INPDP

الهيئة الوطنية لحماية المعطيات الشخصية

INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES

NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

PROTECTION DES DONNÉES PERSONNELLES - GUIDE PRATIQUE À DESTINATION **DES MÉDECINS**

Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

Source :
Commission nationale de l'informatique et des libertés, France :
Guide de la CNIL et de l'Ordre national des médecins (France)

GUIDE PRATIQUE SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

ÉDITION JUIN 2018

https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf

POURQUOI UN GUIDE PRATIQUE SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ?

La loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel est entrée en application le 02 août 2004. Elle constitue le socle de la réglementation sur la protection des données personnelles en Tunisie.

Le présent guide pratique a pour ambition d'orienter les médecins, en exercice libéral, dans la mise en œuvre des obligations prévues par la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et par la délibération n°4 du 5 septembre 2018 de l'Instance nationale de protection des données personnelles (INPDP) concernant le traitement des données à caractère personnel liées à la santé.

Si vous exercez au sein d'un établissement de santé, d'une maison de retraite, 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 chargé de protection des données personnelles (DPO), ce dernier est l'interlocuteur privilégié pour vous renseigner sur l'état de conformité de votre structure à la loi ou répondre à toutes vos questions.

POURQUOI ÊTES-VOUS CONCERNÉ PAR LA LOI ORGANIQUE N° 2004-63 DU 27 JUILLET 2004, PORTANT SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ?

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 générale, vous collectez également des informations pour gérer votre cabinet (p. 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 à caractère personnel.

La loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel définit les données à caractère personnel comme étant «*toutes les informations quelle que soit leur origine ou leur forme et qui permettent directement ou indirectement d'identifier une personne physique ou la rendent identifiable, à l'exception des informations liées à la vie publique ou considérées comme telles par la loi*». Au sens de l'article 5 de ladite loi : «*Est réputée identifiable, la personne physique susceptible d'être identifiée, directement ou indirectement…*».

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 (p. ex. nombre d'enfants), sa couverture sociale (p. ex. assurance maladie obligatoire, assurance maladie complémentaire, etc.) et surtout d'informations relatives à sa santé (pathologies, diagnostics, prescriptions, soins, etc.) et 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'immatriculation à la Caisse nationale d'assurance maladie-CNAM) pour facturer les actes réalisés.

Pour toutes ces situations où vous utilisez ces données personnelles, vous êtes concerné par la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel.

FICHE 1

QUEL CADRE APPLIQUER AUX DOSSIERS DES PATIENTS ?

Check-list des bonnes pratiques à respecter :

- Je limite les informations collectées au strict 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 loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel. 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 à caractère personnel.

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 transmission 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, l'INPDP 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 d'immatriculation à la Caisse nationale d'assurance maladie : uniquement pour l'édition des feuilles de soins et la transmission 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
- Les 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 (p. 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 (p. 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, l'INPDP préconise de s'aligner sur les délais de conservation recommandés pour les dossiers médicaux des établissements de santé :

- 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.

Cette information peut se faire par voie d'affichage dans la salle d'attente ou par la remise d'un document spécifique (p. 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 des données, y compris les finalités ultérieures
- Les destinataires des données
- La durée de conservation
- Les droits de la personne concernée : accès, rectification, à certaines conditions effacement, limitation, opposition, introduction d'une réclamation auprès de l'INPDP
- Le 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 (p. ex. si un médecin souhaite utiliser ultérieurement les données à des fins de recherche)

Vos patients disposent de droits. Ils peuvent :

- Accéder aux données les concernant
- Rectifier ces données en cas d'erreur
- S'opposer au traitement des données pour des raisons tenant à leur situation particulière
- Obtenir que leurs données soient effacées, 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 ne dépassant pas un mois à compter de la date de dépôt de la demande.

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 (p. ex. équipe de soin 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. 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, n° CNAM, date de la consultation) sont adressées aux organismes d'assurance maladie via la transmission des feuilles de soins.

Si une recherche était finalement menée, une information individuelle devrait être réalisée. Elle sera préalable à la mise en œuvre de la recherche et spécifique à chaque recherche.

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 les lire.

