'applique pas aux traitements mis en œuvre par les services de soins (établissements de santé, centres de santé, communautés professionnelles territoriales de santé, etc.), ni à ceux mis en œuvre par les services de médecine d'entités publiques ou privées (médecine du travail, médecine scolaire, PMI, etc.), par les pharmaciens, par les laboratoires d'analyses de biologie médicale ou par les opticiens.

2. **Portée du référentiel**

Les traitements visant à permettre la gestion médicale et administrative au sein des cabinets médicaux et paramédicaux, 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 loi du 6 janvier 1978 modifiée (LIL) ainsi qu'aux dispositions du code de la santé publique.

Les professionnels de santé concernés, en tant que responsables de traitement, doivent 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. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant.

Les traitements mis en œuvre par les professionnels de santé doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir modèle de registre dans le guide pratique à destination des médecins).

Ce référentiel n'a pas de valeur contraignante. Il permet en principe d'assurer la conformité des traitements de données mis en œuvre par les professionnels de santé exerçant à titre libéral aux principes relatifs à la protection des données et au secret médical, dans un contexte d'évolution des pratiques à l'ère numérique.

Les professionnels de santé qui s'écarteraient 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

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 par ailleurs trouver à s'appliquer.

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 nécessaire.

La CNIL publie régulièrement des guides pratiques afin d'accompagner les professionnels dans la mise en œuvre des obligations prévues par la nouvelle réglementation sur la protection des données personnelles que ces derniers sont invités à consulter en complément du présent référentiel (1).

3. **Objectif(s) poursuivi(s) par le traitement (finalités)**

Le traitement mis en œuvre doit répondre à un objectif précis et être justifié au regard des missions et des activités du professionnel de santé.

Il est mis en œuvre afin de permettre l'exercice des activités de prévention, de diagnostic et de soins ainsi que de gestion administrative.

Il permet notamment, pour les besoins de la prise en charge des patients :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux ;
- la gestion et la tenue des dossiers nécessaires au suivi du patient ;
- le recours aux pratiques de soins à distance requérant des technologies de l'information et de la communication, telles que la télémédecine et le télésoin ;
- les communications entre professionnels identifiés et structures de soins participant à la prise en charge de la personne concernée et à la coordination de celle-ci ;
- l'établissement et la télétransmission des documents destinés à la prise en charge des frais de santé par l'assurance maladie (feuilles de soins, arrêt de travail, protocole de soins électroniques, etc.) ;
- la tenue de la comptabilité.

Les données personnelles de santé ne peuvent être utilisées que dans l'intérêt direct du patient ou de la gestion du cabinet médical, dans les conditions déterminées par la loi, pour les besoins de la santé publique et des obligations des professionnels de santé.

Elles peuvent être réutilisées pour des études lorsqu'elles sont réalisées par les personnels assurant le suivi du patient et destinées à leur usage exclusif. A défaut, elles devront faire l'objet de formalités en application des articles 72 et suivants de la loi Informatique et Libertés relatifs aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

4. **Base(s) légale(s) du traitement**

Chaque finalité du traitement doit reposer sur l'une des bases légales fixées par la réglementation (cf. La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD).

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 un impact sur l'exercice de certains droits, ces bases légales font partie des informations devant être portées à la connaissance des personnes concernées.

Afin d'aider les professionnels de santé dans cette analyse, le présent référentiel propose, à titre indicatif, un choix de base légale pour chaque finalité dans le tableau ci-dessous (2).

Finalités	Bases légales envisageables (3)
La tenue du dossier médical	Obligation légale
L'établissement et la télétransmission des documents à destination de l'assurance maladie	Obligation légale

Finalités	Bases légales envisageables (3)
La tenue du dossier de prise en charge sanitaire (comme par exemple le dossier de soins infirmiers)	Obligation légale
La prise de rendez-vous	Intérêt légitime
La tenue de la comptabilité	Intérêt légitime
La télémédecine (art. L. 6316-1 du CSP), le télésoin (art. L. 6316-2 du CSP)	Intérêt légitime

5. **Données personnelles concernées**

Principe de pertinence, de loyauté et de minimisation des données

Dans un souci de minimisation des données personnelles traitées, le professionnel de santé doit veiller à ne collecter et utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de traitement de gestion médicale et administrative de sa patientèle. Sont en principe considérées comme pertinentes, pour des finalités rappelées ci-dessus, les données suivantes :

a) L'identité et coordonnées du patient (telles que les nom, prénom, date de naissance, adresse postale, adresse électronique et numéro de téléphone) ;

b) L'identifiant national de santé (INS) pour la prise en charge sanitaire ou médico-sociale d'un patient ;

c) Le numéro de sécurité sociale à des fins de facturation et de prise en charge financière des dépenses de santé ;

d) La situation familiale (telle que la situation matrimoniale, le nombre d'enfants) ;

