INPDP

الهيئة الوطنية لحماية المعطيات الشخصية

INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES

NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

SENSIBILISATION À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL DANS LE SECTEUR DE LA SANTÉ

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

Programme de réalisation
Conseil de l'Europe et Union européenne :
Appui aux instances indépendantes en Tunisie (PAII-T)

Équipe du projet
Anne Boyer-Donnard, Ikram Ben-Sassi, Hela Rezouga

Rédaction
Anne-Christine Lacoste, Frédérique Lesaulnier,
Natalia Rusu, Sara Ben Fraj.

Comités techniques.
Le Projet tient à remercier chaleureusement les membres des Comités techniques pour leurs commentaires constructifs tout au long du développement de cette Boîte à Outils et pour le temps qu'ils y ont consacré : Dr. Amel Ben Said, Dr.Hend Bouacha, Dr. Slim Ben Salah, Dr. Noomene El Kadri, M. Bassem Kchaou et Mme. Leila Trojett

Conception graphique et impression
Impact
Tunis, 2021

Cette publication est produite avec le soutien de l'Union européenne et le Conseil de l'Europe dans le cadre du «Projet d'appui aux instances indépendantes en Tunisie». Ni l'Union européenne, ni le Conseil de l'Europe ne pourront être tenus responsables de l'usage qui pourrait être fait des informations qu'elle contient.

PRÉFACE

« Admis dans l'intimité des personnes, je tairai les secrets qui me seront confiés ».

Au cœur de l'engagement de tous les professionnels de santé résonne le serment d'Hippocrate, l'ancêtre exemplaire qui sera considéré comme tel dans le monde arabe à partir du Xe siècle.

Même si ce texte a été conçu pour les médecins et leurs collaborateurs, il est certain que ses engagements essentiels s'imposent à tout professionnel intervenant dans le secteur de la santé. Si pendant longtemps, ce principe n'a porté que sur la personne même du professionnel, l'évolution fulgurante des technologies, qui certes permettent des progrès à tous les niveaux, fait peser de nouveaux risques à la nécessaire confidentialité des informations relatives à la santé des personnes dans une ampleur encore jamais connue.

La protection des données personnelles est aujourd'hui au cœur des problématiques du monde moderne et s'agissant des données de santé, elle est encore plus cruciale.

L'actualité récente démontre tristement que les principes de la protection des données personnelles ne sont pas suffisamment appliqués et font porter des risques d'une gravité inégalée jusque-là.

Partout dans le monde, on recense des exemples de fuites, de pertes et de vols de données de santé. Bien sûr, beaucoup de pays comme la Tunisie, ont pris conscience de ces dangers et se dotent des législations et des structures pour y faire face.

Mais sans une prise de conscience collective de la nécessité de protéger ces données si sensibles et si indispensables, non seulement à la vie des personnes, mais également à leur autonomie, à la souveraineté des États et à la sécurité de la démocratie, les meilleurs textes juridiques seuls, sont bien souvent impuissants.

Le Conseil de l'Europe et l'Union européenne partagent ce souci. Ils travaillent à l'élaboration de normes et textes d'orientation dans ce domaine et joignent leurs forces à travers des programmes conjoints pour appuyer les États européens et leurs partenaires dans leurs efforts pour relever ces défis.

Une des missions des autorités chargées du contrôle de la protection des données personnelles est la sensibilisation des personnes et de la société en général à l'importance de protéger les données personnelles, l'information sur les moyens de le faire et les recours existants en cas de violation.

L'objectif de cette « Boîte à outils » de sensibilisation du secteur de la santé à la protection des données personnelles est d'aider les autorités de protection à créer et réhausser la prise de conscience de tous les intervenants du secteur de la santé et de mettre en œuvre un accompagnement qui leur permette d'acquérir une expertise supplémentaire en matière de protection des données personnelles.

Nous espérons que cette « Boîte à outils » , élaborée en collaboration avec l'Instance nationale de protection des données personnelles de Tunisie l'INPDP, atteindra son but et deviendra un outil incontournable.

Marcus Cornaro
Ambassadeur de l'Union européenne
en Tunisie

Christos Giakoumopoulos
Directeur général Droits de l'homme et État de droit
Conseil de l'Europe

Cette « Boîte à Outils » relative au secteur de la santé a pour objectif d'apporter aux professionnels et aux intervenants ainsi qu'aux patients des outils pour agir chacun suivant sa mission ou sa position dans une totale conformité aux normes de protection des données personelles.

Ces données sont sensibles et leur traitement peut constituer un danger pour la vie privée des individus, ce qui fait peser sur les professionnels des obligations encore plus lourdes que dans d'autres secteurs et explique le régime d'exception mis en place par le législateur tunisien qui, dans l'article 14 de la loi a interdit, par une déclaration de principe, le traitement de ces données. Il mettra en place les règles devant être respectées quand ces données à titre d'exception pourront être traitées.

La « Boîte à Outils » présente les principes fondamentaux à respecter, les bases juridiques applicables et offre des exemples d'outils – documents, sites web, brochures – qui peuvent servir de modèle ou d'inspiration aux acteurs de la santé pour développer leurs propres documents de sensibilisation et de mise en conformité de leurs traitement de ces données sensibles.

