Autorité de Protection des Données à caractère Personnel

Protéger les données personnelles au Bénin

Télémédecine et protection des données personnelles

FORMATRICE : Carolina TAMADAHO AÏTCHEOU
COMPLIANCE OFFICER/Juriste numérique
Email : contact@innovationcompliance.com
Site web: https//www.innovationcompliance.com

Octobre 2022

Introduction

La soixante et onzième Assemblée Mondiale de la santé a reconnu le 26 mai 2018, ***« le potentiel que recèlent les technologies numériques pour progresser sur la voie des objectifs du développement durable, en particulier pour soutenir les systèmes de santé de tous les pays pour la promotion de la santé et la prévention des maladies, et …….. «***

Quant à Madame Christine BALAGUÉ, vice-présidente du Conseil National du Numérique Française, elle a tenu les propos ci-après : ***« La santé vit ce que tous les secteurs vivent avec le numérique. Le numérique est notamment un formidable outil de prévention et il est sous-utilisé. Nous avons la capacité de tirer un très grand profit de ces technologies ; il faut trouver le moyen organisationnel de faire bouger les choses”.***

Ces propos illustrent bien les enjeux de la transformation digitale qui s’opèrent actuellement dans tous les secteurs, privés comme publics dans le monde.

Introduction

Depuis 2016, le Bénin a choisi de faire de la télémédecine un outil de réduction des inégalités d'accès aux soins. Un projet du PAG est dédié à cela.

D'ici l'horizon 2030, le Bénin vise à utiliser la télémédecine pour contribuer à réduire la mortalité maternelle, réduire les évacuations sanitaires et à faciliter un accès équitable aux soins.

L'atteinte de cet objectif suppose la levée de réelles difficultés notamment la mise en place de mesures tendant à éviter la violation des données à caractère personnel des patients.

Introduction

Par violation, il faut entendre “ la destruction, la perte définitive ou temporaire, l’altération, la divulgation non autorisée, l’accès non autorisé de données lors de traitement par les professionnels de santé.”

La question se pose alors de savoir comment les professionnels de la santé peuvent-ils écouter, examiner, conseiller ou soigner à distance et garantir en même temps la confidentialité des données sensibles des patients ?

Quelles mesures doivent-ils mettre en place pour assurer la protection des données sensibles de leurs clients?

Ce sont là autant d’interrogations qui trouveront réponses dans la présente présentation.

SOMMAIRE

OBJECTIF

- Permettre aux professionnels de la santé de maîtriser la notion de télémédecine et ses exigences au regard de la protection des données de santé
- Les obligations des intervenants professionnels de santé) dans la chaîne de traitement des données sensibles, les droits des patients
- Le niveau de sécurité exigée par la législation, dans le cadre d'une pratique médicale à distance, pour la protection des données personnelles

SOURCES ESSENTIELLES

- Loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin
- Loi n° 2020-35 du 06 janvier 2021 modifiant la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin
- Ordonnance 73-14 du 8 février 1973 instituant le code de déontologie médicale au Bénin impose le respect de la vie privée des patients et le secret professionnel au médecin
- Les résolutions de l'assemblée mondiale de la santé en date du 26 mai 2018 relative à la santé numérique :
- La stratégie globale de l'OMS sur la santé numérique 2020-2024 consultable ici : Global Strategy on Digital Health 2020-2024 (who.int)

SOURCES ESSENTIELLES

- Décret n°2020-281 du 20 mai 2020 fixant les conditions d'établissement et d'exploitation de réseaux et services de l'internet des objets en République du Bénin

  - Application : tout système composé d'équipements électroniques et/ou logiciels de traitement comportant des objets connectés et permettant de fournir des services

  - dispositif : tout équipement ou ensemble d'équipements doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données, de traitement de données et destinée à collecter des données et/ou contenus bruts.

