INPDP

الهيئة الوطنية لحماية المعطيات الشخصية

INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES

NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

PROTECTION DES DONNÉES PERSONNELLES DANS LES ÉTABLISSEMENTS DE SANTÉ - **OBLIGATION LÉGALES DES PERSONNELS**

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

Ce document présente deux exemples d'information à l'attention du personnel des établissements de santé (hôpitaux, cliniques, laboratoires, cabinets de radiologie, etc...). Ils ont pour objectif de les guider dans les obligations légales et de bonnes pratiques en matière de protection des données à caractère personnel, des patients comme des membres du personnel.

Afin de faciliter leur adaptation par l'établissement qui souhaiterait les utiliser, les éléments à modifier (noms, adresse, contacts, sites webs, etc...) sont clairement identifiés dans les textes.

Les documents sources qui ont servi de base à ces modèles sont accessibles ci-dessous par QR code.

Source:

Dépliant à destination du personnel des Sherwood Forest Hospitals, Code des Gloucestershire Hospitals

https://www.sfh-tr.nhs.uk/media/1964/code-of-conduct-leaflet-gdpr-compliant.pdf

https://www.gloshospitals.nhs.uk/media/documents/Data_Protection__Confidentiality_Policy_B0734.pdf

LOGO DE L'HÔPITAL

PROTECTION ET CONFIDENTIALITÉ DES DONNÉES À CARACTÈRE PERSONNEL

OBLIGATIONS LÉGALES DES MEMBRES DU PERSONNEL

INTRODUCTION

Tous les employés de l'hôpital XXX sont responsables du maintien de la confidentialité des données du personnel et des patients, et ce devoir de confidentialité est inscrit dans les contrats de travail/dans le principe du respect du secret professionnel (selon qu'il s'agit d'une structure publique ou privée).

Le personnel est autorisé à accéder aux données à caractère personnel selon le principe du besoin d'en connaître, afin de permettre l'exercice de ses fonctions. L'accès à des données qui ne sont pas nécessaires à l'exécution du travail ou la transmission de données à une personne qui n'est pas autorisée à les recevoir constitue une violation de la confidentialité qui peut entraîner des mesures disciplinaires.

Les violations graves de la législation sur la protection des données personnelles peuvent entraîner des sanctions pécuniaires.

Recommandations de bonnes pratiques :

Le principe de responsabilisation est au cœur des bonnes pratiques de l'hopital XXX . Il recouvre notamment les pratiques suivantes :

1. Traiter les données d'une manière transparente et légitime.
2. Collecter les données pour des finalités spécifiques, claires et légitimes.
3. Traiter les données conformément à la finalité assignée et sur la base du consentement de la personne concernée tel que défini par la délibération n°4 de l'INPDP ou des fins légitimes mentionnées dans ladite délibération.
4. Collecter les données auprès de la personne concernée dans la mesure du possible, ou le cas échéant, auprès d'autres sources, à condition de respecter les principes de transparence, de légitimité et de secret professionnel stipulés dans la législation en vigueur.
5. Assurer l'exactitude des données, leur mise à jour et leur cohérence avec la finalité du traitement et dans ses limites.
6. Prendre, dès la conception des systèmes de traitement des données, les mesures techniques nécessaires pour protéger ces données.
7. Respecter les droits de la personne concernée.
8. Protéger les données personnelles et les incorporer dans le système de traitement des données existant, ou les prendre en compte dès la conception de ce système.
9. Le responsable du traitement des données et son sous-traitant doivent prouver à l'INPDP qu'ils ont pris toutes les mesures appropriées pour réaliser cette protection conformément aux obligations qui leur incombent et énoncées dans la délibération n°4.
10. Le responsable de traitement et son sous-traitant, qui ne font pas partie des professions de santé, traitent les données à caractère personnel liées à la santé dans le cadre du respect des règles du secret professionnel et avec le même niveau de protection exigé des membres des professions de santé.

Le terme «données à caractère personnel» fait référence à 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. Par exemple, le nom, l'adresse, le code postal, le numéro d'identité ou la situation familiale, etc. Toute donnée à caractère personnel, qu'elle soit sensible ou non, doit être traitée de manière confidentielle.

PRINCIPES ESSENTIELS

Toute donnée à caractère personnel collectée dans un but précis ne doit pas être utilisée dans un autre but sans le consentement de la personne concernée.

Le droit d'un individu à la confidentialité est protégé par l'éthique et la loi. Les personnes qui font appel aux services de l'hôpital XXX ou qui sont employées par l'hôpital XXX ont le droit de savoir quelles données sont collectées et pourquoi, ainsi que les objectifs du partage de ces données.

Une personne a le droit de choisir de divulguer ou non ses données et peut modifier sa décision à tout moment.

