ORDRE NATIONAL DES MEDECINS
Conseil National de l'Ordre

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

GUIDE PRATIQUE SUR LA PROTECTION DES DONNÉES PERSONNELLES

ÉDITION JUIN 2018

TABLE DES MATIÈRES

Pourquoi un guide pratique sur la protection des données personnelles ?

Le Règlement Général sur la Protection des Données (RGPD)[1] est entré en application le 25 mai 2018. La loi française Informatique et Libertés[2] a été adaptée en conséquence par la loi sur la protection des données personnelles en cours de promulgation. Ces deux textes constituent désormais le socle de la nouvelle réglementation sur la protection des données personnelles.

Le présent guide pratique a pour ambition d'orienter les médecins, en exercice libéral, dans la mise en œuvre des obligations prévues par la nouvelle réglementation sur la protection des données personnelles. En complément de ce guide, la CNIL vient de mettre en ligne une fiche thématique : « RGPD et professionnels de santé libéraux : ce que vous devez savoir » (https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir). Elle propose d'autres fiches thématiques dédiées aux problématiques de santé (télémédecine, application mobile, etc.) que vous pouvez consulter sur : https://www.cnil.fr/fr/sante.

Si vous exercez au sein d'un établissement de santé, d'un EHPAD, ou encore d'un centre de santé, vous pouvez vous rapprocher de la direction, ou de toute personne susceptible de gérer la question des données personnelles. Si votre structure a désigné un délégué à la protection des données (DPO), ce dernier est l'interlocuteur privilégié pour vous renseigner sur l'état de conformité de votre structure au RGPD ou répondre à toutes vos questions.

Pourquoi êtes-vous concerné par le RGPD ?

En tant que médecin en exercice libéral, vous êtes amené à recevoir ou à émettre des informations sur vos patients pour assurer leur suivi que ce soit dans le dossier « patient » (papier ou informatique), dans le cadre de l'utilisation d'une plateforme en ligne de gestion des rendez-vous ou encore de la réalisation d'actes de télémédecine. De manière plus globale, vous collectez également des informations pour gérer votre cabinet (ex : gestion des fournisseurs, des personnels que vous employez, etc.). Ces informations que vous recevez et / ou émettez, à l'occasion de votre activité professionnelle, sont considérées comme des données personnelles.

Le RGPD définit les données personnelles comme *« toute information se rapportant à une personne physique identifiée ou identifiable »* c'est-à-dire une personne physique qui peut être identifiée, directement ou indirectement[3].

[1] 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 (règlement général sur la protection des données).
[2] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[3] Art. 4 1) du RGPD.

En pratique, il peut s'agir de données d'identification comme les nom, prénom, adresse, ou numéro de téléphone, d'informations sur la vie personnelle du patient (ex : nombre d'enfants), sa couverture sociale (ex : assurance maladie obligatoire, assurance maladie complémentaire, etc.) et surtout d'informations relatives à sa santé (pathologie, diagnostic, prescriptions, soins, etc.), les éventuels professionnels qui interviennent dans sa prise en charge. Vous détenez également, dans le cadre de votre exercice, le numéro de sécurité sociale des patients (Numéro d'Inscription au Répertoire des Personnes Physiques - NIR) pour facturer les actes réalisés.

Pour toutes ces situations où vous utilisez ces données personnelles, vous êtes concerné par le RGPD.

Fiche 1.

Quel cadre appliquer aux dossiers des patients ?

Check-list des bonnes pratiques à respecter :

→ Je limite les informations collectées au nécessaire et j'utilise les dossiers patients conformément aux finalités définies (suivi des patients) ;

→ Je tiens un registre à jour de mes « traitements » (voir annexe n° 2 « Registre des activités de traitement) ;

→ Je supprime les dossiers patients et de manière générale toute information ayant dépassé la durée de conservation préconisée ;

→ Je mets en place les mesures appropriées de sécurité de mes dossiers « patients » ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir l'annexe n° 1 « Exemple de notice d'information »).

Vous utilisez, dans votre exercice professionnel, un logiciel fourni par un prestataire informatique pour tenir vos dossiers « patients », ou vous tenez vos dossiers « patients » sous format papier. Ces dossiers contiennent nécessairement des données personnelles sur vos patients et les autres professionnels de santé intervenant dans leur suivi.

Vous êtes donc considéré comme « responsable de traitement » au sens de la réglementation sur la protection des données personnelles. Vous devez vous assurer de la conformité des dossiers avec cette réglementation.

Quelles sont vos obligations ?

Vous devez vous assurer que l'usage des dossiers « patients » respecte les principes fondamentaux de la protection des données personnelles[4].

[4] Art. 5 RGPD et art. 6 loi Informatique et Libertés.

1. Vos dossiers papiers ou votre logiciel médico-administratif doit répondre à des finalités déterminées, explicites et légitimes.

Ainsi, les informations que vous collectez dans les dossiers « patients » sont utilisées pour exercer votre activité de prévention, de diagnostic et de soins et servent à gérer votre cabinet. Elles répondent aux besoins de la prise en charge de vos patients. Il s'agit notamment de permettre :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux ;
- l'édition des ordonnances ;
- l'envoi de courriers aux confrères ;
- l'établissement et la télétransmission des feuilles de soins.

Toute autre utilisation des informations que vous collectez à l'occasion de la prise en charge doit être réalisée avec précaution. En particulier, toute utilisation personnelle ou commerciale des dossiers de vos patients est naturellement prohibée.

2. Les données que vous collectez et que vous reportez, dans les dossiers de vos patients, doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.

Toutes les informations que votre patient a pu vous révéler, dans le cadre de vos échanges, ne doivent pas nécessairement intégrer son dossier. Seules celles qui sont utiles au suivi de votre patient peuvent être enregistrées et conservées.