En guise d'introduction, il est nécessaire de commencer par définir les notions ou termes les plus utilisées à partir des textes juridiques en vigueur et plus spécialement la loi organique 2004-63 :

Données à caractère personnel, plus communément dénommées données personnelles : ce sont « 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 (article 4 de la loi) ». 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 (article 5 de la loi)».

Données à caractère personnel liées à la santé ou **Données de santé** : il s'agit des données personnelles sensibles relatives à des 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 résultant notamment de l'analyse d'un échantillon biologique de cette personne, ainsi que « la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne (article 4 § 15 du RGPD) ».

Traitement des données à caractère personnel : ce sont les opérations réalisées d'une façon automatisée ou manuelle, et qui ont pour but notamment la collecte des données personnelles, leur accès, leur enregistrement, leur sauvegarde, leur organisation, leur correction, leur exploitation, leur utilisation, leur envoi, 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 (article 6 §1 loi 2004-63). Il s'agit donc de toute action réalisée sur des données personnelles, et ce de leur collecte jusqu'à leur effacement.

Responsable de traitement : c'est toute personne physique ou morale, du secteur privé ou public, qui détermine la nature des données à traiter ainsi que la finalité et les modalités de leur traitement.

Personne concernée : toute personne physique dont les données personnelles font l'objet d'un traitement.

Bénéficiaire : toute personne physique ou morale recevant des données à caractère personnel.

Sous-traitant : toute personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement et sous sa supervision.

Délégué à la protection des données personnelles (DP²) : la personne chargée en interne de veiller au bon respect de la protection des données dans une structure publique ou privée et qui établit les liens avec l'INPDP et les personnes concernées par le traitement des données.

Instance nationale de protection des données personnelles (INPDP) : l'autorité chargée de la protection des données personnelles en Tunisie **www.inpdp.nat.tn**.

CONTEXTE

THÈMES IDENTIFIÉS

LES ACTEURS CONCERNÉS 1. Public 2. Privé 3. Formation 4. Autre

LA SITUATION EN TUNISIE

LES OUTILS EUROPÉENS / INTERNATIONAUX

THÉMES IDENTIFIÉS

- Formation des professionnels aux différents niveaux d'intervention (médecins, infirmiers, personnels administratifs…)
- Modules spécialisés dans les cursus de formation universitaire
- Actions de sensibilisation du public au sens large
- Guides méthodologiques thématiques (informatisation, télémédecine, partage de données …)
- Chartes institutionnelles
- Exemples de clauses contractuelles ou des contrats types (hébergement, …)
- Autres sujets évoqués :
  - Harmonisation et modernisation des textes règlementaires
  - Propriété des données médicales
  - Problèmes liés à l'accès à l'information
  - Cybersécurité face au développement du « ransomware » (hôpitaux)
- Suggestions / idées complémentaires :
  - Une rubrique FAQ sur le site de l'INPDP
  - Des « procédures simplifiées »

LES ACTEURS CONCERNÉS

1. Public

- Ministère de la santé
- Instance nationale en matière de santé
- Centres publics de recherche médicale
- Système national de sécurité sociale
- Hôpitaux publics

2. Privé

- Conseils régionaux et conseil national de l'ordre des médecins
- Conseil de l'ordre des pharmaciens
- Centres de dialyse, laboratoires de biologie et d'analyse, cabinets de radiologies, de soins dentaires, de soins de kinésithérapie...
- Laboratoires de recherche
- Assurances santé
- Hôpitaux privés

3. Structures de formation

- Facultés de médecine
- Instituts supérieurs dans le domaine de la santé

4. Autre

- Personnes
- Associations de protection des malades
- Association des droits de l'homme

LA SITUATION EN TUNISIE

La Tunisie est devenue en 2002 le 32e État à constitutionnaliser le droit à la protection des données à caractère personnel. Plusieurs textes législatifs ont été adoptés :

1. La loi organique n° 2004-63 du 27 juillet 2004 relative à la protection des données à caractère personnel, notamment ses articles 7, 10, 11, 14, 15 et 62 à 65.
2. La Loi n° 5-2004 du 3 février 2004 relative à la sécurité informatique.
3. En mai 2017, la Tunisie a ratifié la Convention 108 du Conseil de l'Europe.
4. Le 5 décembre 2018, l'Instance nationale de protection des données personnelles (INPDP) a adopté la délibération n°4 du 5 septembre 2018 concernant le traitement des données à caractère personnel liées à la santé, qui vise à renforcer et préciser les principes juridiques de la protection des données personnelles.
   Ce texte prend en considération les évolutions technologiques et soulève entre autres la question de l'internet des objets et plus particulièrement les dispositifs permettant de développer des pratiques médicales, tels que des applications liées au mode de vie et des systèmes de consultation et de surveillance personnalisés.
5. Une nouvelle loi organique de protection des données est actuellement en projet (à la date de publication).