Chaque membre du personnel a l'obligation de protéger la confidentialité et a le devoir de vérifier que toute autre personne demandant accès à ces données en a l'autorisation. Cela permet de garantir que les données ne sont transmises qu'aux personnes qui ont le droit de les consulter. Tous les membres du personnel doivent comprendre qu'il leur incombe de protéger les données qu'ils recueillent et suivre les règles et les conseils qui leur sont donnés.

Les données concernant la santé des patients ne peuvent être utilisées à des fins commerciales.

Les règles protègent à la fois le patient et le personnel contre les violations de confidentialité. Toutefois, elles ne doivent pas être appliquées d'une manière si rigide qu'elles ne soient pas pratiques à suivre ou qu'elles nuisent à la santé et aux soins de la personne concernée.

Consentement

Pour être valable, le consentement doit être donné volontairement et librement. Un patient/employé doit être pleinement informé et savoir quelle sera l'utilisation ou la divulgation envisagée de ses données personnelles.

Le consentement explicite d'un patient doit toujours être demandé en cas d'utilisation de ses données d'une manière qui ne contribue pas directement à ses soins de santé.

Dans certaines circonstances, il peut être légal de partager des données à caractère personnel sans le consentement du patient (par exemple, dans le cadre d'une enquête sur un crime grave, pour protéger les enfants ou pour des raisons d'intérêt public).

SÉCURITÉ DE L'INFORMATION

Toutes les précautions raisonnables doivent être prises pour protéger la sécurité physique des données contre la perte, la détérioration ou la destruction accidentelle et contre la divulgation non autorisée ou accidentelle.

- N'utilisez pas le mot de passe de quelqu'un d'autre pour accéder aux informations contenues dans les ordinateurs.
- Aucune donnée personnelle ne doit être conservée sur un appareil mobile (par exemple, un ordinateur portable, un assistant numérique personnel, une clé USB), à moins qu'elle soit cryptée selon une norme approuvée.
- La télécopie n'est pas sécurisée. Les données personnelles ne doivent être faxées que lorsqu'il n'y a pas d'autre solution et que leur réception immédiate est nécessaire à des fins cliniques. Des procédures spécifiques doivent être respectées en cas de transfert vers l'étranger.
- Les enveloppes contenant des données personnelles doivent être scellées de manière sûre, porter la mention «confidentiel» et être clairement adressées à une personne contact identifiée.
- Les procédures de validation des appels téléphoniques doivent être suivies pour confirmer l'identité des appelants avant que des informations leur soient communiquées.
- Le personnel doit toujours s'assurer que la politique de l'hôpital XXX est respectée lors de l'envoi de données à caractère personnel par courrier électronique.
- Suivez les politiques et procédures de l'hôpital XXX en matière de protection des données, de confidentialité et de sécurité des informations et demandez conseil en cas de doute.

Si vous n'êtes pas sûr de devoir divulguer des informations, consultez votre supérieur hiérarchique et/ou, si nécessaire, demandez conseil au chargé de protection des données personnelles (DP2).

LÉGISLATION

- Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, telle que modernisée à la lumière de la Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
- 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

L'organisme de santé doit se conformer à six principes clés de traitement des données à caractère personnel.

Les données personnelles doivent être :

1. Traitées de manière équitable, loyale et légale
2. Traitées uniquement pour des finalités licites, déterminées et explicites
3. Adéquates, pertinentes et non excessives
4. Conservées de manière exacte et à jour
5. Ne pas être conservées plus longtemps que nécessaire
6. Conservées en toute sécurité et protégées contre toute divulgation, perte ou dommage accidentel

Le code de conduite

Le code de conduite définit les règles qui régissent l'utilisation des informations relatives aux patients au sein de l'hôpital XXX et le contrôle que le patient peut exercer à cet égard. Elle porte sur les droits d'accès des individus à leurs propres informations, sur la manière dont les informations seront partagées et sur la manière dont les décisions relatives au partage des informations seront prises. Toute personne travaillant pour l'hôpital XXX doit se conformer à ces directives.

Pour plus d'information ou un conseil :
Gouvernance de l'information

(À compléter selon le cas : pages site web dédiées, nom et contact du DP2,
d'un responsable de l'information, Responsable de la sécurité des systèmes d'information (RSSI) etc...)

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

SITES WEB UTILES

Instance nationale de protection des données personnelles (INPDP)
http://www.inpdp.nat.tn/

l'hôpital XXX

Ministère de la santé
http://www.santetunisie.rns.tn/fr//

Code de conduite (si applicable)

Adresse de l'hôpital

Tel: .....

Site: .....

NOM DE L'HÔPITAL

CODE DE CONDUITE RELATIF À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (MISE À JOUR : MOIS/ANNÉE)

INTRODUCTION

Conformément à la loi organique n° 2016-22 du 24 mars 2016, relative au droit d'accès à l'information, ce document peut être mis à la disposition du public et des personnes extérieures à XXX (nom de la structure de santé).

