INPDP
الهيئة الوطنية لحماية المعطيات الشخصية
INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES
NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

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

Séminaire de concertation des professionnels de la santé sur la protection des données personnelles

ARGUMENTAIRE

ATELIER DE CONCERTATION DES INTERVENANTS

AUTOUR DE LA PROTECTION DES DONNÉES PERSONNELLES DANS LE SECTEUR DE LA SANTÉ

POURQUOI UN ATELIER SUR LA PROTECTION DES DONNÉES PERSONNELLES DANS LE SECTEUR DE LA SANTÉ ?

Un enjeu au cœur de l'engagement des professionnels de santé

« *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 jusqu'au XIIIe siècle. Depuis, la matérialisation de ces principes dans un texte juridique date en Tunisie de 1973, avec la publication du premier Code de déontologie médicale et l'article 254 du code pénal tel que modifié par le décret du 25 avril 1940 sur la violation du secret médical.

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 fait peser des nouveaux risques à la nécessaire confidentialité des informations relatives à la santé des personnes.

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.

Des actions législatives fortes entreprises par la Tunisie

La Tunisie a pris la mesure de ces risques et est devenue en 2002, le 32ème État à constitutionnaliser le droit à la protection de la vie privée à travers celle plus spécifique des données personnelles.

Une série de textes législatifs ont suivi :

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 ;

La Loi n° 5 de 2004 du 3 février 2004 relative à la sécurité informatique ;

En mai 2017, la Tunisie a ratifié la Convention 108, premier texte international contraignant dans le domaine de la protection des données personnelles.

Enfin, le 5 décembre 2018, l'Instance nationale pour la protection de données personnelles (INPDP) a pris une délibération visant à renforcer et préciser les principes juridiques de la protection des données personnelles. Ce texte résolument moderne prend en considération l'avenir de la Santé en soulevant entre autres la question des IOT (Internet of Things – 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.

Malheureusement, ces initiatives fortes n'ont pas encore eu l'impact souhaité.

Les Risques

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.

Risques d'atteintes à la vie privée

Le développement de l'usage des nouvelles technologies a créé des risques inédits d'atteintes à la vie privée des personnes. Même si ces outils permettent des progrès à tous niveaux, les risques d'une perte de confidentialité sont plus forts que jamais.

Récemment, le rapport d'activité de l'INPDP mentionnait le cas d'un laboratoire pharmaceutique mettant en ligne des données de santé et notamment des bilans, sans mesures de sécurité appropriées.

La Tunisie est loin d'être un cas isolé ; des violations graves de données sont recensées partout dans le monde. En outre, les intérêts commerciaux des grandes sociétés du numérique font peser sur les données des risques à la hauteur de leur taille : l'objectif affiché de Google, par exemple, est d'exploiter des données collectées auprès de nombreux hôpitaux américains (résultats de laboratoires, données hospitalières, historique de santé des patients, etc.) pour alimenter des outils d'intelligence artificielle afin de créer des logiciels dédiés à la santé et de les vendre à d'autres hôpitaux.

Plus grave encore, les hackers sont devenus, ces dernières années, très friands de données de santé. Et si les vols augmentent, c'est que le butin se monnaie très cher sur le dark web. Les données de santé sont vendues, en moyenne, trois fois plus cher que des données « classiques », et elles permettent des escroqueries d'envergure.

Risques pour la santé même des personnes concernées

Ces scandales inacceptables ne doivent pas cacher d'autres situations encore plus graves qui mettent directement en danger la vie des patients.

Durant les dernières années, les hackers ont identifié que les hôpitaux et établissements de santé étaient particulièrement peu protégés contre les attaques informatiques et les ont ciblés de manière systématique afin d'obtenir des rançons.