Dans ce cadre, la CNIL estime légitime de collecter certaines catégories de données personnelles, notamment :

- les données d'identification : nom, prénom, date de naissance, adresse, numéro de téléphone ;
- le numéro de sécurité sociale : uniquement pour l'édition des feuilles de soins et la télétransmission aux caisses d'assurance maladie ;
- selon les contextes, la situation familiale : situation matrimoniale, nombre d'enfants ;
- selon les contextes, la vie professionnelle : profession, conditions de travail ;
- la santé : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le médecin;
- informations relatives aux habitudes de vie : si collectées avec l'accord du patient et dans la stricte mesure où elles sont nécessaires au diagnostic et aux soins.

Si d'autres informations vous paraissent pertinentes et nécessaires pour votre exercice professionnel, vous pouvez les collecter (ex : origine ethnique ayant une influence particulière sur une pathologie déterminée ou un traitement médical, habitudes alimentaires).

En revanche, toute information qui serait sans lien avec l'objet de la consultation du patient ou qui ne serait pas indispensable au diagnostic ou à la délivrance des soins doit être exclue. Par exemple, vous ne devez pas inscrire des informations sur la vie privée du patient qui ne sont pas médicalement nécessaires (ex : religion du patient, orientation sexuelle, etc.).

3. Les données que vous collectez sur vos patients doivent être conservées pour une durée qui n'excède pas la durée nécessaire à l'utilisation que vous en faites.

Il est important de prendre en compte les délais de prescription des éventuelles actions en responsabilité et / ou toutes dispositions particulières.

En l'absence de dispositions spécifiques portant sur la durée de conservation des dossiers des professionnels exerçant en libéral, le Conseil national de l'Ordre des médecins préconise de s'aligner sur les délais de conservation prévus pour les dossiers médicaux des établissements de santé [5]:

- 20 ans à compter de la date de la dernière consultation du patient ;
- si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date ;
- dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès ;
- en cas d'action tendant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais de conservation.

Les doubles des feuilles de soins doivent être conservés 3 mois.

4. Vous devez informer les patients de l'existence de vos dossiers et de leurs droits à cet égard[6].

Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un document spécifique (ex : dépliant remis au patient ou mis à disposition dans la salle d'attente). Un exemple de notice d'information figure en annexe n° 1 du présent guide pratique.

L'information doit comporter impérativement les éléments suivants :

- votre nom et vos coordonnées ;
- les finalités et la base juridique du traitement, y compris les finalités ultérieures ;
- les destinataires des données ;
- la durée de conservation ;

[5] Article R. 1112-7 du code de la santé publique
[6] Art. 13 RGPD

- les droits de la personne : accès, rectification, à certaines conditions effacement, limitation, opposition, introduction d'une réclamation auprès de la CNIL ;
- caractère obligatoire des données fournies et des conséquences éventuelles d'un défaut de réponse ;
- le cas échéant, utilisation ultérieure des données pour une finalité autre que celle pour laquelle les données ont été collectées (ex : si un médecin souhaite utiliser ultérieurement les données à des fins de recherche)7.

Vos patients disposent de droits. Ils peuvent[8] :

- accéder aux données les concernant ;
- rectifier ces données en cas d'erreur ;
- s'opposer au traitement pour des raisons tenant à leur situation particulière ;
- effacer les données, dans certaines situations particulières (dossier patient conservé trop longtemps, données non adéquates, par exemple).

Chaque demande portant sur ces droits doit être examinée dans un délai raisonnable. Dans le cas d'une demande d'accès au dossier « patient », le délai est obligatoirement de 8 jours, porté à 2 mois lorsque les informations datent de plus de 5 ans[9].

Pour tout savoir sur l'exercice des droits des patients, vous pouvez consulter la fiche thématique « Les droits pour maîtriser vos données personnels » (https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles).

5. Vous devez prendre toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données de santé.

En effet, seules certaines personnes sont autorisées, au regard de leurs missions et en vertu de dispositions législatives les y habilitant, à accéder aux données de santé des patients (ex : équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, etc.).

En pratique, il sera important de veiller au respect des règles relatives à l'échange et au partage de données entre professionnels (sur ce point, voir la fiche pratique du CNOM « Echange et partage d'informations », déc. 2016) https://www.conseil-national.medecin.fr/sites/default/files/cnomechangepartageinfos_0.pdf. Ainsi, tout professionnel de santé intervenant dans la prise en charge du patient peut avoir un accès spécifique aux seules informations nécessaires à cette prise en charge, ou si cela n'est pas possible, le médecin peut envoyer les informations nécessaires directement à ces professionnels. Quant au personnel administratif, il ne peut avoir un accès global aux dossiers des patients. Certaines données (nom, prénom, code acte, NIR, date de la consultation) sont adressées aux organismes d'assurance maladie via la télétransmission ou les feuilles de soins.

---

[7] Si une recherche était finalement menée, une information individuelle devra être réalisée. Elle sera préalable à la mise en œuvre de la recherche et spécifique à chaque recherche.
[8] Art. 15 à 23 RGPD et art. 38 à 43 ter loi Informatique et libertés.
[9] Art. L.1111-7 du Code de la santé publique.

En cas de recours à un prestataire de service pour assurer la maintenance du logiciel gérant les dossiers de vos patients, celui-ci n'est pas censé accéder aux données de santé à caractère personnel. Il a un rôle purement technique. En principe, les données doivent être chiffrées afin de permettre au technicien d'assurer ses missions sans pouvoir lire ces données.

Si vous confiez le stockage des dossiers « patients » à un prestataire chargé d'en assurer la conservation, dans des serveurs à distance, celui-ci 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 toute hypothèse, dès que vous sollicitez les services d'un prestataire (société de maintenance, hébergeur de données de santé agréé ou certifié), celui-ci agit pour votre compte. Vous devez donc formaliser la relation que vous entretenez avec lui en passant un contrat de sous-traitance. Ce contrat mentionne que le prestataire en tant que sous-traitant[10] :

- ne traite les données à caractère personnel que sur votre instruction ;
- 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 votre autorisation écrite préalable ;
- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement notamment lorsque des patients ont des demandes concernant leurs données ;
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- collabore dans le cadre d'audits.

6. Vous devez prendre toutes les mesures nécessaires pour sécuriser et protéger les données personnelles que vous traitez[11].

Vous devez respecter les mesures prévues par les référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du code de la santé publique).