SOURCES ESSENTIELLES

- Loi n°2020-37 du 03 février 2021 portant protection de la santé des personnes en République du Bénin
- Décret n°2020-078 du 19 février 2020 portant attributions, organisation et fonctionnement du ministère de la santé

  - consacrent la promotion de la télémédecine en son article 8
  - En france, les dispositions des articles L.6316-1 et R.6316-1 du code de la santé publique prévoient les conditions de mise en oeuvre et d'organisation de l'activité de la télémédecine

QU'EST-CE QUE LA TÉLÉMÉDECINE

- La télémédecine est une pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de la santé parmi lesquels figure nécessairement un professionnel de santé médical.

- Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, d'effectuer une surveillance de l'état des patients.

Télémédecine et protection des données des patients (sham.fr)

ACTES CONSTITUTIFS DE LA TÉLÉMÉDECINE

- constituent des actes de télémédecine :
  - la téléconsultation : consultation donnée à distance à un patient par un professionnel médical assisté, le cas échéant, d'autres professionnels
  - la téléexpertise : avis sollicité à distance par un professionnel médical auprès d'un ou de plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations liées à la prise en charge d'un patient
  - la télésurveillance médicale : interprétation à distance des données nécessaires au suivi médical d'un patient, et le cas échéant, prise de toutes les décisions nécessaires à la prise en charge de ce patient
  - la téléassistance médicale : assistance à distance réalisée par un professionnel médical au profit d'un autre professionnel de santé au cours de la réalisation d'un acte
  - Dans le cadre de la régulation médicale : la réponse médicale apportée au titre des services d'aide médicale urgente et de la permanence des soins ambulatoires

INCONVÉNIENTS ET AVANTAGES DE LA TÉLÉMÉDECINE

- INCONVÉNIENTS
  - logiiels inadaptés
  - erreurs de diagnostics en raison de limites techniques
  - Indisponibilité des données à un moment crucial
  - le défaut d'intégrité des données de santé

- AVANTAGES
  - Partage rapide et efficace des informations entre professionnels
  - communication des résultats d'analyse ou encore pour de simple renouvellement d'ordonnance
  - Absence de contrainte de déplacement en cohérence avec l'avènement du télétravail et la volonté de réduire les déplacements inutiles pour des raisons environnementales
  - Un meilleur suivi des patients notamment l'institution du DMP en France.

    Le Dossier Médical Partagé (DMP) est un carnet de santé numérique qui conserve et sécurise toutes les informations de santé du patient (traitements, résultats d'examens, allergies,)qui peut les partager avec les professionnels de santé de son choix.

    La télésurveillance et la téléassistance permettent par ailleurs aux professionnels de santé de mieux partager les informations et mieux se coordonner dans le traitement d'un patient, notamment ceux en ALD (Affection de Longue Durée)

ACTES CONSTITUTIFS DE LA TÉLÉMÉDECINE

L’état des lieux suivant a été fait :

- entre 2009 et 2011, une expérience de la coopération française dans 10 hôpitaux (téléconsultation, télé expertise médicale)
- en 2019, l’expérience de la coopération chinoise au CHD de Mono-Couffo (télé ECG)
- le protocole d’entente avec le gouvernement de l’Inde pour la mise en œuvre du projet eVRAB (télé enseignement, télé formation)
- de 2005 à ce jour, l’expérience de l'hôpital de Saint-Jean de Dieu de Tanguiéta (télé expertise, télé imagerie)

Ces diverses expériences visent la mutualisation des compétences entre les différents hôpitaux

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D'INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d'informations

La sécurité implique une organisation technique, humaine et procédurale qui vise à garantir la confidentialité, l'intégrité et la disponibilité de l'information.

Le code du numérique du Bénin soumet à une obligation de sécurité le médecin qui fait de la télémédecine.

Il lui impose de prendre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel des patients contre les risques d'atteinte à la confidentialité des données ou accès non autorisé aux données, à l'intégrité des données ou la modification non autorisée des données ou à la disponibilité des ou la perte des données.