Attention : seuls sont valables les documents les plus récents (voir date de mise à jour).

À L'USAGE DE :

Ce code de conduite doit être observé par l'ensemble du personnel et des prestataires de (nom de la structure de santé) XXX.

ACCÈS RAPIDE *(mettre le lien du document correspondant)* :

- **Politique de gouvernance de l'information**
- **Politique de sécurité informatique**
- **Politique de gestion des dossiers**
- **Normes sur la tenue des dossiers cliniques**

1. INTRODUCTION / OBJECTIF

Le cadre offert par le présent code vise à ce que *(nom de la structure de santé)* respecte les exigences des textes réglementaires et légaux relatifs à l'utilisation des données personnelles, notamment :

- Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
- Convention n°108 pour la protection des personnes à l'égard du traitement automatis des données à caractère personnel
- 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
- 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

2. DÉFINITIONS

Terme / Expression	Explication
Doit / devra / il faut	Ces expressions s'appliquent à une disposition obligatoire.
Devrait / il convient de	Ces expressions s'appliquent à une disposition recommandée.
Peut / pourrait / il est possible	Ces expressions s'appliquent à une disposition facultative.
« Données à caractère personnel » ou « Données personnelles »	La définition utilisée ici est celle de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable.
Traitement des données	Toute opération ou série d'opérations réalisée sur des données personnelles.
Pseudonymisation	Opération effectuée sur les données à caractère personnel d'une manière qui permette de ne plus identifier directement la personne concernée par le traitement et ce à travers le recours à un code conservé séparément et soumis à des mesures techniques et organisationnelles afin de garantir la non-identification de la personne à travers ses données personnelles.
Données de santé	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 des données, 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. Ces données font partie des catégories particulières de données bénéficiant d'une protection spécifique dans la loi du 27 juillet 2004.
Instance nationale de protection des données personnelles (INPDP)	Il s'agit de 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**.
Délégué à la protection des données (DP2)	Personne qualifiée désignée pour assurer le respect des règles et principes de la protection des données à caractère personnel. Cette personne est l'interlocuteur, interne comme externe, pour toute question portant le sujet.

3. DÉCLARATION DE PRINCIPE

Le présent code de conduite offre un cadre solide qui permet d'assurer une approche cohérente de la conformité et des bonnes pratiques en matière de protection des données personnelles dans toute la structure de santé. Elle vient conforter les exigences énoncées dans le code de déontologie en matière de confidentialité. Ce code s'applique à tout le personnel (y compris le personnel temporaire, intérimaire et bénévole) et fait partie des conditions d'emploi de l'ensemble du personnel.

Le présent code de conduite assure la conformité avec les principes de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, et de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé et avec les politiques de *(Nom de la structure de santé)* concernant la conservation et la suppression des données personnelles.

Les personnes désignées comme responsables du traitement des données sont tenues d'observer les principes de ce code.

Le présent code de conduite vient à l'appui des objectifs et des normes énoncées à (l'article ou la section xx de [titre du document de politique de la structure de santé en matière de gouvernance de l'information et/ou en matière de confidentialité et de sécurité des données personnelles]. Elle couvre l'ensemble des données personnelles créées, traitées et archivées par *(Nom de la structure de santé)*, y compris mais pas uniquement, les données relatives aux patients et aux membres du personnel.

TOUT MANQUEMENT À CE CODE DE CONDUITE PEUT DONNER LIEU À DES SANCTIONS DISCIPLINAIRES.

4. RÔLES ET RESPONSABILITÉS

Fonction / équipe	Détails
Délégué à la protection des données personnelles (DP2)	Comme prévu par les articles 3 et 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, notamment : • Informer et conseiller la structure de santé employés sur les obligations qui leur incombent en vertu de la législation sur la protection des données • Contrôler le respect de la législation sur la protection des données • Dispenser des conseils concernant les analyses d'impact relatives à la protection des données et vérifier leur exécution
Conseil d'administration de la (nom de la structure de santé) ou organe de direction approprié, (selon le cas)	• Approuver la politique de la structure de santé en matière de gouvernance de l'information, en tenant compte des exigences juridiques et de ses propres exigences. Ce rôle peut être délégué à une sous-commission ou à une direction exécutive appropriée • Recevoir, au moins une fois par an, des rapports sur l'exécution de la politique de nom de la structure de santé en matière de gouvernance de l'information
Responsable de la gouvernance et de la sécurité de l'information ou l'administration de la structure (selon le cas)	• Assurer le rôle de responsable de la gouvernance et de la sécurité de l'information pour la structure de santé • Présider le Comité des dossiers médicaux et de la gouvernance de l'information mis en place par la structure de santé • Nommer le/la délégué à la protection des données personnelles • Superviser les questions de gouvernance de l'information au quotidien • Élaborer et mettre à jour les politiques, normes, procédures et orientations • Coordonner les questions de gouvernance de l'information au sein de la structure de santé et sensibiliser à ces questions • Coordonner la réalisation et la présentation annuelle des questions de gouvernance des données • Diriger le suivi des incidents informationnels graves nécessitant une enquête (politique de gestion des risques)