Pour une information détaillée, vous pouvez consulter le guide de la sécurité des données personnelles publié par la CNIL[12] et le mémento relatif à la sécurité informatique pour les professionnels de santé en exercice libéral publié par l'Agence des systèmes d'information partagés de santé (ASIP Santé)[13].

[10] Art. 28 RGPD.
[11] Art. 32 RGPD et art. 34 loi Informatique et libertés.
[12] https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf).
[13] http://esante.gouv.fr/sites/default/files/Memento_Securite.pdf

En ce qui concerne la sécurisation du système informatique, vous devez respecter les grands principes suivants :

- utilisation d'un mot de passe conforme aux recommandations de la CNIL, 12 caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux), renouvelé régulièrement ;
- verrouillage de votre session informatique automatiquement après maximum 30 minutes d'inactivité ;
- antivirus à jour, pare-feu, application systématique des correctifs de sécurité du système informatique et des logiciels ;
- sauvegardes régulières des données (sauvegarde au minimum hebdomadaire, avec conservation des sauvegardes mensuelles sur 12 mois glissants) et leur conservation dans un lieu différent que votre cabinet ;
- chiffrement des données avec un logiciel adapté ;
- absence ou minimisation des connexions d'appareils non professionnels sur le réseau ;
- authentification via votre Carte de professionnel de santé (CPS) ou tout moyen alternatif d'authentification forte.

La CPS doit rester strictement personnelle. En aucun cas, vous ne pouvez communiquer vos codes secrets à votre personnel (ex : secrétaire médicale). Vous pouvez mettre en place une authentification forte pour votre personnel au moyen d'un mot de passe à usage unique par exemple (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 votre Caisse primaire d'assurance maladie[14].

Si votre logiciel gérant vos dossiers « patients » est accessible à distance et est hébergé par un prestataire (votre éditeur de logiciel en général), vous devez vous assurer que ce tiers ou son sous-traitant est agréé ou certifié pour l'hébergement des données de santé conformément à l'article L. 1111-8 du code de la santé publique.

Si vous conservez vos dossiers sous format papier, vous devez également vous assurer de leur sécurité (locaux sécurisés, armoire contenant les dossiers fermée à clé).

En cas de violation de données (destruction, perte, altération, divulgation non autorisée de données à caractère personnel, accès non autorisée à de telles données), vous devez avoir les réflexes suivants :

- analyser, dans la mesure du possible, l'étendue du problème afin d'identifier les démarches à accomplir et éviter que cet incident se reproduise : qui a eu accès aux données ? quelle est l'origine du problème ? les données ont-elles été envoyées à un tiers ? des données de santé sont-elles concernées ? quelles mesures auraient pu empêcher l'événement ou quelles mesures peuvent en atténuer les conséquences ?

[14] http://esante.gouv.fr/services/espace-cps/cartes-professionnelles-de-sante

- s'il existe un risque pour les droits et libertés des personnes, notifier à la CNIL la violation de données[15]. Cette notification détaillée contient les éléments suivants : nature de la violation, catégories et nombre approximatif de personnes concernées et d'enregistrements de données, nom et coordonnées du contact de votre cabinet, conséquences probables de la violation de données, mesures prises ou à prendre pour remédier à la violation, y compris, le cas échéant, mesures pour en atténuer les éventuelles conséquences négatives. Pour procéder à une notification de violation de données, vous devez remplir le formulaire que vous trouvez sous le lien suivant : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.
- si la violation de données engendre un risque élevé pour les droits et libertés des personnes concernées, sur demande de la CNIL ou à votre initiative, communiquer dans les meilleurs délais à la personne concernée cette violation, excepté si les données avaient été chiffrées rendant impossible leur lecture, ou si des mesures ultérieures prises garantissent que le risque élevé n'est plus susceptible de se matérialiser[16]. Cette communication doit intervenir individuellement ou, si cela exige des efforts disproportionnés, par une communication publique. Elle contient a minima les éléments suivants : nom et coordonnées du contact de votre cabinet, conséquences probables, mesures prises ou à prendre pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
- inscrire cette violation de données à caractère personnel. Cette inscription peut se faire dans un registre spécifique, un tableau récapitulatif des incidents ou même au sein du registre des activités de traitement (sur le registre des activités de traitement, voir précisions apportées ci-dessous).
- contacter, le plus rapidement possible, votre assurance de responsabilité professionnelle pour l'informer de l'incident.

Attention, si l'incident a eu lieu au sein d'établissements de santé, d'hôpitaux des armées, de laboratoires de biologie médicale ou de centres de radiothérapie, votre structure doit également notifier l'incident à l'Agence régionale de santé compétente.

Devez-vous accomplir une formalité particulière auprès de la CNIL ?

Depuis le 25 mai 2018, vous ne devez plus réaliser, auprès de la CNIL, d'engagement de conformité à la norme simplifié 50 (NS-050), comme le prévoyait auparavant la loi pour la gestion des cabinets médicaux.

En revanche, vous devez tenir un registre des activités de traitement recensant tous les traitements que vous mettez en œuvre dans le cadre de votre activité, notamment : celui que vous utilisez pour le suivi des patients (les dossiers « patients ») mais aussi ceux résultant de l'utilisation de la messagerie électronique sécurisée[17] ou d'un dispositif de télémédecine, etc.

[15] Art. 33 RGPD.
[16] Art. 34 RGPD.
[17] La CNIL travaille actuellement à la mise à jour du référentiel consacré à la messagerie électronique sécurisée.

Le registre des activités de traitement doit inclure vos nom et coordonnées ainsi que les caractéristiques essentielles du traitement (finalité du traitement, personnes concernées, destinataires, transferts de données, etc.).
Vous trouverez un modèle pré-rempli (voir l'annexe n° 2 « Registre des activités de traitement »). Ce modèle est à adapter à votre situation particulière.

Devez-vous désigner un délégué à la protection des données (DPO) ?