Les principes essentiels de la loi organique n° 2004-63 et de la délibération n°4 relative au traitement des données de santé : ces principes exigent que les données personnelles soient :

- Traitées de manière licite, loyale et transparente (principe de licéité, loyauté et transparence)
- Collectées pour des finalités déterminées, explicites et légitimes et non traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation de la finalité)
- Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données)
- Exactes et tenues à jour (principe d'exactitude)
- Conservées aussi longtemps, mais pas plus longtemps que nécessaire (principe de limitation de la conservation)
- Dûment protégées contre les usages non autorisés, la perte ou la divulgation (principe d'intégrité et confidentialité)

Conditions de traitement des données de santé en vertu de la loi de 2004 et de la délibération de 2018 (pouvoir réglementaire de l'INPDP – art 76.3)

- Autorisation préalable de l'INPDP
- Charte éthique interne
- Finalité claire et légitime
- Minimisation de la collecte des données
- Information suffisante
- Consentement libre, explicite, éclairé et univoque et preuve du consentement
- Pseudonymisation ou anonymisation des données
- Sécurité des données
- Hébergeur agréé national
- Durée limitée de conservation
- Accès et portabilité des données
- DP2 (cf art. 15 délibération)

Note :
Mise en place en 2016 (horizon 2020) d'un programme de développement e-santé avec le soutien de l'Agence française de développement, en quatre axes :

(i) appui à la conception et à la mise en œuvre des projets prioritaires d'e-santé : Dossier médical informatisé (DMI), Distribution journalière informatisée et nominative du médicament (DJINM), Tunisie sans films, Archives médicales numérisées dans les hôpitaux et les Pôles de santé numérique

(ii) développement d'une approche territoriale de l'e-santé

(iii) appui à la numérisation des services de la CNAM

(iv) animation transversale d'une dynamique e-santé

LES OUTILS EUROPÉENS/INTERNATIONAUX

Recommandation CM/Rec(2019)2 du Comité des Ministres aux États membres en matière de protection des données relatives à la santé, Conseil de l'Europe	Recommandation (UE) 2019/243 du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés	Organisation mondiale de la santé, Cadres juridiques sur la confidentialité et la e-Santé, EN : https://www.who.int/goe/publications/legal_framework_web.pdf	Mandat du Rapporteur spécial des Nations Unies sur le droit à la vie privée - Groupe de travail sur la vie privée et la protection des données de santé : Projet de recommandation sur la protection et l'utilisation des données liées à la santé
https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168093b26b	https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019H0243&from=EN	https://www.who.int/goe/publications/legal_framework_web.pdf	https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf

PRESTATAIRES DE SOINS

MÉDECINS

HÔPITAUX PUBLICS ET PRIVÉS

PHARMACIENS

TÉLÉMÉDECINE

STRUCTURES DE FORMATION

MÉDECINS

1. Objectifs

Dans le contexte des soins de santé, la qualité de la relation médecin - patient est un élément essentiel à une prise en charge efficace. Il s'agit non seulement de respecter le cadre réglementaire mais de favoriser une relation de confiance entre le prestataire de soins et le patient, d'où l'importance de la sensibilisation des médecins à leurs obligations en termes de confidentialité et transparence vis-à-vis des patients et de protection des données sensibles dont ils sont dépositaires. L'accent est mis sur les risques spécifiques que le traitement de ce type de données peut occasionner aux personnes concernées (risques de discrimination, vulnérabilité du patient).

Les priorités suivantes sont identifiées comme formant partie intégrante d'un programme de sensibilisation :

• La clarification des principales obligations légales :

1. Limitation des informations collectées et gestion des dossiers conformément aux finalités définies (suivi des patients)
2. Conditions de collecte restrictives, en lien avec le caractère sensible des données
3. Registre à jour des « traitements des données», suppression de manière générale de toute information ayant dépassé la durée de conservation préconisée
4. Mesures appropriées de sécurité des dossiers « patients », y compris les conditions d'hébergement des données
5. Information des patients et respect de leurs droits

• La communication avec les patients sous forme électronique :
  - La prise de rendez-vous et les plateformes intermédiaires
  - La messagerie électronique
  - Les téléphones portables et tablettes
  - La télémédecine

• Le partage de données :
  - Le parcours coordonné de soins et le dossier médical partagé
  - La recherche

2. Public cible

Médecins (profession libérale), assistant(e)s de cabinet médical, ordre des médecins, patients.

3. Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Vulgariser les obligations légales à l'intention des professionnels des soins de santé, par des **documents courts**, simples et pratiques	Fiches thématiques sur les obligations légales (base légale, DP2, etc), la sécurité, le partage des données, les droits du patient, à destination des médecins et assistants médicaux	**Guide** de la CNIL et de l'Ordre national des médecins (FR) **Lignes directrices** de l'Association belge des syndicats médicaux (BE) Fiche de **sensibilisation** de l'Ordre national des médecins (FR)
Fournir un document standardisé de référence, plus développé, transposant la loi en obligations concrètes et apportant une valeur ajoutée en termes d'éthique, de dignité humaine et de relation avec le patient	Code de conduite de l'ordre des médecins / charte éthique Référentiels détaillés et guides expliquant les diverses obligations du prestataire de soins	**Guide** du CLUSIF concernant le traitement des données de santé (FR) **Référentiel** de la CNIL relatif au traitement de données à caractère personnel pour les cabinets médicaux et paramédicaux (FR) **Guide** pour le traitement des données personnelles dans le domaine médical (CH) The Royal College of Physicians of Ireland, **Code d'éthique sur la protection des données et pratique médicale** (IE)
Permettre aux patients de comprendre facilement leurs droits et les moyens de les exercer, par des documents courts et éventuellement imagés, adaptés au contexte et à leur situation (mineurs, handicapés, etc.)	Flyers, posters à destination des patients : relation directe avec le médecin, parcours coordonné de soins	**Guide** de la CNIL et de l'Ordre national des médecins (FR), **Guide** du parcours coordonné de soins sur le site du service public (FR)
Fournir un outil directement opérationnel (par exemple tableau, cases à cocher) permettant de guider les praticiens dans le respect de la loi	Check-list de conformité pour les soins de santé et les services sociaux	Fiche type d'un registre : **Guide** de la CNIL et de l'Ordre national des médecins (FR),

HÔPITAUX PUBLICS ET PRIVÉS

1. Objectifs

La sensibilisation du personnel hospitalier aux principes de protection des données est un enjeu majeur car, à la différence du médecin traitant, elle concerne des structures complexes impliquant une grande variété d'acteurs (médecins, infirmiers et autre personnel soignant, personnel administratif) et une plus grande circulation des données entre ces différents acteurs. Les hôpitaux sont également une cible vulnérable en ce qui concerne les attaques informatiques, ce qui nécessite des mesures de sécurité particulièrement strictes.

La sensibilisation a pour but de clarifier les principes suivants :

- Identification des finalité(s) de traitement des données et des données à collecter
- Analyse de la proportionnalité du traitement de données, le cas échéant analyse d'impact
- Transparence
- Mise en œuvre des droits des personnes concernées
- Responsabilisation (*accountability*), DP2
- Partage de données et transferts hors Tunisie (y compris la question du tourisme médical)

La sécurité des données fait l'objet d'une attention particulière :

- Gestion interne des données (mesures physiques, organisationnelles et informatiques)
- Conditions d'hébergement des données par un tiers

Trois questions spécifiques aux hôpitaux sont également abordées :

- La vidéo-surveillance dans les hôpitaux publics et privés
- Les interactions avec les médias: le conflit entre la confidentialité des données et le bien public ou l'intérêt général.
- La sensibilisation et l'information des patients sur les conditions de collecte et de traitement de leurs données et sur leurs droits.

2. Public cible

Médecins, infirmiers, autres personnels soignants, personnel administratif, patients/visiteurs, épidémiologistes, chercheurs.
Médias.
Police, autorités judiciaires (nécessité d'une requête spécifique).

3. Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Sensibiliser le personnel hospitalier au caractère sensible des données traitées et aux exigences de la loi en matière de protection de la vie privée des patients	Code de conduite interne, charte éthique, plans de formation, slides et fiches/guides à destination du personnel Notes de services internes	**Code de conduite** (FR) avec fiches pratiques pour les différents destinataires Exemple de **présentation interne** – hôpital St Luc, (BE) **Dépliant** à destination du personnel des Sherwood Forest Hospitals et **code** des Gloucestershire Hospitals (UK)
Clarifier pour le personnel en charge de la gestion des données les **obligations en matière de sécurité**	Guides détaillés sur la sécurité du réseau Cycles de formation pour le personnel concerné	**Guide ENISA** (EU) concernant la cyberdéfense dans les hôpitaux au niveau européen Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) avec **neuf guides pratiques** élaborés par le gouvernement (FR) • dispositifs connectés • accès Wifi (public et interne) • interventions à distance • destruction de données lors du transfert de matériels informatiques • règles de sauvegarde • plan de continuité informatique • accès web au SIS pour des tiers • mécanismes de protection de l'intégrité des données stockées • gestion des habilitations d'accès **Sécurité des systèmes d'information dans le secteur de l'imagerie médicale**, avis de l'Ordre des médecins (BE)
Fournir des précisions sur les exigences en cas **d'hébergement des données par un tiers** Note : l'hébergement se fait par le Centre informatique du Ministère de la santé (CIMS) pour le secteur public de la santé en Tunisie	Contrats types et référentiels en matière d'hébergement	Exemple de **certification** des hébergeurs de données de santé en France : **référentiel** incluant les exigences des normes ISO 27001, 27018, 20000, et du RGPD (FR)
Fournir des informations pratiques sur les conditions d'utilisation de la **vidéo-surveillance** dans la structure hospitalière	Fiche pratique sur la vidéo-surveillance Cycle de formation pour le personnel concerné	**Fiche technique** vidéo-surveillance dans les commerces (FR)
Clarifier les relations entre **l'hôpital et les médias**, et les conditions de communication de données de santé	Fiche d'information sur le site web d'un hôpital Guide détaillé des relations avec les médias	**Page web d'information** des hôpitaux de Toulouse, Angoulême et Strasbourg Guide de procédure détaillé, hôpital de Toulouse
Sensibilisation et information des patients quant aux conditions de collecte et de traitement de leurs données, ainsi que de leurs droits	Flyers/posters à destination des patients et des visiteurs Messages sur le site web de l'hôpital	Exemple d'information du patient dans le contexte hospitalier (FR), **Protection des données patients pour les établissements du GHT - Loire**