Managers	Comme prévu par les articles 3 et 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, notamment : • Veiller à ce que le présent code et les documents afférents se traduisent dans les processus en place au niveau local • Veiller à ce que le développement de tout nouveau système respecte les exigences en matière de protection des données personnelles
Tous les membres du personnel	• Connaître les exigences et les normes en matière de protection des données personnelles, y compris les responsabilités liées à leur rôle spécifique, et respecter ces normes et responsabilités • Suivre la formation obligatoire sur la gouvernance de l'information et le code de confidentialité • Signaler tout incident relatif à la protection et à la confidentialité des données, y compris les violations de données, via un outil de signalement de la structure de santé • Faire remonter à leurs supérieurs hiérarchiques toute préoccupation relative à la protection et à la confidentialité des données
Gestionnaires des systèmes	• Veiller à ce que tous les fournisseurs, qu'ils installent de nouveaux systèmes ou assurent la maintenance des anciens, attestent respecter les exigences en matière de protection des données personnelles • Présenter les formulaires demandés relatifs aux systèmes de gouvernance de l'information • Attester, sur demande, de leur conformité aux exigences en matière de protection des données personnelles

5. PROTECTION DES DONNÉES PERSONNELLES

5.1 Principes de protection des données personnelles

(Nom de la structure de la santé) et les membres de son personnel (y compris temporaire et intérimaire) observent constamment les principes de protection des données énoncés aux articles 11, 12, 14, 17, 24, 27, 28, 30, 39, 49, 47 (principe de traitement licite, loyal et transparent), aux articles 10, 11, 12, 47, 48, 49 (principe de limitation de la finalité), aux articles 11 et 33 (principe de minimisation des données), à l'article 11 (principe d'exactitude), à l'article 45 (principe de limitation de la conservation), aux articles 18, 19 et 37 (principe d'intégrité et de confidentialité) de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel. Ces principes exigent (en résumé) que les données personnelles soient :

· Traitées de manière licite, loyale et transparente (principe 1)
· Collectées pour des finalités déterminées, explicites et légitimes et non traitées ultérieurement d'une manière incompatible avec ces finalités (principe 2)
· Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe 3)
· Exactes et tenues à jour (principe 4)
· Conservées aussi longtemps, mais pas plus longtemps que nécessaire (principe 5)
· Dûment protégées contre les usages non autorisés, la perte ou la divulgation (principe 6)

5.2 Conformité – Principe 1 (traitement licite, loyal et transparent)

(Nom de la structure de la santé) met en place des procédures et des mesures visant à assurer la conformité au principe 1, dont les suivantes (liste non exhaustive) :

- Élaborer, pour tous les types de données traités, des notes sur la protection des données mises à la disposition des patients sur le site internet public de (la structure de santé), actualisées, mises à la disposition des personnes concernées et conformes aux exigences de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé, et de toute recommandation proposée par l'INPDP
- Nommer un délégué à la protection des données personnelles et mettre ses coordonnées à la disposition des personnes concernées
- Veiller à ce que la base juridique du traitement des données soit identifiée et citée dans les notes sur la confidentialité des données
- Lorsque le consentement de la personne intéressée est requis, veiller à ce qu'il soit donné librement et de manière spécifique, informée et non ambiguë et obtenu par une déclaration ou une affirmation claire et, dans le cas des catégories particulières de données, à ce que ce consentement soit explicite
- Veiller à ce qu'aucune donnée personnelle ne soit transmise ou divulguée informellement à un tiers. Les transmissions et divulgations doivent être contrôlées, dûment autorisées et prévues par la loi. Elles sont notifiées aux personnes concernées (si leur consentement n'a pas été recueilli) sauf si la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel prévoit une exception et s'il existe une raison valable et licite de l'appliquer

S'agissant de ses patients, dans la plupart des cas, (nom de la structure de santé) considère traiter les données personnelles dans l'exercice des fonctions de santé dont (il ou elle, en fonction de la structure) est investi(e), qui suppose qu'(il ou elle, en fonction de la structure) établisse de manière sécurisée un dossier exact, complet et à jour pour chacun de ses usagers, en vertu de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel.