Dès lors que vous exercez à titre individuel, vous n'êtes pas soumis à l'obligation de désigner un DPO. Néanmoins, si en raison de votre activité, vous estimez que vous traitez des données de santé à grande échelle (ex : exercice au sein d'un réseau de professionnels, maisons de santé, centre de santé, dossiers partagés entre plusieurs professionnels de santé, etc.), vous devez soit désigner un DPO en interne, soit solliciter les services d'un DPO externe (consultants, cabinets d'avocats, etc.).

Pour en savoir plus, vous pouvez consulter la fiche thématique « Devenir délégué à la protection des données ».

Pouvez-vous être sanctionné ?

Si vous ne respectez pas vos obligations, vous pouvez faire l'objet d'une sanction administrative de la CNIL, voire d'une sanction pénale[18].

Il est donc impératif de vous mettre en conformité avec la réglementation et de documenter cette conformité (registre des activités de traitement, traçabilité des violations de données, engagements de confidentialité du personnel, etc.). Si la CNIL constate un défaut de conformité et vous met en demeure de vous conformer, vous avez encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction.

La CNIL a indiqué que les contrôles de conformité qu'elle pourrait réaliser seront, dans les premiers mois d'application du RGPD, à visée pédagogique. L'essentiel est de pouvoir démontrer que vous êtes engagé dans une démarche de mise en conformité.

[18] La CNIL peut prononcer, en fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.

Fiche 2.

Quel cadre appliquer à la prise de rendez-vous ?

Check-list des bonnes pratiques à respecter :

→ Je limite les informations collectées par le prestataire et vérifie la conformité du prestataire avec la réglementation et notamment la présence des mentions obligatoires dans le contrat de sous-traitance que je passe avec lui ;

→ Je tiens un registre à jour de mes « traitements » (voir annexe n° 2 « Registre des activités de traitement ») ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir l'annexe n° 1 « Exemple de notice d'information »).

Dans le cadre de votre exercice professionnel, vous avez souhaité faire appel à une plateforme de prise de rendez-vous en ligne ou à un prestataire de permanence téléphonique. Ce tiers est amené à collecter des informations sur les patients prenant rendez-vous, notamment les éventuels motifs de consultation.

Quelles sont vos obligations ?

A l'occasion des prises de rendez-vous, sont collectées, enregistrées et utilisées des données personnelles concernant vos patients, en particulier leur identité et leurs coordonnées personnelles. Les motifs de consultation peuvent parfois être demandés avec un degré de précision qui varie selon les spécialités et les nécessités de préparation à un examen particulier. Ces informations peuvent renseigner sur l'état de santé des patients, de même que la simple connaissance d'une consultation d'un spécialiste peut donner une indication sur l'état de santé (ex. consulter un cardiologue régulièrement).

Que la prise de rendez-vous soit assurée par votre cabinet ou par un prestataire tiers de permanence téléphonique, ou par une plateforme en ligne, vous restez « responsable de traitement » des données d'identification des patients et des données de santé collectées lors de la prise de rendez-vous.

En tant que responsable de traitement, vos obligations sont identiques à celles applicables pour les dossiers « patients » : enregistrement des données strictement nécessaires, utilisation légitime des informations obtenues dans le cadre de la prise de rendez-vous, inscription dans le registre des activités de traitement, limitation des accès, sécurisation du planning et de son contenu, notification à la CNIL en cas de violation des données, etc.

Attention !

- Si la consultation ne nécessite pas de préparation au préalable ou la réservation d'outils spécifiques, les motifs de la consultation n'ont pas à être renseignés.

- Contrairement aux dossiers « patients » qui ont une durée de conservation assez longue, les données relatives à la prise de rendez-vous peuvent être supprimées lorsqu'elles ne sont plus nécessaires. Cette durée doit être pensée en fonction de votre activité, sachant que les dates des examens et consultations médicaux sont, de toute manière, inscrites dans les dossiers de vos patients.

- Le prestataire est également responsable de traitement des données relatives aux comptes créés par les patients et les professionnels de santé.

Les droits des patients sont identiques à ceux précédemment évoqués pour les dossiers « patients ». Ils s'exercent auprès de vous de la même manière. Une information spécifique doit leur être délivrée.

Quelles sont les obligations du prestataire tiers gérant la prise de rendez-vous ?

Le prestataire tiers, que ce soit une plateforme de prise de rendez-vous en ligne ou un prestataire de permanence téléphonique, agit pour votre compte. Il est considéré comme sous-traitant en vertu de la réglementation. Il doit être guidé par la volonté de protéger au mieux les informations concernant vos patients et de respecter la réglementation applicable. Il ne peut ainsi utiliser les informations concernant vos patients que pour le strict accomplissement de ses missions.

Le prestataire doit notamment mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité et la confidentialité des données confiées. Cela passe par la mise en place d'accès sécurisés, d'une politique d'habilitation (accès accordés aux personnes autorisées uniquement), d'un chiffrement des données (rendant impossible la lecture par un tiers ne possédant pas la clé de déchiffrement), d'une protection contre les attaques informatiques (antivirus, etc.).

La relation avec votre prestataire doit être formalisée par un contrat de sous-traitance. Vous devez relire attentivement, avant toute signature, ce contrat afin de vérifier que le prestataire [19] :

- ne traite les données à caractère personnel que sur votre instruction ;
- 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 votre autorisation écrite préalable ;
- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement, notamment lorsque des patients ont des demandes concernant leurs données ;
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- collabore dans le cadre d'audits.

Le prestataire tiers, en cas d'incident lié aux données qu'il gère pour votre compte (faille de sécurité, piratage, perte, etc.), doit vous en informer dans les meilleurs délais[20], afin que vous remplissiez vos propres obligations à cet égard (voir la fiche n° 1 « Quel cadre appliquer aux dossiers des patients »).

Si votre prestataire héberge informatiquement les informations issues de la prise de rendez-vous par vos patients, et notamment des données de santé, il doit faire appel à un hébergeur de données de santé agréé ou certifié[21].

Le prestataire tiers doit tenir un registre des activités de traitement mentionnant les utilisations, les enregistrements ou toutes les opérations qu'il réalise sur des données personnelles pour votre compte.