Par exemple, le CHU de Rouen en France a fait l'objet d'une attaque sur des applications critiques, comme celles de l'accueil des patients et de la rédaction des prescriptions, et rendant impossible l'accès aux données. Pour enrayer la propagation de l'infection, tous les ordinateurs du CHU ont dû être arrêtés et le personnel en revenir pendant plusieurs jours « *à la bonne vieille méthode du papier et du crayon* ». Cela a entraîné en outre de nombreux retards dans plusieurs services, allant parfois jusqu'à plusieurs heures pour une prise en charge aux urgences. Il semblerait que le CHU ait été confronté à un piratage par ransomware, chiffrant les données en l'échange d'une rançon.

De multiples incidents ont été relevés en 2019, prouvant les trop faibles mesures de sécurité des hôpitaux. Comme exemples on peut citer des chercheurs qui ont réussi à créer un *malware* capable de truquer des scans de tumeurs cancéreuses, ou encore une faille au sein des appareils respiratoires et d'anesthésie fabriqués par General qui permettait alors de les contrôler à distance.

Renforcer sa sécurité informatique n'est plus une option, mais une nécessité de premier ordre.

L'ATELIER

Devant l'importance des risques et le constat d'une prise de conscience insuffisante des problématiques liées à la protection des données personnelles, l'INPDP a identifié la Santé comme un secteur prioritaire.

Objectifs

L'objectif de l'INPDP est de rehausser la prise de conscience de tous les intervenants du secteur de la Santé et de mettre en œuvre un accompagnement leur permettre d'acquérir une expertise supplémentaire en matière de protection des données personnelles.

Dans un premier temps, le projet implique un atelier est organisé pour :

- rappeler la problématique de la protection des données dans le domaine de la santé,
- mettre à niveau les connaissances sur le sujet,
- recueillir les besoins en matière de sensibilisation.

Nécessité de leaders inspirants

Dans une démarche de sensibilisation et de mise en conformité, rien n'est possible sans leaders qui acceptent de se saisir du sujet.

L'action de sensibilisation à la protection des données personnelles sera pour eux l'occasion de participer à la définition de la stratégie de sensibilisation que l'INPDP souhaite développer et des outils pratiques qui en découleront. Ils pourront ensuite les relayer à une plus grande échelle et assurer leur mise en œuvre pratique

Recueil des besoins

Une part essentielle de cet atelier est de permettre un échange entre les intervenants (INPDP et expertes) et les professionnels de santé souhaitant s'impliquer dans ce projet.

Au-delà d'un rôle de modèle, l'implication des participants permettra une réalisation efficace de l'atelier qui devra nécessairement prendre en considération les réalités de terrain. Il ne s'agit pas de calquer des solutions toutes faites mais bien d'identifier non seulement les spécificités du secteur de la Santé en Tunisie mais aussi de permettre aux participants d'exprimer leurs besoins.

MÉTHODOLOGIE DE L'ATELIER ET OUTILS PROPOSÉS

Au terme de l'atelier, les expertes seront dotées d'une meilleure connaissance des spécificités du secteur de la Santé en Tunisie et seront ainsi en mesure de proposer des outils d'accompagnement efficaces. Il fera donc une large place à l'expression des participants.

Des outils pratiques et adaptés

Les outils définis devront permettre une mise en œuvre de pratiques simples, d'un usage pratique et adaptés aux différents besoins, qu'ils soient individuels ou pour des structures d'importance variable. En effet, un médecin exerçant en individuel ne peut bien sûr pas se doter des mêmes outils informatiques qu'un hôpital d'envergure.

Ce point sera essentiel dans l'élaboration des outils proposés.

Formation et sensibilisation

Enfin, cet atelier sera l'occasion pour les professionnels participants d'être en priorité sensibilisés aux principes essentiels.

Une fois les outils développés, des actions de sensibilisation et de formation à grande échelle seront organisées, et ce à destination de l'ensemble des maillons du secteur de la Santé pour permettre une effectivité maximale des actions entreprises.

C'est la raison pour laquelle l'INPDP a souhaité inviter l'ensemble des professionnels ou organisations concernés par ce thème (universités, ordres, hôpitaux, cliniques, associations des malades, instituts de formation de personnel paramédical, assurances, institutions de recherches médicales, comités d'éthique, etc...).