Lorsque les dossiers des patients comportent des données de santé, leur traitement a généralement pour base juridique le consentement de la personne concernée à un tel traitement. Le traitement des données de santé peut aussi se fonder sur d'autres bases juridiques notamment la réalisation de finalités prévues par la loi ou les règlements, ou le développement et la protection de la santé publique entre autres pour la recherche sur les maladies, ou lorsqu'il s'avère que le traitement de ces données est bénéfique pour la santé de la personne concernée ou qu'il est nécessaire, à des fins préventives ou thérapeutiques, pour le suivi de son état de santé, ou lorsqu'il est effectué dans le cadre de la recherche scientifique dans le domaine de la santé. (Article 62 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel)

5.3 Conformité – Principe 2 (limitation de la finalité)

(nom de la structure de santé) met en place des procédures et des mesures visant à assurer la conformité au principe 2, dont les suivantes (liste non exhaustive) :

- Tenir un registre des équipements d'information. Y sont inscrits la base juridique du traitement des équipements et tout contrôle effectué sur les flux de données afférents, dont les communications d'informations et les modalités suivies
- Concernant les traitements de données de santé, réaliser des analyses d'impact sur la protection des données

5.4 Conformité – Principe 3 (minimisation des données)

(nom de la structure de santé) met en place des procédures et des mesures visant à assurer la conformité au principe 3, dont les suivantes (liste non exhaustive) :

- Réaliser des audits réguliers, dans le cadre des bonnes pratiques de gestion des données
- Veiller au respect des politiques et des directives professionnelles relatives aux dossiers, dont les normes pertinentes de tenue des dossiers cliniques
- S'assurer que tout traitement de données personnelles s'en tienne au minimum nécessaire pour que (la structure de santé) puisse remplir sa mission et ses objectifs, et que l'accès aux données personnelles soit réservé aux seules personnes qui en ont besoin pour leur travail
- Veiller à ce que, si possible sans ingérence dans le travail nécessaire de (la structure de santé) ni dans celui des tiers avec lesquels des données sont partagées ou auxquels des données sont divulguées, toutes les données personnelles soient anonymisées ou pseudonymisées avant d'être utilisées, partagées ou divulguées
- Consigner dans des registres les accords conclus avec des tiers sur le partage et le traitement des données. Ces accords sont conclus par écrit, répondent aux exigences de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et notamment ses articles 6, 20, 21, 22, 23, 24, 26 et imposent à tous les acteurs du traitement des données des responsabilités équivalentes à celles énoncées dans le présent code

5.5 Conformité – Principe 4 (exactitude)

(nom de la structure de santé) met en place des procédures et des mesures visant à assurer la conformité au principe 4, dont les suivantes (liste non exhaustive) :

- S'assurer que les services internes indiquent des informations exactes et prendre des mesures raisonnables pour vérifier l'exactitude des informations que (la structure de santé) reçoit des personnes concernées ou de toute autre personne
- Réaliser des audits réguliers, dans le cadre des bonnes pratiques de gestion de la qualité
- Offrir au personnel des orientations sur les bonnes pratiques de gestion des dossiers, comprenant des orientations sur les normes de tenue des dossiers cliniques
- Signaler aux personnes concernées qu'elles ont le droit de demander des rectifications et veiller à ce qu'il soit donné suite à leurs demandes en ce sens.

5.6 Conformité – Principe 5 (limitation de la conservation)

(nom de la structure de santé) met en place des procédures et des mesures visant à assurer la conformité au principe 5, dont les suivantes (liste non exhaustive) :

- Tenir et réviser régulièrement une politique de gestion des dossiers ou des politiques et procédures couvrant la création, la gestion et la suppression sécurisée des dossiers de (la structure de santé), du personnel et des patients
- Veiller à ce que les utilisateurs des données vérifient régulièrement les systèmes afin de supprimer les informations périmées ou inexactes
- Respecter le code de déontologie médicale en matière de gestion des dossiers.

5.7 Conformité – Principe 6 (intégrité et confidentialité)

(nom de la structure de santé) met en place des procédures et des mesures visant à assurer la conformité au principe 6, dont les suivantes (liste non exhaustive) :

- Tenir et réviser régulièrement une politique de sécurité informatique et des procédures afférentes
- Tenir et réviser régulièrement une politique et des procédures relatives à l'examen et à la gestion des atteintes, ou des soupçons d'atteintes, à la protection des données, à la confidentialité et/ou à la sécurité des informations
- Réaliser des analyses d'impact sur la protection des données chaque fois qu'un traitement des données de santé est mis en place et modifié
- Veiller à ce que les processus de (la structure de santé) intègrent la protection des données personnelles dès la conception et par défaut, en particulier à l'occasion de la commande de nouveaux équipements d'information et de la mise en place de nouvelles méthodes de traitement ou de nouvelles technologies
- Observer les normes de la loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique, et les recommandations de l'Agence nationale de la sécurité informatique (ANSI) en matière de gestion de la sécurité, y compris la cybersécurité
- S'assurer que tous les équipements d'information aient des propriétaires et des gestionnaires connus et que des évaluations des risques liés à ces équipements et aux flux d'informations associés soient entreprises et revues avec la régularité voulue
- Mener à bien un programme d'audit consacré à la protection, la sécurité et la confidentialité des données
- Veiller à ce que les membres du personnel disposent d'orientations et de formations appropriées sur les mesures qu'ils doivent prendre pour respecter le présent code
- Veiller à l'existence de procédures appropriées de sécurisation et d'envoi par télécopie pour la transmission des données personnelles
- Veiller à interdire les transferts de données de santé hors de la Tunisie. Toutefois, pour les transferts de données de santé vers l'étranger qui répondent à l'un des cas prévus par les textes en vigueur, veiller à ce qu'ils respectent les exigences et les formalités prévues : obtenir une autorisation de l'INPDP pour le transfert, et s'assurer que le pays destinataire garantisse un niveau de protection adéquat.