Pouvez-vous être sanctionné ?

Les mêmes sanctions sont applicables en cas de non-respect de la réglementation dans le cadre de la prise de rendez-vous en ligne ainsi qu'en matière de gestion des dossiers « patients » (voir la fiche n° 1 « Quel cadre appliquer aux dossiers des patients »).

[19] Art. 28 RGPD.
[20] Art. 33 RGPD.
[21] Art. L1111-8 du Code de la santé publique.

Fiche 3.

Quel cadre appliquer à l'utilisation de la messagerie électronique ?

Check-list des bonnes pratiques à respecter :

→ J'utilise un service de messagerie sécurisée de santé pour mes échanges avec d'autres professionnels de santé ;

→ Si j'utilise une messagerie électronique standard ou des messageries instantanées, je m'assure que ces messageries sont bien sécurisées et adaptées à mon utilisation professionnelle ;

→ Je chiffre les pièces jointes lorsque j'utilise des messageries standard sur internet qui ne garantissent pas la confidentialité des messages.

Dans le cadre de votre exercice professionnel, vous êtes amené à échanger des informations avec d'autres professionnels de santé ou avec vos patients. Vous utilisez peut-être une messagerie sécurisée de santé ou bien un service de messagerie standard.

En tant que responsable de traitement et personne soumise au secret professionnel, vous devez assurer la protection des données que vous échangez. Cette protection nécessite le respect de règles particulières.

Qu'est-ce que le système de messagerie sécurisée de santé ?

Le système de messagerie sécurisée de santé est un espace dématérialisé qui permet l'échange de données de santé en toute confiance entre professionnels de santé et, plus largement, entre professionnels des secteurs sanitaire, social et médico-social. Il intègre également un annuaire commun et certifié de l'ensemble des professionnels habilités ou des structures au sein desquelles ils exercent.

De nombreux acteurs de la santé ont intégré ce système fondé, avant l'entrée en application du RGPD, sur la réalisation d'un engagement de conformité à l'autorisation unique 037 (AU portant sur la mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données de santé à travers un système de messagerie sécurisée).

Depuis l'entrée en application du RGPD, l'utilisation de la messagerie sécurisée est possible sans avoir à accomplir une formalité auprès de la CNIL. Pour autant, le traitement découlant de l'utilisation de la messagerie sécurisée devra être inscrit sur votre registre des activités de traitement (sur ce point, voir l'annexe n° 2 « Registre des activités de traitement »). A terme, il devra être conforme à un référentiel élaboré par la CNIL (référentiel en cours de rédaction).

Pouvez-vous utiliser des services de messagerie électronique standard ?

Votre obligation de sécuriser vos échanges, en particulier en ce qui concerne les données de santé, impose de passer par une messagerie électronique sécurisée[22]. Néanmoins, l'utilisation d'une telle messagerie n'est possible qu'entre professionnels de santé.

Pour les échanges avec d'autres professionnels, non professionnels de santé, intervenant dans la prise en charge du patient (ex : ostéopathes, psychologues, etc.) ou avec les patients, l'envoi de données de santé via une messagerie électronique standard implique de :

- chiffrer les pièces sensibles à transmettre. À ce sujet, il convient de se référer aux préconisations de la CNIL figurant sur la fiche « Sécurité : utiliser des fonctions cryptographiques » ;
- utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP ou HTTPS, en utilisant les versions les plus récentes des protocoles ;
- garantir le secret nécessaire à la lecture du fichier (ex : mot de passe) en utilisant un canal de nature différente (ex : téléphone, SMS, etc.).

Aussi, l'utilisation de toute messagerie ne chiffrant pas les données et hébergeant les données dans un pays ou auprès d'un prestataire qui ne garantit pas la protection des données conformément aux règles européennes est à proscrire.

De même, les messageries instantanées ou « chat » doivent être utilisées avec la plus grande précaution. L'utilisation d'une telle messagerie doit être sécurisée.

Attention !

Les messageries standard sur internet ne garantissent pas toutes la confidentialité des messages. Si ce n'est pas le cas, le chiffrement des pièces jointes s'impose alors.

[22] Art. L.1110-4-1 et L.1111-8 du Code de la santé publique.

Fiche 4.

Quel cadre appliquer aux téléphones portables et tablettes ?

Check-list des bonnes pratiques à respecter :

→ Je sécurise l'accès à mon téléphone ou à ma tablette et à son contenu (mot de passe, chiffrement, etc.)

→ Je ne stocke pas d'informations médicales relatives à mes patients sur mon téléphone portable ou ma tablette ;

→ Je m'assure que l'accès à mon logiciel de dossiers « patients » sur mon téléphone portable ou ma tablette est sécurisé ;

→ Je consulte mon logiciel de dossiers « patients » avec précaution.

Dans le cadre de votre exercice professionnel, vous êtes amené à utiliser votre téléphone portable ou votre tablette pour consulter des informations relatives à votre patient ou communiquer avec d'autres professionnels de santé ou avec les patients.

Pouvez-vous utiliser votre téléphone portable ou votre tablette pour accéder à vos dossiers patients ?

Votre tablette ou votre téléphone portable peut être utilisé, dans un contexte professionnel, à conditions que les règles de sécurité soient respectées.

Il est fortement déconseillé de conserver des informations d'ordre médical dans la mémoire interne de votre tablette ou de votre téléphone portable (cela permet d'éviter de graves conséquences pour les patients dans l'hypothèse d'un vol ou d'une perte du matériel). Néanmoins, en pratique, si vous êtes amené à passer outre ce conseil, la conservation des données doit s'effectuer *a minima* dans le respect des règles de sécurité suivantes : utilisation de mots de passe conformes aux recommandations de la CNIL (12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux), verrouillage automatique après un court délai, chiffrement des données sensibles. D'une manière plus générale, vous devez éviter de prêter votre téléphone ou votre tablette et de les laisser sans surveillance.

Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, l'accès à distance aux dossiers de vos patients doit se faire conformément aux référentiels d'interopérabilité et de sécurité élaborés par l'ASIP santé. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la CNIL. Dans l'attente de la publication des textes réglementaires permettant l'entrée en vigueur de ces dispositions, la CNIL demande que l'authentification des professionnels de santé intervienne au moyen d'une carte de professionnel de santé (CPS) ou d'un dispositif équivalent agréé par l'ASIP santé.

Dans le cadre de vos déplacements, vous devez toujours vérifier, lorsque vous consultez des informations relatives à des patients sur votre tablette ou votre téléphone portable, que votre écran est à l'abri des regards indiscrets.

Attention !

L'utilisation de supports mobiles (clés USB, disque dur externe) est fortement déconseillée. Si malgré tout, vous en utilisez, il convient de chiffrer les données sensibles qui y sont conservées.

Comment pouvez-vous utiliser votre téléphone portable ou votre tablette comme moyen de communication ?

Vous pouvez utiliser votre téléphone portable comme moyen de communication avec vos patients, d'autres professionnels de santé ou votre personnel. Assurez-vous, dans le cadre de vos déplacements, à ce que votre conversation de nature professionnelle ne soit pas entendue par des personnes à proximité.

L'utilisation de communications orales, de messageries instantanées ou « chat », via des applications reliées à internet et non sécurisées, est à proscrire. En effet, seule une application présentant les garanties suffisantes de protection des données peut être utilisée dans le cadre de votre exercice professionnel. A défaut, aucune information relative à un patient ou à un professionnel de santé intervenant dans sa prise en charge ne peut être échangée.

Vous pouvez consulter votre messagerie électronique sécurisée sur votre tablette ou votre téléphone portable en respectant les règles de sécurité décrites ci-dessus (voir la fiche n° 3 « Quel cadre appliquer à l'utilisation d'une messagerie électronique ? »).

Fiche 5.

Quel cadre appliquer aux recherches ?

Check-list des bonnes pratiques à respecter :

→ Je réalise une analyse d'impact avant la réalisation d'études internes sur les données de mes patients si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;

→ Dans le cadre de recherches en partenariat avec un tiers, je m'assure que les recherches sont menées conformément à la réglementation ;

→ Je tiens à jour le registre des activités de traitement (voir annexe n° 2 « Registre des activités de traitement ») ;

→ J'informe mes patients et m'assure du respect de leurs droits (voir annexe n° 1 « Notice d'information »).

Vous menez vous-même des études sur des patients dont vous assurez la prise en charge (« études internes ») ou vous intervenez dans des recherches médicales en partenariat avec des instituts de recherches, des CHU, etc.

Quelles sont vos obligations dans le cadre d'études internes ?

Vous souhaitez mener des études sur les données relatives à vos patients, à partir des données de santé, que vous avez obtenues à l'occasion de leur suivi.

Dans la mesure où ces études sont réalisées par vous et sont destinées à votre usage exclusif, aucune autorisation de la CNIL n'est nécessaire. Seul un avis favorable du Comité de Protection des Personnes (CPP) doit être recueilli préalablement à la mise en œuvre de la recherche si celle-ci implique la personne humaine.

En revanche, vous devrez :

- réaliser une analyse d'impact relative à chaque recherche ou à un ensemble de recherches similaires si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Une réflexion doit être menée sur l'utilisation qui va être faite des données personnelles dans le cadre de la recherche, sur les risques qui peuvent en résulter en ce qui concerne les droits et les libertés des personnes concernées et sur le niveau de protection nécessaire au regard de ces risques. La CNIL a mis en place un outil simple permettant de réaliser une analyse d'impact, accessible sur son site internet. Pour tout savoir sur l'analyse d'impact, vous pouvez consulter :

    - les fiches thématiques « Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données » (https://www.cnil.fr/fr/PIA-privacy-impact-assessment), « L'analyse relative à la protection des données » (https://www.cnil.fr/fr/PIA-privacy-impact-assessment)
    - les trois guides PIA (https://www.cnil.fr/fr/PIA-privacy-impact-assessment)
    - le logiciel que la CNIL met à votre disposition gratuitement pour procéder à vos analyses d'impact (https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia).

- renseigner votre registre des activités de traitement pour indiquer la nouvelle utilisation des données et les modalités (voir annexe n° 2 « Registre des activités de traitement ») et informer les patients de la réalisation de ces études. Il suffit d'ajouter une mention dans l'affichette d'information de votre salle d'attente.

Les règles de sécurité sont les mêmes que pour vos dossiers patients (voir l'annexe n° 1 « Exemple de notice d'information »).

Les droits des personnes doivent également être respectés.

Quelles sont vos obligations lors de recherches médicales en partenariat avec un tiers (recherche dite multicentrique) ou nécessitant un recueil de données supplémentaires ?

Si vous participez à des recherches médicales en partenariat avec un tiers ou nécessitant un recueil de données supplémentaires, que ce soit un institut de recherche ou un établissement de santé, que les données soient collectées dans le cadre de soins ou spécifiquement pour la recherche, un processus spécifique s'applique en amont de la recherche[23].

[23] Dispositions spécifiquement applicables aux traitements à des fins de recherche, étude ou évaluation dans le domaine de la santé du chapitre IX loi Informatique et libertés n°78-17 du 6 janvier 1978.

Le promoteur de la recherche, la personne à l'initiative et qui porte le projet de recherche (qui n'est pas forcément celui qui réalise en pratique la recherche ou qui contribue à la recherche), doit en tant que responsable de traitement, si une méthodologie de référence existe, procéder à une déclaration de conformité à cette méthodologie de référence. À défaut, il doit obtenir une autorisation de la CNIL.

Attention !

- Les formalités à accomplir auprès de la CNIL sont réalisées par le responsable de traitement.

- Si la recherche implique la personne humaine, le promoteur de la recherche ou celui qui porte le projet devra également vérifier, que la recherche relève d'une méthodologie de référence ou d'une demande d'autorisation, d'un avis favorable du Comité de Protection des Personnes (CPP).

- Si la recherche n'implique pas la personne humaine et seulement pour celles relevant d'une demande d'autorisation, le promoteur ou celui qui porte le projet doit également obtenir un avis du Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé (CEREES). Le dossier doit être adressé à l'Institut national des données de santé (INDS) qui assure le guichet unique.