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 un hébergeur qualifié et accrédité pour l'hébergement de données de santé conformément aux dispositions de l'article 16 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

En toute hypothèse, dès que vous sollicitez les services d'un prestataire (société de maintenance, hébergeur de données de santé qualifié et accrédité), 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 :

- Ne traite les données à caractère personnel que sur votre instruction
- Veille à la signature d'engagements de confidentialité par son 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 des données 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.

Vous devez respecter les mesures de sécurité recommandées par l'INPDP.

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 l'ANSI (voir sur ce point, le guide de sécurité informatique «Bien choisir un mot de passe»), au moins 8 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 un moyen d'authentification forte

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).

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 qualifié et accrédité pour l'hébergement des données de santé conformément à la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

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, code, etc).

En cas de violation de données (destruction, perte, altération, divulgation non autorisée de données à caractère personnel, accès non autorisé 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 ?
- S'il existe un risque pour les données personnelles des personnes physiques, il est recommandé de notifier la violation de données à l'INPDP. 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.
- Si la violation de données engendre un risque élevé pour les données personnelles des personnes concernées, sur demande de l'INPDP 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.
Cette communication doit être faite 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 de votre structure, vous devez notifier cet incident à l'Agence nationale de la sécurité informatique (ANSI), conformément à la loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique et notamment son article 10. En ce qui concerne l'INPDP, la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel ne prévoit pas de disposition explicite de notification mais il est recommandé de lui notifier l'incident, en vertu du principe de la transparence du traitement.

Devez-vous accomplir une formalité préalable particulière auprès de l'INPDP pour le traitement des données de santé ?

Tout traitement de données à caractère personnel liées à la santé est soumis à une déclaration et une autorisation préalable de l'Instance, conformément aux articles 7 et 14 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, aux dispositions du décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel

et à l'article 8 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

Le traitement des données à caractère personnel relatives à la santé ne peut être mis en œuvre que par des médecins ou des personnes soumises, en raison de leur fonction, à l'obligation de garder le secret professionnel (Article 63 de la loi organique n° 2004-63). Pour autant, le responsable de traitement doit être en mesure de démontrer, à tout moment, la conformité du traitement de données aux exigences de la loi en traçant toutes les démarches entreprises, la réalisation d'une analyse d'impact, la tenue du registre des activités de traitement, etc.

Vous devez tenir un registre des activités de traitement, que vous conservez en interne, 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 ou d'un dispositif de télémédecine, etc.

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 plus loin 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 chargé de protection des données personnelles (DPO) ?

Chaque responsable du traitement des données doit désigner un chargé de protection des données à caractère personnel, informer l'INPDP de la décision de nomination et la rendre publique, conformément à l'article 15 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

Le chargé de la protection des données à caractère personnel accomplit les tâches suivantes, avec toute impartialité et indépendance :

- Tenir un registre des activités de traitement effectuées par le responsable du traitement ou le sous-traitant. Toute personne concernée peut y accéder à sa demande
- Accepter les demandes d'accès aux données personnelles
- Réglementer toutes les activités internes liées à la protection des données personnelles
- Préparer un programme d'action pour améliorer la protection des données à caractère personnel en coopération avec le responsable du traitement
- Préparer un rapport annuel sur les activités liées à la protection des données personnelles qui sera envoyé par voie électronique à l'INPDP et publié sur le site internet de l'organisme
- Faire le lien entre la structure responsable du traitement et l'Instance nationale de protection des données à caractère personnel

Le responsable du traitement doit mettre à la disposition du chargé de protection des données personnelles les moyens humains et matériels requis pour effectuer ses tâches.

Pouvez-vous être sanctionné ?

Toute violation des dispositions réglementant le traitement des données à caractère personnel liées à la santé peut entrainer des sanctions prévues par la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel.

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 sa conformité 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 des données » (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 (p. ex. consulter un cardiologue régulièrement).

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

En tant que responsable du 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 l'INPDP 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, qui effectue la sous-traitance d'un service de prise de rendez-vous en ligne ou celui de permanence téléphonique (données d'agenda), est aussi un responsable de traitement pour ce qui concerne les données de ses propres salariés. Il est également responsable de traitement de façon limitée des données d'identification créées par les patients et les professionnels de santé dans le cadre de la gestion de comptes en ligne (identifiant, mot de passe).

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 loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel. 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. Ceci s'effectue 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).