6. DROITS DES PERSONNES CONCERNÉES

Les personnes concernées ont accès à des procédures simples leur permettant d'exercer les droits énoncés ci-dessous. Ces procédures sont mises à leur disposition sur le site internet de (la structure de santé) qui s'attache à répondre aux demandes d'accès aux données personnelles dans le respect de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel. (nom de la structure de santé) observe les normes de ladite loi et la politique de conservation des données personnelles adoptée.

À l'attention de ses employés et des personnes qui interagissent avec lui/elle (selon le cas), (nom de la structure de santé) applique des procédures et des orientations adéquates pour veiller à ce que chacun puisse exercer ses droits en vertu de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé, notamment :

- Le droit à l'information sur le traitement de ses données personnelles conformément à l'article 31 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, sous forme de notes sur la confidentialité des données sur le site internet de (la structure de santé), dans les contrats et les brochures d'information, et via des explications dans les courriers lorsque nécessaire
- Le droit d'accès à ses données personnelles conformément aux articles 32 et 41 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
- Les droits de rectification, d'effacement et de limitation du traitement, en vertu des articles 32 et 37 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
- Le droit de s'opposer au traitement de ses données, conformément aux articles 42 et 43 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, et de limiter les décisions individuelles automatisées, en vertu de l'article 1er de la même loi.

7. CONFIDENTIALITÉ

7.1 Principes

(nom de la structure de santé) et son personnel respectent à tout moment le droit en matière de confidentialité, les exigences de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, dans la mesure où elles touchent aux obligations de confidentialité, selon lesquelles il convient que (la structure de santé) :

1. Justifie pour quelle(s) finalité(s) elle/il (en fonction du cas) utilise des données personnelles
2. Ne les utilise qu'en cas de stricte nécessité
3. N'en utilise que le minimum nécessaire
4. En réserve l'accès aux seules personnes autorisées
5. Veille à ce que chacun connaisse ses responsabilités
6. Veille à ce que chacun connaisse et respecte la loi

La structure de santé adhère aux principes énoncés dans le code de déontologie médicale.

7.2 Le secret professionnel médical

(nom de la structure de santé) respecte les règles relatives au secret professionnel médical telles qu'énoncées par le code de déontologie médicale et attend de tout son personnel qu'il fasse de même.

Règle n° 1 : respecter et garder secrètes les informations confidentielles relatives aux usagers ou aux patients

Tous les membres du personnel sont tenus de garder confidentielles les informations relatives aux patients et au personnel et de ne les transmettre qu'aux personnes qui ont besoin de les connaître pour leur travail. La discrétion est de mise, en particulier, dans les conversations téléphoniques et les communications électroniques.

Les informations confidentielles ne doivent pas être divulguées à des tiers sans discussion préalable avec un supérieur hiérarchique au sein de la structure de santé, qui doit approuver cette divulgation.

Les membres du personnel n'ont pas à consulter des informations, sous quelque forme que ce soit (électronique ou papier), concernant des amis ou des proches de patients ou de collègues (époux, enfants, parents, etc.).

Des clauses de confidentialité figurent dans les contrats de travail et d'embauche/les statuts (selon le cas). Une clause de confidentialité figure dans les contrats conclus avec des prestataires et fournisseurs extérieurs lorsqu'ils traitent des données personnelles.

Règle n° 2 : au sein des équipes soignantes, partager les informations confidentielles lorsque la sécurité et l'efficacité des soins l'exigent

Les modalités de partage des informations sont expliquées aux patients dans la note sur la confidentialité des données, et régulièrement abordées lors des contacts avec les patients lorsque le moment s'y prête. Le cas échéant, le consentement au partage des données peut être implicite aux fins d'une prise en charge directe.

Le partage de données dans le cadre d'un parcours de soins devrait rester pertinent, nécessaire et proportionné.

Dans certaines circonstances exceptionnelles exposées à l'article 7.4 du présent code, le partage de données personnelles sans consentement ne viole pas nécessairement l'obligation de confidentialité.

Règle n° 3 : anonymiser les informations divulguées dans l'intérêt de la communauté médicale

On entend par anonymisation, le traitement de données à caractère personnel d'une manière qui ne permet nullement d'identifier la personne concernée par le traitement.