Le promoteur ou celui qui porte le projet de recherche, en tant que responsable de traitement, doit réaliser une analyse d'impact si le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques et renseigner le registre des activités de traitement.

Les droits des personnes concernées devront être respectés. Ils devront être informés en amont de la recherche, de l'utilisation de leurs données pour cette recherche, de ses finalités, de leurs droits à cet égard. Ils disposent notamment d'un droit d'accès et d'un droit d'opposition. La note d'information doit vous être fournie par le promoteur de l'étude.

Fiche 6.

Quel cadre appliquer à la télémédecine ?

Check-list des bonnes pratiques à respecter :

→ Je m'assure que le prestataire de télémédecine choisi est bien conforme avec la réglementation ;

→ Je vérifie la présence des mentions obligatoires dans son contrat.

→ Je contrôle que le patient a bien été informé ;

Vous consacrez une partie de votre exercice professionnel à la télémédecine, que ce soit de la téléexpertise ou de la téléconsultation, via des plateformes de télémédecine.

Vos obligations changent-elles dans le cadre de la télémédecine ?

La télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication[24]. Lorsque vous réalisez une téléconsultation ou une téléexpertise, vous réalisez un acte médical.

L'ensemble de vos obligations déontologiques habituelles s'appliquent, ainsi que vos obligations relatives aux informations que vous êtes amené à connaître sur vos patients ou sur d'autres professionnels de santé intervenant dans leur prise en charge.

Les règles relatives à l'échange et au partage de données entre professionnels sont également applicables
(voir la fiche pratique du CNOM « Echange et partage d'informations », déc. 2016).
https://www.conseil-national.medecin.fr/sites/default/files/cnomechangepartageinfos_0.pdf

[24] Art. L.6316-1 du Code de la santé publique.

Quelles sont les obligations de la plateforme de télémédecine ?

Lorsque vous décidez d'utiliser une plateforme de télémédecine à l'occasion de votre activité, vous devez vous assurer que le prestataire (qui met à votre disposition cette plateforme et qui est votre sous-traitant), respecte la réglementation.

Le contrat de sous-traitance[25] doit bien indiquer que le sous-traitant :

- ne traite les données à caractère personnel que sur votre instruction ;
- 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 votre autorisation écrite préalable ;
- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement, notamment lorsque des patients ont des demandes concernant leurs données ;
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- collabore dans le cadre d'audits.

S'agissant des données de santé, la plateforme doit être hébergée par un hébergeur de données de santé agréé ou certifié.

[25] Art. 28 RGPD.

ANNEXES

Annexe n°1 : exemple de notice d'information pour la gestion d'un cabinet médical

Vous trouverez ci-dessous un exemple de notice d'information à utiliser pour votre cabinet médical.

« Votre médecin, le Dr. XX, [adresse], est amené à recueillir et à conserver dans un dossier, [votre dossier patient], des informations sur votre état de santé.

Pourquoi votre médecin tient-il un dossier sur vous ?
La tenue du dossier « patient » est obligatoire. Ce dossier a pour finalité d'assurer votre suivi médical et de vous garantir la prise en charge la plus adaptée à votre état de santé. Il garantit la continuité de la prise en charge sanitaire et répond à l'exigence de délivrer des soins appropriés.

Quelle est sa durée de conservation ?
Il est conservé en principe pendant 20 ans à compter de la date de votre dernière consultation, par référence aux dispositions de l'article R. 1112-7 du code de la santé publique applicables aux établissements de santé.

[Dans le cas d'un logiciel hébergé par un prestataire] *Votre dossier 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. Le 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 médecin 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 votre dossier ?
Seuls ont accès aux informations figurant dans votre dossier votre médecin et, dans une certaine mesure, au regard de la nature des missions qu'il exerce, son personnel. Votre médecin, avec votre consentement, pourra également transmettre à d'autres professionnels de santé des informations concernant votre état de santé. Enfin, afin de permettre la facturation des actes qu'il réalise, votre médecin 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 votre dossier. 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 médecin. 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 des dossiers des patients. Si d'autres traitements sont mis en place (ex : recherche, utilisation d'une plateforme sécurisée de gestion des rendez-vous), 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.

Annexe n° 2 : registre des activités de traitement

Vous trouverez ci-dessous un modèle pré-rempli d'un registre des activités de traitement pour un médecin exerçant en libéral. Ce modèle est à adapter en fonction de votre situation particulière et doit être rempli avec précision (votre éditeur de logiciel ou votre prestataire informatique assurant la maintenance peut vous donner les informations nécessaires).

Le registre peut être tenu sous format papier ou informatique.

Vous pouvez télécharger le modèle publié par la CNIL ici : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

Registre des activités de traitement du Dr. Hippocrate

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Dr. Charles Hippocrate 4 rue Léon Jost 75017 PARIS 01 22 15 .. .. charles.hipocrate@cabinethippocrate.fr
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	/

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités (exemples)
Activité 1	*Suivi des patients*
Activité 2	*Prise de rendez-vous (en cas d'externalisation de la prise de rendez-vous)*
Activité 3	*Etudes internes*
Activité 4	*Gestion de la paie*
Activité 5	*Gestion des fournisseurs*
Activité 6	*Sécurisation des locaux (si utilisation d'un dispositif de vidéosurveillance ou de badge de sécurité)*
Activité 7	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre pour l'activité 1est disponible sur la page suivante.