PHARMACIENS

1. Objectifs

Dans le cadre de leur activité professionnelle, les pharmaciens sont amenés à collecter des données sensibles concernant leurs clients. Les données de santé peuvent ainsi être utilisées pour différentes finalités :

- dans le cadre d'un dossier clients tenu par la pharmacie en interne (destiné à contacter les clients dans le cadre de leur traitement ou leur offrir des remises sur certains produits)
- dans le cadre d'un dossier pharmaceutique partagé, destiné à vérifier les interactions entre médicaments et éviter le cumul d'effets secondaires
- dans le cadre de l'intervention des assurances santé (publiques et privées).

On constate en outre l'émergence des e-pharmacies pour l'achat de produits pharmaceutiques, y compris ceux délivrés sur prescription, ce qui implique le traitement de plusieurs catégories de données à caractère personnel : sensibles, financières et d'identification. Le traitement de ces données de façon abusive peut s'avérer particulièrement dommageable pour les personnes concernées.

Par ailleurs, comme les hôpitaux, les pharmaciens utilisent parfois des systèmes de vidéo-surveillance qui sont soumis à une réglementation stricte.

L'objectif de cette section est de sensibiliser les pharmaciens aux conditions de traitement des données de leurs clients dans ces différents contextes, en mettant l'accent sur le caractère sensible des données traitées et les précautions à prendre lors de leur partage.

Principes essentiels :

- Les bases légales du traitement des données (en particulier pour les données sensibles, d'identification, financières, de géolocalisation, les préférences etc.)
- La transparence du traitement des données
- Le respect des droits de la personne concernée
- L'hébergement des données
- La sécurité du site internet
- Les conditions générales d'utilisation du web, en particulier pour la vente de médicaments en ligne (modalités et conditions d'utilisation des données, profilage du client, politique de confidentialité, politique de cookies, liens avec l'INPDP

2. Public cible

Pharmaciens, ordre des pharmaciens, clients de la pharmacie

3. Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Sensibilisation des pharmaciens aux conditions de collecte et de traitement des données du patient, à leur **partage** dans le cadre du dossier pharmaceutique et de l'assurance santé	Fiches thématiques à destination du pharmacien concernant les principes de protection des données de santé, la collecte et le partage des données (dossier médical partagé)	Le dossier pharmaceutique : **fiche pratique de la CNIL** (FR) Memo de l'assurance santé à destination des pharmaciens concernant le **dossier médical partagé** (FR)
Fournir au pharmacien des informations pratiques sur les conditions d'utilisation de la **vidéo-surveillance** dans l'officine	Fiche pratique sur la vidéo-surveillance	Fiche technique de la CNIL : **vidéo-surveillance dans les commerces** (FR)
Informer les patients des **conditions de traitement** de leurs données	Fiche pratique à destination des patients sur le dossier pharmaceutique	Information du patient sur le **dossier pharmaceutique** : page web de la fonction publique (FR)
Sensibilisation à la protection des données dans le cadre de la **vente de produits pharmaceutiques en ligne**	Fiche pratique à l'intention des responsables de traitement dans le cadre de la vente de médicaments en ligne	Fiche pratique de la CNIL : **vente en ligne** de médicaments (FR)
Permettre au responsable la **vérification concrète** du respect de la loi par un document d'utilisation aisée	Check-list de conformité	**Référentiel** de la CNIL sur les activités pharmaceutiques (FR)

TÉLÉMÉDECINE

1. Objectifs

La télémédecine met en rapport via les outils de communication électroniques les patients avec un ou plusieurs professionnels des soins de santé, dans le cadre d'une consultation ou d'un suivi médical. Elle implique le partage de données entre professionnels dans le cas de sollicitations d'avis à distance, et nécessite des précautions spécifiques afin de garantir la protection des données des patients.

Ces précautions concernent en particulier les conditions de partage des données entre professionnels, ainsi que la sécurité des données lors de l'accès à la plateforme (authentification), et du stockage des données (conditions d'hébergement).

L'objectif est de préciser les conditions de collecte, de partage et de stockage des données des patients, et d'informer les patients de leurs droits.

On note à ce propos que la Tunisie développe actuellement un programme de télémédecine en partenariat avec la France : la Société tunisienne de télémédecine et de l'e-santé (STTe) est en contact à cet effet avec la Société française de télémédecine (SFT-antel). Elle coordonne le développement du programme et assure la formation des acteurs médicaux.