Des informations anonymisées peuvent être divulguées dans l'intérêt de la communauté, notamment pour la recherche et la gestion des services de santé. (nom de la structure de santé) applique la norme d'anonymisation XXX ainsi que les recommandations de l'INPDP.

Les données personnelles ne peuvent servir à d'autres finalités que la prise en charge directe d'un patient, sauf dans les cas suivants :

- (la structure de santé) dispose d'un consentement explicite et pleinement éclairé autorisant d'autres fins
- Il existe une obligation légale (voir l'article 7.4 du présent code)
- La loi autorise cette divulgation pour une raison spécifique dans une situation où l'intérêt général l'emporte, comme la nécessité d'endiguer une épidémie, ou lorsque la réglementation et la législation l'autorisent

Règle n° 4 : respecter le droit de chacun à s'opposer au partage des informations confidentielles le concernant

Les patients qui s'opposent au partage de leurs données devraient se voir expliquer les conséquences probables de leur décision, mais s'ils persistent, leur objection doit être respectée, sauf circonstances exceptionnelles (voir l'article 7.4 du présent code pour des exemples). Les personnes concernées devraient bénéficier d'explications concernant ces circonstances.

Au moment d'examiner une opposition, (la structure de santé) tient compte des questions suivantes :

- Refuser l'opposition portera-t-il atteinte à l'efficacité des soins ?
- Refuser l'opposition entraîne-t-il un risque démontrable pour la sécurité du patient ?
- Existe-t-il des motifs impérieux et légitimes eu égard à la situation du patient ?

Règle n° 5 : pour les organisations, mettre en place des politiques, procédures et systèmes visant à assurer le respect des règles de confidentialité

Le présent code et les documents et procédures afférents sont conformes à la règle n° 5.

Conformément à la politique de gestion des incidents de (la structure de santé), le personnel doit signaler via un outil de signalement tout incident ou soupçon d'incident qui pourrait avoir porté atteinte à la sécurité ou à la confidentialité.

L'ensemble du personnel est tenu de signer un code de conduite en matière de confidentialité qui adopte ces règles. Les membres du personnel ne devraient pas accéder aux informations les concernant dans les dossiers de (la structure de santé), dont les registres sanitaires et relatifs aux employés, sauf s'ils participent directement à la prise en charge clinique du patient/client ou à l'administration des employés pour le compte de (la structure de santé).

(nom de la structure de santé) veille à ce que tout les destinataires avec lesquel elle partage des informations confidentielles s'engagent à respecter les règles de confidentialité.

7.3 Dossiers des patients

Lors de l'admission et/ou du premier contact avec le service pour une raison particulière, il convient de demander à tous les patients à quels proches, amis ou tuteurs ils souhaitent que soient adressées les informations relatives à leur traitement, en cas de besoin, et à quelles personnes spécifiques ils ne donnent pas l'autorisation de recevoir ces informations. Les réponses doivent être notées dans le dossier clinique.

Lorsque des proches ont été associés de près à la prise en charge d'un patient, il faut explicitement demander au patient jusqu'à quel point ces proches peuvent être tenus informés. C'est particulièrement important lorsque les proches demandent des informations sur l'état de santé du patient, parfois avant que le patient lui-même en ait été informé.

(nom de la structure santé) participe activement à des travaux de recherche. Par conséquent, son personnel peut étudier les dossiers des patients pour identifier, avec l'autorisation du consultant concerné, de potentiels participants à des recherches. Le personnel peut aussi discuter avec des patients de leur éventuelle participation à une étude spécifique, en vue de recueillir leur consentement.

Si un patient est incapable de consentir au partage ou à l'utilisation de ses données, il convient d'observer le cas échéant les règles du droit commun.

Les professionnels de santé devraient également adhérer aux orientations et aux normes de confidentialité publiées par leur organisme professionnel. Les principales références sont regroupées à l'article 9 du présent code.

7.4 Divulgation d'informations sans le consentement du patient

En certaines circonstances, il est possible que des informations personnelles doivent être divulguées sans le consentement du patient, voire en dépit de son opposition. En pareil cas, le personnel doit apprécier la nécessité de divulguer les informations et noter à qui et pour quelle raison elles ont été transmises. En cas de doute, il convient de solliciter l'avis de son chef d'équipe/clinicien sénior, du responsable de la gouvernance et de la sécurité de l'information.