Fiche de registre de l'activité de suivi des patients

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	**01/07/2018**
Date de dernière mise à jour de la fiche	**/**
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	**/**
Nom du logiciel ou de l'application *(si pertinent)*	**Logiciel Dioclès**

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Le logiciel Dioclès permet le suivi des patients du cabinet. Il sert à mon activité de prévention, de diagnostic et de soins et à gérer le cabinet. Il permet les actions suivantes :

- la gestion des rendez-vous ;
- la gestion des dossiers médicaux ;
- l'édition des ordonnances ;
- l'envoi de courriers aux confrères ;
- l'établissement et la télétransmission des feuilles de soins.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

1. Patients
2. Professionnels de santé
3 Le cas échéant, famille du patient
4. ……

Catégories de données collectées

Listez les différentes données traitées

[X] Etat-civil, identité, données d'identification, images (nom, prénom, adresse, photographie, date et lieu de naissance, etc.)
……
……

[X] Vie personnelle (habitudes de vie, situation familiale, etc.)
Si nécessaire à la prise en charge du patient ……

[X] Vie professionnelle

Profession ou conditions de travail si ces données ont un impact sur la prise en charge médicale

[ ] Informations d'ordre économique et financier *(revenus, situation financière, données bancaires, etc.)*
……
……

[ ] Données de connexion *(adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
……
……
[ ] Données de localisation *(déplacements, données GPS, GSM, ...)*
……
……

[ ] Internet *(cookies, traceurs, données de navigation, mesures d'audience, ...)*
……
……

[ ] Autres catégories de données *(précisez)* :
……
……
……
……

Des données sensibles sont-elles traitées ?

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

[X] Oui [ ] Non

Si oui, lesquelles ? : Données de santé

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

20 …… ☐ jours ☐ mois ☒ ans

☐ Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

……

……

……

……

……

……

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

1. Secrétaire médical
2. ……
3 ……
4. ……

Organismes externes

1. Sécurité sociale
2. Professionnels de santé intervenant dans la prise en charge
3 ……
4. ……

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Éditeur de logiciel Diocèse s'il assure une prestation de maintenance informatique ou d'hébergement de données de santé
2. ……..
3. . ……..
3 ……..
4. ……..

Transferts des données hors UE

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

☐ Oui ☒ Non

Si oui, vers quel(s) pays :

……..

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés. Si vous ne disposez pas ces informations, demandez à votre éditeur de logiciel.

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures : Accès avec CPS par le Dr. Hippocrate et accès spécifique pour le secrétaire médical avec CPE

……..

☒ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Journalisation des accès des utilisateurs sur 6 mois avec conservation des identifiants, date et heure de connexion, durée de connexion et documents ou dossiers consultés

……..

[X] Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Installation d'antivirus et de pare-feu

……
……

……
……

[X] Sauvegarde des données

Décrivez les modalités :

Données sauvegardées hebdomadairement sur un serveur distinct

……
……

……
……

[X] Chiffrement des données

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.)* :

Le logiciel chiffre les données contenues.

……
……

……
……

[X] Contrôle des sous-traitants

Décrivez les modalités :

Vérification des engagements pris par le sous-traitant relativement à la sécurité des données dans le cadre du contrat de sous-traitance.

……
……
……

[ ] Autres mesures :

……

……

……

……

……

……

Lexique

→ **« Donnée à caractère personnel » ou « donnée personnelle »** : elle est définie comme *« toute information se rapportant à une personne physique identifiée ou identifiable »*, c'est-à-dire une *« personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*

→ **« Données de santé »** : elles désignent les « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

→ **« Traitement »** dans la réglementation relative à la protection des données n'a pas le sens médical habituel. Ce terme désigne *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».* Il s'agit donc de toute action réalisée sur des données personnelles, et ce dès la collecte de données.

→ **« Responsable de traitement »** : il s'agit de *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».*

→ **« Personne concernée » :** la personne physique (par opposition à une personnes morale, société privée, un organisme ou encore une autorité publique) identifiée ou identifiable à laquelle se rapport une information.

→ **« Destinataire »** : c'est *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ».*

→ **« Sous-traitant »** : il s'agit de « *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* ».

→ **Commission nationale de l'informatique et des libertés (CNIL)** : la CNIL est l'autorité compétente pour la protection des données personnelles en France. Vous trouverez des informations sur la réglementation sur son site internet : www.cnil.fr.

Cas pratique de synthèse
pour une bonne compréhension des termes du lexique

Le Docteur Hippocrate exerce seul en libéral. Il reçoit, pour la première fois, le patient Alphonse. Celui-ci lui parle de ses problèmes de dos, séquelles d'un vieil accident. Dr. Hippocrate créé un dossier patient dans son logiciel Dioclès, qu'il a mis en place il y a tout juste un mois, et y note ses observations. Un confrère lui avait recommandé ce logiciel très simple d'utilisation, accessible à distance et qui lui assurait la sécurité de ses dossiers. A la fin de la consultation, Dr Hippocrate effectue la télétransmission vers la sécurité sociale grâce à la carte vitale d'Alphonse. Il remet à Alphonse une ordonnance et rédige une lettre à un confrère spécialiste qu'il enverra.

Dans cette situation, y-a-t-il un traitement de données personnelles ?
La réponse est oui :

→ Données à caractère personnel : nom, prénom, informations relatives aux problèmes de dos, historique médical en lien avec l'accident, numéro de sécurité sociale ;

→ Données de santé : informations portant spécifiquement sur l'état de santé (problèmes de dos, historique médical en lien avec l'accident) ;

→ Traitement : enregistrement des données concernant Alphonse dans le logiciel Dioclès, hébergement des données par l'éditeur du logiciel Dioclès ou par son sous-traitant, télétransmission à la sécurité sociale, échange avec un confrère ;

→ Responsable de traitement : Dr. Hippocrate ;

→ Personne concernée : Alphonse ;

→ Destinataires : sécurité sociale, confrère, secrétaire médical ;

→ Sous-traitant : éditeur du logiciel Dioclès ou son sous-traitant hébergeur pour l'hébergement des données.

www.conseil-national.medecin.fr
www.cnil.fr

CONSEIL NATIONAL
DE L'ORDRE DES MÉDECINS
4 RUE LÉON JOST
75017 Paris
Tél. : 01 53 89 32 00
Fax : 01 53 89 32 01
conseil-national@cn.medecin.fr
@ordre_medecins

COMMISSION NATIONALE DE
L'INFORMATIQUE ET DES LIBERTÉS
3, PLACE DE FONTENOY - TSA 80715
75334 PARIS CEDEX07
Tél. : 01 53 73 22 22
Fax : 01 53 73 22 00