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D'INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d'informations

La sécurité d'un système d'information s'articule autour des concepts ci-après :

- la pseudonymisation : les données faisant l'objet de pseudonymisation permettent de ne plus être attribuées à une personne concernée. Elle permet de remplacer un attribut d'un ensemble de données par des identifiants aléatoires susceptibles d'être lu grâce à une clé d'identification protégée.
- le chiffrement : procédé qui inclut l'usage d'algorithmes cryptographiques consistant à chiffrer les données qui ne seront lisibles que par une clé de chiffrement
- L'anonymisation : (art 33 CNB)
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D'INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d'informations

Dans le cadre de la télémédecine, les données personnelles devant faire l'objet d'échanges via réseaux et services internet interposés, les précautions élémentaires suivantes doivent être prises :

a. la sécurité physique des installations du système d'information

- Sécuriser les postes de travail : mécanisme de verrouillage automatique, installer un pare-feu, utiliser des antivirus régulièrement mis à jour, configurer des mis à jour de sécurité automatique, limiter la connexion de supports mobiles, recueillir l'accord de l'utilisateur pour toute assistance à distance
- Sécuriser l'informatique mobile : Sensibiliser les utilisateurs aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (ex : vol de matériel) et aux procédures prévues pour les limiter.
- Protéger le réseau informatique interne : Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D'INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d'informations

Dans le cadre de la télémédecine, les données personnelles devant faire l'objet d'échanges via réseaux et services internet interposés, les précautions élémentaires suivantes doivent être prises :

a. la sécurité physique des installations du système d'information

- ❖ Sécuriser les serveurs : La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données.
- ❖ Sécuriser les sites web : Tout site web doit garantir son identité et la confidentialité des informations transmises.
- ❖ Sauvegarder et prévoir la continuité d'activité : effectuer des sauvegardes fréquente des données, stocker les sauvegardes sur un site extérieur; rédiger un plan de reprise et de la continuité d'activité

a. La sécurité logique du système d'informations

- ❖ Encadrer la maintenance et la destruction des données : enregistrer les interventions dans une main courante, rédiger et mettre en oeuvre une procédure de suppression sécurisée des données, supprimer de façon

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. LA GARANTIE DE LA SÉCURITÉ DES DONNÉES DES PATIENTS

Dans le cadre de la télémédecine, les données personnelles devant faire l'objet d'échanges via réseaux et services internet interposés, les précautions élémentaires suivantes doivent être prises :

b. La sécurité logique du système d'informations

- Sécuriser les échanges avec d'autres organismes : chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur portable) et utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers; assurer la confidentialité des secrets
- Protéger les locaux : L'accès aux locaux doit être contrôlé pour éviter ou ralentir un accès direct, non autorisé, que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.
- Encadrer les développements informatiques : intégrer la protection de la vie privée, y compris ses exigences de sécurité des données, dès la conception de l'application ou du service; mener une réflexion sur les paramètre relatifs à la vie privée, pour tout développement à destination du grand public
- Chiffrer, garantir l'intégrité ou signer : Les **fonctions de hachage** permettent d'assurer **l'intégrité des données. Les signatures numériques,** en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité. Enfin, **le chiffrement,** parfois improprement appelé cryptage, permet de garantir **la confidentialité** d'un message.
- Archiver de manière sécurisée : définir un processus de gestion des archives, mettre en oeuvre des modalités d'accès spécifiques aux données archivées, choisir un mode opératoire garantissant que l'intégralité d'une archive a été détruit

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D'INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d'informations

c. la sensibilisation des utilisateurs aux contraintes de sécurité

- Sensibiliser les utilisateurs : sensibiliser les utilisateurs aux risques liés aux libertés et à la vie privée, documenter les procédures d'exploitations, rédiger une charte informatique et lui donner une force contraignante
- Authentifier les utilisateurs : s'assurer qu'un utilisateur accède uniquement aux données dont il a besoin en le dotant d'un identifiant propre et il doit s'authentifier avant toute utilisation des moyens informatiques
- Gérer les habilitations : définir des profils d'habilitation dans les systèmes en séparant les tâches et réaliser une revue annuelle des habilitations
- Tracer les accès et gérer les incidents : *Tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte* ***à la confidentialité, l'intégrité ou la disponibilité).***
- Gérer la sous-traitance : faire appel uniquement à des sous-traitants présentants des garanties suffisantes et documenter l'effectivité de ces garanties
- Évaluer le niveau de sécurité des données personnelles :

II. L’organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

A. LES MESURES LIÉES AU SYSTÈME D’INFORMATION DU RESPONSABLE DU TRAITEMENT

1. La sécurité des systèmes d’informations
2. La neutralité des systèmes d’information

La **neutralité du Net** ou la neutralité du réseau est un principe devant garantir **l'égalité de traitement de tous les flux de données sur Internet**.