e) La situation professionnelle (telle que la profession, les conditions de travail) ;

f) La santé (telles que le poids, la taille, les antécédents médicaux, les diagnostics médicaux, la thérapie suivie, les traitements prescrits, la nature des actes effectués, les résultats d'examens, des renseignements d'ordre biologique, physiologique et pathologique propres à influencer la réaction du patient à sa prise en charge médicale et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le professionnel de santé) ;

g) Les informations relatives aux habitudes de vie en fonction du contexte, dès lors qu'elles sont collectées avec l'accord du patient et qu'elles sont nécessaires au diagnostic et aux soins du patient (telles que relatives à la dépendance [seul, en institution, autonome, grabataire], à l'assistance [aide-ménagère, familiale], à l'exercice physique [intensité, fréquence, durée], au régime et comportement alimentaire, aux loisirs) ;

h) Les traces fonctionnelles (celles qui rendent compte des actions métiers 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).

Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il utilise, le professionnel de santé doit par ailleurs vérifier, tout au long de la durée de vie du traitement, la qualité des données qu'il traite. Cela signifie en pratique que conformément à la règlementation, les données doivent être mises à jour.

6. **Destinataires et accès aux informations**

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

- 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, y compris via l'accès au dossier médical partagé et à l'espace numérique de santé ;
- les personnes en charge du secrétariat, qui doivent n'avoir accès, dans le respect des dispositions sur le secret professionnel, qu'aux informations nécessaires à l'accomplissement de leurs missions, c'est-à-dire aux informations relatives à la gestion du cabinet et en particulier à la gestion des rendez-vous ainsi qu'à certaines informations à caractère médical dans des conditions strictement limitées à ce qui est nécessaire à l'exercice de leurs missions et sous le contrôle du professionnel de santé ;
- afin de permettre le remboursement des actes, des prestations et leur contrôle, les personnels des organismes d'assurance maladie, qui ont connaissance, dans le cadre de leurs fonctions et pour la durée nécessaire à l'accomplissement de celles-ci, de l'identité de l'assuré, de son numéro de sécurité sociale et de numéro de code des actes et prestations exécutées et des pathologies diagnostiquées dans les conditions définies à l'article L. 161-29 du code de la sécurité sociale ;
- les personnels des organismes d'assurance maladie complémentaire, autorisés de par leur fonction à traiter des données de santé, notamment de l'identité de leurs assurés, de leur numéro de sécurité sociale et sous la forme de codes regroupés, des catégories des actes et prestations effectués ;
- les organismes de recherche dans le domaine de la santé et les organismes spécialisés dans l'évaluation des pratiques de soins, qui peuvent être destinataires de données personnelles de santé dans les conditions définies par le RGPD et la loi du 6 janvier 1978 modifiée (notamment dans le respect du principe de la minimisation des données).

En cas de recours à un prestataire de service pour assurer la maintenance du logiciel et des postes de travail gérant les « dossiers patients », celui-ci accède aux données personnelles dans le respect du secret médical. Les données devront être protégées par des moyens physiques et logiques, tels que le chiffrement, afin de permettre au technicien d'assurer ses missions sans pouvoir lire ces données.

Lorsque le logiciel de gestion des « dossiers patients » 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 une plateforme de télémédecine) ou si le stockage des données de santé de patients est confié à un prestataire chargé d'en assurer la conservation dans des serveurs à distance (par exemple, un prestataire de sauvegarde ou de permanence téléphonique), ce prestataire doit être hébergeur agréé ou certifié 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.

En cas de recours à une plateforme de prise de rendez-vous en ligne, il conviendra de procéder à une répartition claire des responsabilités en fonction des services proposés.

En toute hypothèse, dès qu'un prestataire de services est sollicité pour traiter des données personnelles pour le compte du professionnel de santé (société de maintenance, plateforme en ligne, hébergeur de données de santé agréé ou certifié), cette 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. Il 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 ;
- 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 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 (faille 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 (4).

7. **Durées de conservation**

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

Au regard des finalités de gestion du cabinet médical ou paramédical, les données enregistrées dans l'application peuvent être conservées pendant une durée de vingt ans à compter de la date de la dernière prise en charge du patient : en base active, pendant une durée de cinq ans à compter de la dernière intervention sur le dossier du patient, puis, à l'issue de cette période, sous la forme archivée sur un support distinct pendant quinze ans, dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application.

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.

A 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. A défaut, le professionnel de santé y procèdera manuellement.

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 ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles ont été dûment anonymisées (voir les lignes directrices du CEPD sur l'anonymisation) ; une pseudonymisation n'est pas une anonymisation : effacer les noms et prénoms des personnes concernées ne suffit pas à anonymiser les données.

8. **Information des personnes**

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

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 (voir guide pratique à destination des médecins).

Les personnes concernées doivent par ailleurs être informées de la manière dont elles peuvent exercer leurs droits.