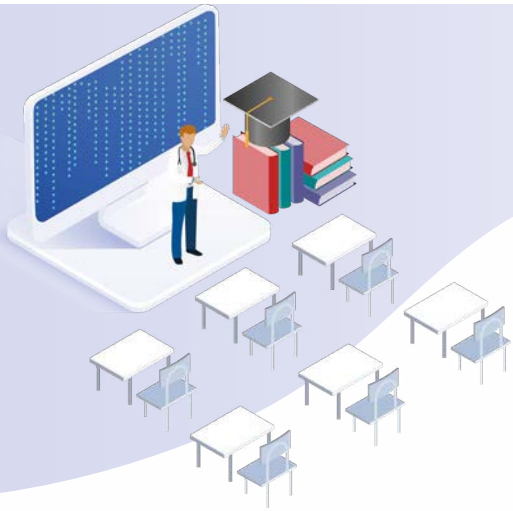
2. Public cible

Médecins, prestataires
de plateforme de télémédecine
Patients

3. Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Sensibilisation des praticiens aux précautions à prendre dans le cadre de la télémédecine, au contact des patients et des autres prestataires de soin	Fiches thématiques sur les conditions de collecte, le partage des données, les droits des personnes	**Fiche pratique** de la CNIL sur la télémédecine (FR) **Guide** de bonnes pratiques et fiche mémo de la Haute autorité de santé française (2019) sur la téléconsultation et la télé-expertise (FR)
Permettre aux prestataires de soin de **choisir un hébergeur** présentant les garanties requises en matière de protection des données des patients	Contrat type d'hébergement	Exemple de **certification** des hébergeurs de données de santé en France : **référentiel** incluant les exigences des normes ISO 27001, 27018, 20000, et du RGPD (FR)
Clarifier auprès des patients les conditions de traitement de leurs données et d'exercice de leurs droits	Document d'information à destination des patients	**Guide d'information** à destination du patient, de la Haute autorité de santé (FR)



STUCTURES DE FORMATION

1. Objectifs

Les actions de sensibilisation, loin de se limiter aux professionnels déjà actifs, devraient être développées en amont dans le cadre des formations universitaires et des autres structures menant aux professions liées aux soins de santé et à la recherche en santé humaine. Il peut s'agir de modules de longue durée ou de formations ou stages plus courts, en fonction des cursus. Sont en outre concernés le contexte de la relation médecin patient « traditionnelle », comme celle de l'e-santé et de la médecine connectée.

2. Public cible

Facultés de médecine et autres structures de formation : administration, professeurs et chargés de cours

Secteurs spécifiques : e-santé, pharmacie, infirmiers, autre personnel soignant, secrétariat médical

3. Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Fournir aux responsables de formation des références utiles dans le cadre de l'élaboration de **modules de sensibilisation au traitement des données des patients**	Modules de formation en protection des données / vie privée Exemples de supports de cours (structure de cours)	Formation de l'université Paris Descartes (FR) **Structure de cours** sur l'hébergement des données de santé (FR)

[1] Le printemps de la santé numérique en Tunisie, novembre 2017 http://www.telemedaction.org/422925659

PATIENTS

Objectifs

Informer les patients de la façon dont sont traitées leurs données est le corollaire indispensable à la sensibilisation des prestataires de soins de santé, afin de garantir une relation de confiance dans le cadre de la prestation de soin et un meilleur respect du cadre légal. Au-delà du respect de la loi, cette information vise aussi à préserver les fondements démocratiques, de liberté individuelle, de la dignité humaine, et de la protection de l'intimité des personnes.

L'objectif est de fournir l'information la plus complète mais aussi la plus claire possible, afin de permettre aux patients d'exercer leurs droits, de consentir le cas échéant au traitement de leurs données, d'avoir accès aux informations les concernant et éventuellement de s'opposer au traitement de leurs données.

Cette section répertorie l'ensemble des liens vers les procédures d'information mentionnées dans les autres sections, à savoir : la visite chez un praticien, dans un hôpital, la télémédecine, le dossier médical partagé, le dossier pharmaceutique et l'assurance maladie.

Public cible

Patients, famille/proches/visiteurs (hôpitaux), via les cabinets médicaux, hôpitaux et pharmacies et les procédures de gestion de soins de santé en ligne.

Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Responsabilisation des prestataires de soins, respect de la confidentialité des données Confiance des patients : rééquilibrer la relation médicale, assurer la confiance entre citoyens et professionnels Renforcer l'autonomie des patients, leur permettre d'exercer un contrôle sur leurs données Adaptation des documents informatifs en fonction de la condition des personnes, respect de leur vulnérabilité (enfants, personnes handicapées, malades graves)	Fiches d'information sur les droits à la protection des données : - visite chez le médecin - hospitalisation - dossier médical partagé - télémédecine - dossier pharmaceutique - assurance santé	**Sensibilisation des prestataires de santé** à l'information des patients : **fiche pratique** de la CNIL (FR) Information du patient dans le cadre d'une **consultation chez un médecin** : **Guide** de la CNIL et de l'Ordre national des médecins (FR), Information des patients sur la nature de leur **dossier médical et les conditions d'accès** à celui-ci (FR) : **page web** de la fonction publique et **fiche pratique** de la CNIL Exemple d'information du patient dans le **contexte hospitalier** (FR), **Protection des données patients pour les établissements du GHT - Loire** **Brochure d'information** de l'assurance santé sur le **dossier médical partagé** (FR) Information du patient sur le **dossier pharmaceutique**: page **web** de la fonction publique (FR) Guide d'information à destination du patient sur la **télémédecine**, de la Haute autorité de santé (FR) Information des **assurés** sur le fonctionnement de la **carte électronique** de **sécurité sociale** (FR) **Exemple d'information** des assurés sur le site de la caisse nationale de l'assurance maladie (FR) Exemple d'information des assurés par une **caisse d'assurance maladie pour indépendants** (FR) **Consultation** des patients (analyse d'impact) en matière d'e-santé (IE) Document informatif à destination des visiteurs du site web d'un cabinet médical (CH)