Les exceptions au droit à la confidentialité sont rares. Elles s'appliquent par exemple :

- Lorsque la vie de la personne est en danger ou lorsqu'elle n'est pas capable de prendre une décision adéquate
- Lorsqu'il existe un danger grave pour d'autres personnes ou lorsque les droits d'autrui peuvent l'emporter sur ceux de la personne concernée, par exemple en cas de risque pour des enfants ou de graves abus de drogue
- Lorsqu'il existe une menace sérieuse pour les professionnels de santé ou d'autres membres du personnel

Au moment de décider d'une divulgation sans consentement pour des motifs extérieurs aux soins, (la structure de santé) vérifie le cadre juridique qui peut permettre d'effectuer cette divulgation. Dans les cas ci-dessous, la divulgation est prévue par la loi sans que le consentement soit nécessaire :

- naissances et décès (Loi XXX)
- maladies transmissibles à déclaration obligatoire (Loi XXX)
- empoisonnements et accidents graves sur le lieu de travail (…)
- maltraitance d'enfants
- toxicomanie
- accidents de la route
- prévention/détection de crimes graves, par ex. meurtres ou attentats
- violence à l'égard des femmes

(nom de la structure de santé) **soutient tout membre de son personnel qui, après un examen attentif et professionnel et après avoir sollicité l'avis de son supérieur, a choisi de divulguer ou de ne pas divulguer des données contre la volonté d'un patient, peut justifier sa décision et l'a dûment consignée.**

8. FORMATION

La formation aux questions de protection des données personnelles fait partie des procédures d'intégration du nouveau personnel et de la formation annuelle obligatoire de mise à jour sur la gouvernance de l'information, destinée à l'ensemble du personnel.

(nom de la structure de santé) analyse les besoins en formation et propose des formations pertinentes au personnel spécialisé, dont le responsable de la gouvernance et de la sécurité de l'information, l'équipe gouvernance de l'information et les personnes qui traitent les demandes d'accès.

9. SUIVI DE LA CONFORMITÉ

Les systèmes ou processus exposés dans ce document ont-ils été contrôlés conformément aux exigences nationales, régionales ou au niveau de (la structure de santé) ?	OUI/NON

Suivi : méthodologie et actions requises	**Fréquence**	**Autres mesures**
• Exigences de suivi énoncées dans la politique de (la structure de santé) sur la gouvernance de l'information	• Voir Politique de gouvernance de l'information	Voir Politique de gouvernance de l'information

10. RÉFÉRENCES

Bien qu'elle s'efforce de veiller à ce que les liens soient exacts, pertinents et à jour, (la structure de santé) décline toute responsabilité à l'égard des pages gérées par des personnes extérieures.

- Ordre national des médecins de Tunisie : http://www.ordre-medecins.org.tn/fr/
- Ministère de la femme, de la famille et des personnes âgées : http://www.femmes.gov.tn/ar/
- Ministère de la santé : http://www.santetunisie.rns.tn/fr/
- INPDP (Instance nationale de protection des données personnelles) : http://www.inpdp.nat.tn/

POLITIQUE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

(fiche technique concernant le Code de conduite et à adapter et compléter par la structure de santé)

PROFIL DU DOCUMENT	
RÉFÉRENCE	XXX
CATÉGORIE	Non clinique
VERSION	XXX
DÉPARTEMENT	Département responsable : Organisation centrale
SPÉCIALITÉ	Spécialité responsable : Gouvernance de l'information
À L'USAGE DE :	Structure de santé XXX
ASSURANCE QUALITÉ	Comité des dossiers médicaux et de la gouvernance de l'information
AUTEUR	Responsable du soutien à la gouvernance de l'information
DATE DE PARUTION	XXX
DATE DE RÉVISION	XXX
AUTRES ENTITÉS DEVANT APPROUVER CETTE POLITIQUE	N/A
DÉTAILS – DATE D'APPROBATION ET DE RATIFICATION	XXX
PERSONNES CONSULTÉES	Membres du Comité des dossiers médicaux et de la gouvernance de l'information de la structure de santé et de l'équipe de spécialistes du Comité
MODALITÉS DE DIFFUSION	Téléversé dans le Registre des codes de conduite, mise à jour mensuelle Le public peut demander un exemplaire de ce code, comme le prévoient le programme de publication de (la structure de santé) et les exigences de transparence en matière d'accès aux documents. Tout document portant sur la confidentialité devrait contenir un lien vers le document de politique sur la confidentialité
MOTS-CLÉS	Gouvernance de l'information, Protection des données personnelles, Confidentialité
DOCUMENTS AFFÉRENTS DE (LA STRUCTURE DE SANTÉ)	Note sur la confidentialité des données
	Politique de sécurité informatique
	Politique de gestion des dossiers, y compris les demandes d'accès
	Accidents, dont les accidents graves
	(Procédure disciplinaire)
	(Stratégie de gestion des risques)
	Procédure d'évaluation et d'enregistrement des risques)
	(Normes sur la tenue des dossiers cliniques)
NORMES ET/OU LÉGISLATION EXTERNES APPLICABLES	• Ministère de la Santé : http://www.santetunisie.rns.tn/fr/ (Confidentialité : code de déontologie médicale)
	• Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel
	• Conseil de l'Europe : Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
	• INPDP (Instance nationale de protection des données personnelles): Délibération n°4 du 5 septembre 2018 concernant le traitement des données à caractère personnel liées à la santé

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