Les personnes dont les données sont enregistrées et conservées dans les traitements de données à caractère personnel du professionnel de santé sont informées par voie d'affichage dans les locaux du cabinet médical ou paramédical ou par la remise d'un document spécifique, notamment dans le cadre des visites à domicile (tel qu'un dépliant remis au patient ou mis à sa disposition dans la salle d'attente ou un courriel confirmant un rendez-vous).

9. **Droits des personnes**

Les personnes concernées disposent des droits suivants, qu'ils 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 au dossier médical ;
- droit d'accès à leur dossier patient, et 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.

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-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd). Ainsi, la tenue d'un dossier médical répond à une obligation légale. Le patient 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 professionnel de santé 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. Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles.

Conformément à l'article L. 1110-4-1 du code de la santé publique, le professionnel de santé devra s'assurer que les systèmes d'information, services ou outils numériques qu'il utilise sont conformes aux référentiels de sécurité (5) et d'interopérabilité (6) approuvés par arrêté du ministre chargé de la santé. Il devra également respecter les consignes de sécurité le concernant prévues par ces derniers.

En particulier, dans le contexte spécifique du présent référentiel, l'organisme 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	Informer et sensibiliser le personnel du cabinet accédant aux données
	Pour un cabinet 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 (7)
	Pour les utilisateurs accédant aux données de santé, utiliser une authentification forte via leur carte de professionnel de santé (CPS) ou tout moyen alternatif à deux facteurs
	Maintenir la CPS au niveau strictement personnel, sans communication du code secret au personnel du cabinet (p. ex. : secrétaire médical) (8)
Gérer les habilitations	Attribuer un profil d'habilitation adapté à chaque utilisateur (distinguant notamment les données administratives et les données médicales)
	Supprimer les permissions d'accès obsolètes
	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

Catégories	Mesures
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de la session informatique
	Permettre la mise à jour régulière des antivirus
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
	Limiter le stockage d'informations d'ordre médical sur une tablette ou un ordiphone (en raison des conséquences pour les patients 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)
	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 un ordiphone ou une tablette à usage professionnel
Protéger le réseau informatique interne	Limiter 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 du cabinet les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques 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 aves les patients	S'assurer qu'il s'agit bien du bon destinataire
	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 ou avec les patients eux-mêmes : – procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard (9) 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)

En cas d'externalisation de l'hébergement des données, 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.

Les prestataires de service chargés de développer, d'assurer la maintenance du logiciel et des postes de travail gérant les « dossiers patients » ou proposant une plateforme de rendez-vous sont invités à adopter les mesures suivantes, sous le contrôle du responsable de traitement :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel du cabinet accédant aux données
	Pour un cabinet mutualisant des ressources informatiques, contribuer à la rédaction d'une charte informatique
Authentifier les utilisateurs	Définir un identifiant (« *login* ») propre à chaque utilisateur
	Intégrer une politique de mots de passe utilisateur conforme aux recommandations de la CNIL (10)
	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 tout moyen alternatif à deux facteurs
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
	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 la session informatique
	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, 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

Catégories	Mesures
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 et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant n'est incorporé aux URL
Sauvegarder et prévoir la continuité d'activité	Prévoir des sauvegardes régulières
	Prévoir le stockage des supports de sauvegarde dans un endroit sûr
	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
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Effacer physiquement les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques 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	Prévoir 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 ou avec les patients eux-mêmes : – prévoir le chiffrement des données avant leur envoi sur une messagerie électronique standard (11) et 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 ; – choisir 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 reconnus
	Conserver les secrets et les clés cryptographiques de manière sécurisée

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

La CNIL estime que la réalisation d'une AIPD et la désignation d'un délégué à la protection des données (DPO) devraient être nécessaires pour les professionnels de santé qui, exerçant en cabinet groupé, partagent un système d'information commun, à partir d'un seuil annuel de 10 000 patients.

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 web.

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.

(1) Par exemple, le guide rédigé conjointement par le CNOM et la CNIL à destination des médecins.
(2) D'autres bases légales, telles que le contrat ou l'intérêt public, pourraient également être retenues.
(3) Sous réserve de choix différents justifiés par un contexte spécifique.
(4) https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser.
(5) https://esante.gouv.fr/securite.
(6) https://esante.gouv.fr/interoperabilite.
(7) https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires.
(8) Il est possible de mettre en place une authentification forte pour le personnel du cabinet, par exemple au moyen d'un mot de passe à usage unique (identifiant, mot de passe et envoi d'un code à chaque connexion) ou au moyen d'une carte de personnel d'établissement (CPE, à demander à l'Agence du numérique en santé).
(9) Les messageries instantanées (« *chat* ») doivent être utilisées avec la plus grande précaution, et de manière sécurisée.
(10) https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires.
(11) Les messageries instantanées ou « *chat* » doivent être utilisées avec la plus grande précaution, et de manière sécurisée.