Ce principe exclut par exemple toute discrimination positive ou négative à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau.

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. L'HÉBERGEMENT ET LA CONSERVATION DES DONNÉES CYBER SANTÉ

❖ QU'EST-CE QUE L'HÉBERGEMENT DES DONNÉES INFORMATIQUES

L'hébergement des données informatiques consiste en une mise à disposition d'un espace de stockage internet.

Classiquement, l'hébergement des données se fait sur disque dur et sur serveurs.

À une époque où le maître-mot est la digitalisation, les entreprises procèdent en masse à la numérisation de divers documents relatifs à plusieurs aspects de leur existence.

Relativement à la télémédecine, l'hébergement se réfère à la conservation des dossiers clients.

Au Bénin, la pratique est relativement récente.

En France, les dispositions de l'article R1112-7 du code de la santé publique prévoit " *Les informations concernant la santé des patients sont soit conservées **au sein des établissements de santé** qui les ont constituées, soit déposées par ces établissements **auprès d'un hébergeur** dans le respect des dispositions de l'article L. 1111-8. (France)*

II. L’organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. L'HÉBERGEMENT ET LA CONSERVATION DES DONNÉES CYBER SANTÉ

❖ QU’EST-CE QUE L'HÉBERGEMENT DES DONNÉES INFORMATIQUES

Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.”

Toute personne morale évoluant dans le domaine des Sciences de la Vie, doit ,en fonction de ses activités et des réglementations, recourir à **un hébergement « HDS »**. Cette contrainte métier a pour objectif principal de protéger les données de santé à caractère personnel traitées durant les activités.

L’objectif de cet hébergement est de protéger les données de santé. Ces données sont catégorisées comme étant des données « sensibles ». **Elles représentent une critique quant à leur gestion. Cela signifie que si des**

II. L’organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. L'HÉBERGEMENT ET LA CONSERVATION DES DONNÉES CYBER SANTÉ

❖ **QUID DE L'HÉBERGEMENT SUR LE CLOUD**

Le cloud computing fait partie des types d’hébergement les plus sollicités. Si vous vous intéressez à cette solution, vous aurez le choix entre le cloud public et le cloud privé.

Dans le premier cas, l’hébergement de vos données se fera dans des **data centers industriels** comme **GOOGLE, AMAZON, MICROSOFT et IBM.**

Dans le second cas, il sera effectué dans des serveurs répondant à vos

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. LA CONSERVATION DES DONNÉES CYBER SANTÉ

L'article 433 du code du numérique du Bénin prévoit que **la conservation des données personnelles**.

En France, la conservation de certaines données personnelles de santé est réglementée par les textes.

D'après l'article R. 1112-7 du Code de la santé publique, les dossiers médicaux doivent être conservés 20 ans à partir de la date de la dernière consultation.

Parallèlement, la commission nationale de l'informatique et des libertés (CNIL) a publié, le 28 juillet 2020 **des référentiels de durée de conservation des données personnelles de santé**. La CNIL a mis en place des référentiels non-contraignants. Ils ont uniquement pour but de guider les professionnels de santé à estimer le temps qu'ils doivent conserver les données de santé.

Les nouveaux référentiels adoptés par la CNIL le 28 juillet 2020 ont pour objectif d'aider les responsables de traitement concernés dans la gestion des traitements courants des cabinets médicaux et paramédicaux et dans le choix de durées de conservation.