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

- Ne traite les données à caractère personnel que sur votre instruction
- Veille à la signature d'engagements de confidentialité par son 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 du 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

En cas d'incident lié aux données qu'il gère pour votre compte (faille de sécurité, piratage, perte, etc.), le prestataire doit vous informer dans les meilleurs délais, afin que vous puissiez remplir 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 qualifié et accrédité conformément à la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.
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 ?

Toute violation des dispositions réglementant le traitement des données à caractère personnel liées à la santé peut entrainer les sanctions prévues par la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel.

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 »).

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 soumis 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.

L'utilisation de la messagerie sécurisée est possible dès lors que vous obtenez une autorisation auprès de l'INPDP. Pour autant, le traitement découlant de l'utilisation de la messagerie sécurisée devra être inscrit sur votre registre des activités de traitement des données (sur ce point, voir l'annexe n° 2 « Registre des activités de traitement »).

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. Néanmoins, l'utilisation d'une telle messagerie n'est possible qu'entre professionnels de santé.

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

- Chiffrer les données sensibles à transmettre. À ce sujet, il convient de se référer aux préconisations de l'INPDP

- 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 (p. ex. mot de passe) en utilisant un canal de nature différente (p. ex. téléphone, SMS, etc.)

Aussi, l'utilisation de toute messagerie hébergeant les données de santé en dehors de la Tunisie 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.

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 pouvez être 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 utilisée, 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 l'ANSI (au moins 8 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 médicaux de vos patients doit se faire conformément aux recommandations de sécurité élaborées par l'INPDP (p. ex. la sécurité des conditions d'accès à distance des données de vos patients). Ces recommandations peuvent être obtenues sur demande d'avis auprès de l'Instance.

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. Dans le cadre de vos déplacements, assurez-vous 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
- 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 des données (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 hôpitaux, 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 à des fins qui n'excèdent pas l'usage exclusif du médecin, à condition qu'elles ne soient pas transmises à des tiers, aucune autorisation de l'INPDP n'est nécessaire.

En revanche, vous devrez 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.

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, procéder à une déclaration et demander une autorisation préalable auprès de l'INPDP.

Attention !

- Les formalités à accomplir auprès de l'INPDP sont réalisées par le responsable de traitement.
- Si la recherche implique des personnes physiques identifiées ou identifiables, le promoteur de la recherche ou celui qui porte le projet devra également vérifier que la recherche relève d'une demande d'autorisation auprès de l'INPDP et d'un avis favorable du Comité de protection des personnes (CPP).
- Le promoteur ou celui qui porte le projet de recherche, en tant que responsable de traitement, doit réaliser une analyse d'impact et renseigner le registre des activités de traitement.
- Les droits des personnes concernées devront être respectés. Elles devront être informées, en amont de la recherche, de l'utilisation de leurs données pour cette recherche, de ses finalités, ainsi que de leurs droits à cet égard. Elles 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 ?

À noter :

- La télémédecine est une activité dont les conditions d'exercice et d'organisation sont réglementées par les dispositions de l'article 23 bis de la loi n° 91-21 du 13 mars 1991, relative à l'exercice et à l'organisation des professions de médecin et de médecin dentiste telle que complétée par la loi n° 2018-43 du 11 juillet 2018.
- Les conditions générales de l'exercice de la télémédecine et les domaines de son application sont fixés par décret gouvernemental.
- Les conditions spécifiques de la réalisation d'actes de télémédecine pour chaque spécialité médicale ou chirurgicale sont fixées par arrêté du ministre chargé de la santé.
- Le décret gouvernemental ainsi que l'arrêté du ministre de la santé ne sont pas encore promulgués (à la date de publication). Les recommandations ci-après devront être prises en compte au regard des spécifications de ces textes une fois adoptés.

Check-list des bonnes pratiques à respecter :

- Je m'assure que le prestataire de télémédecine choisi est bien conforme à 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. 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.

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 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 son 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 de données, 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, qualifié et accrédité pour cette tâche, en vertu d'une décision conjointe émise par l'INPDP, l'Agence nationale de la sécurité informatique et l'Instance nationale de l'évaluation et de l'accréditation en santé, conformément à l'article 16 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

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.