CAISSES D'ASSURANCE SANTÉ

Objectifs

En raison de la nature sensible des données qu'elles collectent, les caisses d'assurance maladie sont soumises à des réglementations strictes en matière de protection des données personnelles. L'objectif est d'encourager les bonnes pratiques de ces responsables de traitement dans leur activités quotidiennes. Au lieu de considérer leur rôle comme une simple tâche administrative, les entreprises devraient prendre en considération les risques qui sont similaires à ceux de tout autre secteur médical, auxquels il faut ajouter la quantité massive de données traitées.

Principes généraux en fonction des différents contextes de l'assurance maladie :

- **Uniformiser** au niveau national la réglementation sur la protection des données concernant les organismes publics et privés d'assurance maladie (règlementations internes, clause contractuelles, clause de confidentialité pour les employés, etc.)

- **Responsabiliser** les entités et favoriser la coopération avec l'INPD (identification du responsable de traitement, analyses d'impact, sécurité du bâtiment et des données, anonymisation et pseudonymisation, cryptage, tests d'intrusions, **mise en avant du principe de « *Privacy By Design***, instauration de régime de co-responsabilité des sous-traitants);

- **Renforcer les droits des personnes concernées** (validité du consentement, droit d'accès, droit d'opposition, droit à la portabilité, etc.).

- **Aborder les questions éthiques** et la légitimité des finalités du traitement des données (législations spécifiques : assurance obligatoire soins de santé et indemnités, sécurité sociale, droits du patient, etc.)

- **Traitement de catégories sensibles de données** : données d'identification, particularités financières, données physiques, données psychologiques, enregistrements d'images (via les caméras de surveillance), caractéristiques personnelles, profession et emploi, enregistrements sonores (via les appels à des centres d'appels)

- **Interopérabilité et partage de données avec d'autres responsables publics / privés :** données émanant du Registre national, données émanant de la sécurité sociale, données judiciaires : mesures judiciaires etc.

- **Communication** de données (sous-traitants et autres organismes publics), clause de **confidentialité** dans les contrats

Public cible

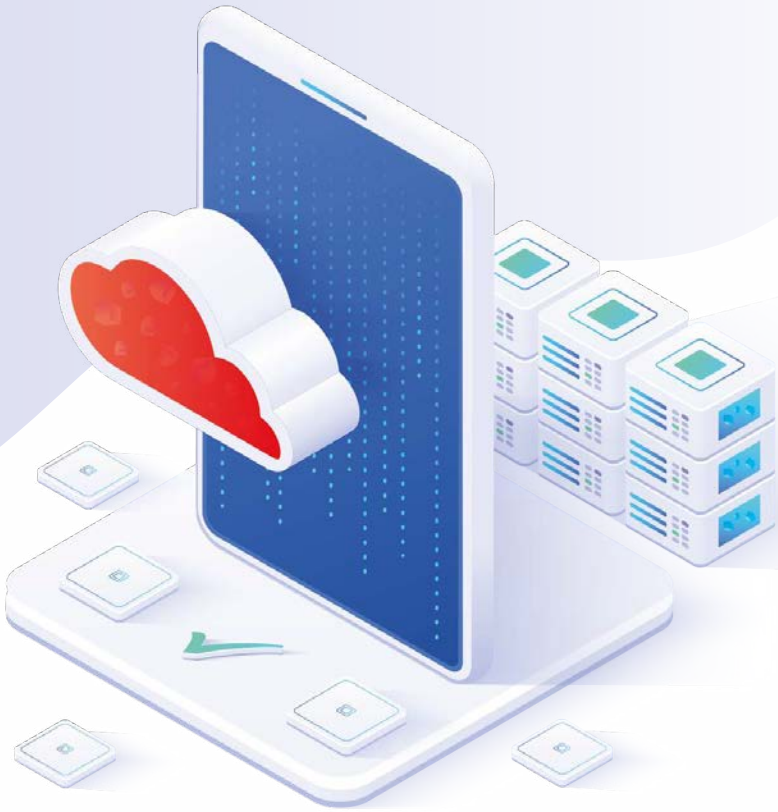
Les participants au processus : acteurs publics et privés de l'assurance maladie, Le Registre national, les employeurs et les hôpitaux, les pharmacies, les personnes visées.

Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Responsabilisation des acteurs publics et privés de l'assurance, au regard du caractère sensible des données traitées et des risques liés aux échanges de données	Sensibilisation des assureurs et mutuelles en matière de santé	Exemple de **sensibilisation** par un acteur privé (solutions de partage de données en ligne) dans le contexte du traitement de données de santé par les mutuelles (FR)
Les conditions d'utilisation de **la carte électronique de sécurité sociale** et/ou d'une application sur smartphone	Fiche d'information des assurés sur le traitement de leurs données via une carte électronique ou une application de sécurité sociale	Information des assurés sur le fonctionnement de la **carte électronique de sécurité sociale** (FR) Exemple d'utilisation d'une **application « sécurité sociale »** sur smartphone (expérimental) (FR)
Information des patients, clarification de leurs droits	Prospectus à destination des personnes dont les données sont traitées	**Exemple d'information** des assurés sur le site de la Caisse nationale de l'assurance maladie (FR) **Exemple d'information** des assurés par une caisse d'assurance maladie pour indépendants (FR)

STOCKAGE ET TRANSFERT DE DONNÉES DE SANTÉ



Objectifs

Avec le perfectionnement des technologies de l'information et de la communication, rares sont les traitements de données de santé limités à un dossier papier. Le dossier médical est aujourd'hui informatisé, que ce soit au niveau d'un cabinet médical, d'un hôpital ou d'un système plus global incluant la recherche. Combiné au développement de la télémédecine et du caractère de plus en plus international des prestations de soins, le traitement des données de santé soulève des questions quant au stockage (local ou via un hébergeur) et au transfert des informations.

Le but de cette section est de clarifier le cadre concernant la manipulation des données médicales :

- au niveau national – qu'il s'agisse des conditions de stockage ou de partage de données entre prestataires de soins en Tunisie,
- et lorsque le traitement présente des aspects internationaux - patients étrangers notamment, requérant la circulation de données médicales entre la Tunisie et un pays tiers. Ce dernier point soulève d'une part la question du niveau de protection dans le pays tiers, mais également de la reconnaissance par la Tunisie de la qualité du destinataire (prestataire de soins de santé) l'habilitant à traiter les données du patient.

Cette section regroupe les liens mentionnés par ailleurs dans ce document en ce qui concerne la gestion des données en Tunisie, et la complète pour les aspects internationaux.

Public cible

Prestataires de soins de santé : médecins et hôpitaux en particulier

Outils

Pour accéder aux liens hypertexte vers les outils, voir bibliographie.

Motifs	Outils	Références
Communication de données au niveau national : Apporter des précisions sur les garanties requises lors de la numérisation du dossier patient, l'archivage des données, leur sécurité, la question de leur stockage sur des serveurs nationaux	Guide pratique sur les conditions de stockage, la durée de conservation et les conditions de communication des données Partage de données entre professionnels en Tunisie. Cadre et référentiels Guide de la sécurité des systèmes d'information de santé	**Conservation** des données de santé : **référentiel** de la CNIL (FR) Exemple de **récapitulatif des durées de conservation**: «dossier du patient, évaluation et recommandations», *p. 44, anaes, 2003 (FR)* **Communication** de données de santé : **fiche pratique** de la CNIL (FR) **Fiche** (2016) et **rapport** (2017) de l'Ordre français des médecins sur le **partage d'informations** entre professionnels (FR) Exemple de **certification** des **hébergeurs de données** de santé en France : **référentiel** incluant les exigences des normes ISO 27001, 27018, 20000, et du RGPD (FR) **Guide ENISA** (EU) concernant la **cyberdéfense** dans les hôpitaux au niveau européen **Politique générale de sécurité** des systèmes d'information de santé (PGSSI-S) avec **neuf guides pratiques** (FR) **Sécurité des systèmes d'information dans le secteur de l'imagerie médicale**, avis de l'Ordre des médecins (BE)
Transferts internationaux de données, en particulier dossiers médicaux Prise en compte de la Convention 108+ du Conseil de l'Europe ou du RGPD en Tunisie	Fiche pratique sur les conditions de transfert de dossiers médicaux de la Tunisie vers un pays tiers Fiche d'information sur la possible application du droit d'un pays tiers à des traitements de données effectués en Tunisie	**Prise de position** de l'Association médicale mondiale sur le **tourisme médical**, point 13 sur les données de santé **Exemple de sensibilisation** des prestataires de soins à la possible application du droit européen à un pays hors UE (CH) **Lignes directrices** détaillées sur la gestion des dossiers patients / **transferts et interopérabilité** (UE)

BIBLIOGRAPHIE: RÉCAPITULATIF ET RÉFÉRENCES COMPLÉMENTAIRES

PRESTATAIRES DE SOINS

MÉDECINS
http://www.inpdp.nat.tn/liens_medecins.pdf

HÔPITAUX
http://www.inpdp.nat.tn/liens_structures.pdf

PHARMACIENS
http://www.inpdp.nat.tn/liens_pharmaciens.pdf

TÉLÉMÉDECINE
http://www.inpdp.nat.tn/liens_telemedecine.pdf

STRUCTURES DE FORMATION
http://www.inpdp.nat.tn/liens_formation.pdf

PATIENTS
http://www.inpdp.nat.tn/liens_patients.pdf

CAISSES D'ASSURANCE SANTÉ
http://www.inpdp.nat.tn/liens_assurance.pdf

STOCKAGE ET TRANSFERT DE DONNÉES MÉDICALES
http://www.inpdp.nat.tn/liens_stockage.pdf

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