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. L'HÉBERGEMENT ET LA CONSERVATION DES DONNÉES CYBER SANTÉ

Référentiel relatif aux traitements de données à caractère personnel destinées à la gestion des cabinets médicaux et paramédicaux (cnil.fr)

Selon le référentiel relatif aux traitements de données à caractère personnel destinées à la gestion des cabinets médicaux et paramédicaux, les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux peuvent être archivées.

C. COMMENT RÉAGIR APRÈS UNE DÉFAILLANCE INFORMATIQUE ?

A la survenance d'une défaillance informatique d'origine malveillance ou pas, conformément à l'Article 427 :

Le responsable du traitement ***doit notifier, sans délai, à l'Autorité et à la personne concernée toute rupture de la sécurité*** ayant affecté les données à caractère personnel de la personne concernée. *Le sous-traitant doit avertir*, sans délai, le responsable du traitement de toute rupture de la sécurité ayant affecté les données à caractère personnel qu'il traite pour le compte et ou nom du responsable du traitement. La notification visée à Alinéa 1er doit, à tout le moins :

- Décrire ***la nature de la rupture de sécurité*** ayant affecté des données à caractère personnel y compris, si possible, ***les catégories et le nombre approximatif de personnes concernées par la rupture*** et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues

II. L'organisation de la confidentialité nécessaire à la protection de la vie privée et la protection des données sensibles de santé

B. L'HÉBERGEMENT ET LA CONSERVATION DES DONNÉES CYBER SANTÉ

C. COMMENT RÉAGIR APRÈS UNE DÉFAILLANCE INFORMATIQUE ?

- Décrire ***les conséquences probables de la rupture de sécurité***
- ***L***a rupture de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives' La communication à la personne concernée visée à l'alinéa 1er n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :
  - le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite rupture, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement
  - le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé a Alinéa 1er n'est plus susceptible de se matérialiser
  - elle exigerait des efforts disproportionnés. Dans ce cos, il est plutôt procédé à une communication publique ou a une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT
B. LA PROTECTION CONTRE L'ACCÈS AU DOSSIER MÉDICAL
    1. le secret médical du professionnel de la santé
    2. Le respect des droits des patients
        - ❖ Particularité du patient en situation de vulnérabilité et de détresse morale

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT

1. L'information préalable de la personne concernée :

L'information du patient est un principe fondamental défini dans le code du numérique du Bénin et le code de déontologie médicale.

Mais que dire au patient et comment ?

- **Le contenu de l'information délivrée au patient**

Selon l'article 35 du code de déontologie médicale (article R.4127-35 du code de la santé publique français), "***le médecin doit à la personne qu'il examine, qu'il soigne ou qu'il conseille une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il lui propose. Tout au long de la maladie, il tient compte de la personnalité du patient dans ses explications et veille à leur compréhension."***

Toute personne a le droit d'être informée sur son état de santé, dit la loi (article L1111-2 du code de la santé publique)

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT

1. L'information préalable de la personne concernée :

L'information que vous devez délivrer au patient doit lui permettre de décider en connaissance de cause. Elle doit être aussi détaillée que possible et doit porter sur :

- **l**es différentes investigations, traitements ou les actions de prévention préconisés ;
- leur utilité et leur urgence éventuelle ;
- leurs conséquences ;
- les risques fréquents ou graves normalement prévisibles qu'ils comportent ;
- les autres solutions possibles ;
- les conséquences prévisibles en cas de refus ..

Le droit du patient à l'information s'exerce avant tout acte médical, de soins, d'investigation ou de prévention. Si, postérieurement, des risques nouveaux sont identifiés, le patient doit en être informé (sauf s'il est impossible de le retrouver).

Lorsque plusieurs professionnels de santé interviennent, chacun informe le patient des éléments **relevant de son domaine de compétences** en les situant dans la démarche globale de soin.

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A L'INFORMATION PRÉALABLE ET LE CONSENTEMENT

1. L'information préalable de la personne concernée :

- **Comment informer le patient ?**

Cette information doit être claire, loyale et appropriée, précise l'article 35 du code de déontologie médicale. Les qualités de l'information : elle doit être **synthétique, hiérarchisée, compréhensible et personnalisée**. Elle doit présenter les **alternatives possibles**, les bénéfices attendus ainsi que leurs inconvénients et les **risques éventuels**.