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 (p. ex. recherche, utilisation d'une plateforme sécurisée de gestion des rendez-vous), vous devrez réaliser une information spécifique concernant ces traitements de données portant notamment sur la finalité de ces traitements, le fondement légal, la durée de conservation des données.

« 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 pendant X années [durée raisonnable estimée en fonction de la nature et de la finalité du traitement des données]*, par référence aux dispositions de l'article 10 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.*

[Dans le cas d'un logiciel hébergé par un prestataire] Votre dossier est hébergé sur les serveurs de XXX, qui dispose d'une accréditation délivrée en application des dispositions de l'article 16 de la délibération n°4 de l'INPDP du 5 septembre 2018 concernant le traitement des données à caractère personnel liées à la santé. 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.xx.

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. Avec votre consentement, votre médecin 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 transmettre 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 l'INPDP d'une réclamation.

ANNEXE N°2

REGISTRE DES ACTIVITÉS DE TRAITEMENT DES DONNÉES

Vous trouverez ci-dessous un modèle pré-rempli de registre des activités de traitement des données 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.

Il est indépendant de l'obligation de déclaration et d'autorisation préalable au traitement des données à caractère personnel auprès de l'INPDP (voir sur ce point, les formulaires nécessaires pour l'accomplissement des procédures légales auprès de l'Instance).
Pour plus d'informations, veuillez consulter le site de l'INPDP qui fournit un modèle général de registre.

Registre des activités de traitement du Dr. XXX

Activités de l'organisme impliquant le traitement de données personnelles

Coordonnées du responsable de l'organisme (responsable de traitement ou son représentant si le responsable est situé en dehors de la Tunisie)	Dr. Adresse Téléphone e-mail
Nom et coordonnées du chargé de protection des données personnelles (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 vidéo-surveillance ou de badge de sécurité)
Activité 7	

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

(Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre pour l'activité 1 est disponible ci-dessous).

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	**JJ/MM/AAAA**
Date de la dernière mise à jour de la fiche	/_ _
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de données est partagée avec un autre organisme)	
Nom du logiciel ou de l'application (si pertinent)	

Objectifs poursuivis

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

Le logiciel XXX 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 *(à adapter selon les cas)* :

- La gestion des rendez-vous
- La gestion des dossiers médicaux
- L'édition des ordonnances
- L'envoi de courriers aux confrères
- L'établissement et la transmission 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
.....
.....

- État civil, identité, données d'identification, images *(nom, prénom, adresse, photographie si applicable, date et lieu de naissance, etc.)*

.....
.....

- Vie personnelle *(habitudes de vie, situation familiale, etc. si nécessaire à la prise en charge du patient)*

.....
.....

- 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 *(si applicable 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 la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et par la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé 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.

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

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

X jours X mois X 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 de maintenance informatique, etc.)

1. Éditeur de logiciel XXX *(s'il assure une prestation de maintenance informatique ou d'hébergement de données de santé)*
2. .....
3. .....
4. .....

Transferts des données en dehors de la Tunisie

Des données personnelles sont-elles transmises en dehors de la Tunisie ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays :
.....

En cas de transfert à l'étranger, des garanties spécifiques devront être prévues et documentées dans le registre. Consultez la délibération n°3 du 5 septembre 2018 de l'INPDP portant identification des États ayant un niveau de protection adéquat en matière de protection des données personnelles.

- 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 des données. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés. Si vous ne disposez pas de ces informations, demandez à votre éditeur de logiciel.

- Contrôle d'accès des utilisateurs

Décrivez les mesures : p.ex. Accès avec un moyen d'authentification forte (utilisation d'un mot de passe conforme aux recommandations de l'ANSI, verrouillage automatique après un court délai, chiffrement des données sensibles) par le Dr. XXX et accès spécifique pour le secrétaire médical.

.....
.....

- 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 (de préférence) avec conservation des identifiants, date et heure de connexion, durée de connexion et documents ou dossiers consultés

.....
.....

- 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

.....
.....
.....
.....

- Sauvegarde des données

Décrivez les modalités :

Données sauvegardées hebdomadairement sur un serveur distinct

.....
.....
.....
.....

- Chiffrement des données

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

Le logiciel chiffre les données contenues.
.....
.....
.....
.....

- Contrôle des sous-traitants

Décrivez les modalités :

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

Autres mesures :
.....
.....
.....
.....

LEXIQUE

SOURCE :

- Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
- Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé

>> « Données à caractère personnel » ou « données personnelles » : Il s'agit de « toutes les informations, quelle que soit leur origine ou leur forme et qui permettent d'identifier une personne physique ou la rendent identifiable, directement ou indirectement à travers plusieurs informations ou symboles, et notamment à travers un élément d'identité spécifique tel que le nom, le numéro d'identité ou la situation familiale ». Est réputée identifiable, « la personne physique susceptible d'être identifiée, directement ou indirectement, à travers plusieurs données ou symboles qui concernent notamment son identité, ses caractéristiques physiques, physiologiques, génétiques, psychologiques, sociales, économiques ou culturelles ».

>> « Données à caractère personnel liées à la santé » ou « Données de santé » : Il s'agit « des données personnelles sensibles qui consistent en toutes les informations liées à l'état de santé physique, mentale ou psychologique de la personne physique concernée par le traitement, ainsi qu'à ses caractéristiques génétiques héréditaires ou acquises et qui fournissent des informations qui lui sont spécifiques ou sur son état de santé et qui résultent notamment de l'analyse d'un échantillon biologique de cette personne, ainsi que des services de soins médicaux qui lui sont fournis et qui peuvent révéler ces informations. »

>> « Traitement des données à caractère personnel » : Ce terme désigne « les opérations réalisées d'une façon automatisée ou manuelle, et qui ont pour but notamment la collecte des données à caractère personnel, leur accès, leur enregistrement, leur sauvegarde, leur organisation, leur correction, leur exploitation, leur utilisation, leur envoi, leur diffusion, leur publication, leur liaison à d'autres données, leur communication, leur transfert, leur exposition de quelque manière que ce soit, l'anonymisation de leur identité, leur pseudonymisation, leur effacement ou leur 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 « toute personne physique ou morale, tunisienne ou étrangère, appartenant au secteur privé ou public, qui détermine la nature des données à caractère personnel liées à la santé, la finalité ainsi que les modalités de leur traitement ».

>> « Personne concernée » : C'est « toute personne physique dont les données à caractère personnel liées à la santé font l'objet d'un traitement, ainsi que son tuteur ou ses héritiers, sauf si la personne s'y oppose explicitement avant son décès ».

>> « Bénéficiaire » : C'est « toute personne physique ou morale recevant des données à caractère personnel ».

>> « Sous-traitant » : Il s'agit de « toute personne physique ou morale qui traite des données à caractère personnel liées à la santé pour le compte du responsable du traitement et sous sa supervision ».

>> « Instance nationale de protection des données personnelles (INPDP) »: C'est l'autorité compétente pour la protection des données personnelles en Tunisie. Vous trouverez des informations sur la réglementation sur son site internet : www.inpdp.nat.tn.

CAS PRATIQUE DE SYNTHÈSE POUR UNE BONNE COMPRÉHENSION DES TERMES DU LEXIQUE

Le Docteur XXX exerce seul en libéral. Il reçoit, pour la première fois, le patient YYY. Celui-ci lui parle de ses problèmes de dos, séquelles d'un vieil accident. Dr. XXX créé un dossier patient dans son logiciel ZZZ, 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. Il remet au patient YYY 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 de données :**
enregistrement des données concernant le patient YYY dans le logiciel ZZZ, hébergement des données par l'éditeur du logiciel ZZZ ou par son sous-traitant, échange avec un confrère

>> **Responsable de traitement :**
Dr. XXX

>> **Personne concernée :**
patient YYY

>> **Destinataires :**
sécurité sociale, confrère, secrétaire médical ;

>> **Sous-traitant :**
éditeur du logiciel ZZZ ou son sous-traitant hébergeur pour l'hébergement des données.

www.inpdp.nat.tn

Mes notes

Conseil national de l'ordre des médecins (CNOM)
Adresse : Rue de Malaga, El Manar I, 2092, Tunis
Tél. : 71 881 275 / 98 707 076
cnom@planet.tn

Instance nationale de protection des données personnelles (INPDP)
Adresse : 1, Rue Mohamed Moalla, 1002, Mutuelleville, Tunis B.P. 525
Tél. : 71 799 853 / 71 799 711
Fax : 71 799 823
inpdp@inpdp.tn