La délivrance de l'information se fait dans le cadre d'un **entretien individuel**. Celui-ci doit permettre un dialogue avec le patient. Cela nécessite un environnement adapté, du temps, de la **disponibilité et du tact de la part du médecin**. L'information peut être délivrée de manière progressive s'il y a lieu.

L'information, qui est toujours orale, est primordiale. En complément de cette information, un document écrit peut être remis au patient pour lui permettre de s'y reporter. Ce document d'information a pour seul objet de donner au patient des renseignements écrits et n'a pas à être signé par le patient.

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT

2. Recueillir le consentement du patient

Le consentement doit être "libre et éclairé". Cela signifie qu'il ne doit **pas être obtenu sous la contrainte**.

Le patient doit donner son consentement après avoir reçu préalablement du médecin une information claire, complète, compréhensible et appropriée à sa situation.

L'article 36 du code de déontologie médicale (article R.4127-36 du code de la santé publique français) et ses commentaires définissent précisément les modalités de recueil du consentement du patient. "*Les actes médicaux justifiant ce consentement doivent être entendus au sens large :* ***en commençant par l'examen clinique habituel dont certains gestes peuvent être désagréables, comprenant d'éventuelles investigations complémentaires, différents traitements, la surveillance du traitement et de ses suites ;*** *le consentement du patient porte également sur sa participation éventuelle à la formation d'étudiants ou de professionnels de santé* (article L.1111-4, 8ème alinéa du code de la santé publique).

Le fait d'intervenir sur un patient contre son consentement est pour un médecin une faute qui engage sa responsabilité civile et l'expose à une sanction disciplinaire.".

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE
B. LA PROTECTION CONTRE L'ACCÈS AU DOSSIER MÉDICAL

1. Le serment d'Hippocrate est considéré comme l'un des textes fondateurs de la déontologie médicale (ordonnance n°73-14).

Le secret médical des professionnels de la santé est un des outils qui contribue à la protection contre l'accès au dossier médical. Avec stratégie de transformation du système de santé, beaucoup de questions se posent sur l**a portée réelle** de cette règle déontologique.

medecins_ns_-_serment.pdf (conseil-national.medecin.fr)

medecins_ns_-_serment.pdf (conseil-national.medecin.fr)

En France par exemple, le comité consultatif national d'éthique pour les sciences de la vie et de la santé est chargé de donner des avis sur les problèmes éthiques et les questions de société soulevées par les progrès de la connaissance dans les domaines de la biologie, de la médecine et de la santé.

Dans de nombreux hôpitaux, des espaces éthiques contribuent à faire vivre la réflexion sur les principes fondamentaux de l'éthique médicale et à interroger son évolution au regard des nouvelles pratiques médicales et des innovations technologiques. Voir notamment le site de l'espace éthique de l'Assistance Publique des Hôpitaux de Paris.

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT
B. LA PROTECTION CONTRE L'ACCÈS AU DOSSIER MÉDICAL

2. Le respect des droits des patients

- le droit d'accès (article 437 CNB)
- le droit de rectification (article 441 CNB)
- le droit d'opposition (article 440 CNB)
- le droit à l'effacement (article 437 CNB)
- le droit à l'oubli (article 443 CNB)
- le droit d'interrogation (article 439 CNB)
- le droit à la portabilité des données (article 438 CNB)
- le droit d'opposition au profilage à des fins de prospection (article 437 CNB)

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE ET DES DONNEES A CARACTERE PERSONNEL DANS LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT
B. LA PROTECTION CONTRE L'ACCÈS AU DOSSIER MÉDICAL

2. Le respect des droits des patients (suite)

- le droit à l'oubli (article 443 CNB)
- le droit d'opposition au profilage à des fins de prospection
- le droit d'introduire une réclamation auprès de l'autorité (article 448 CNB)
- Le droit à un recours juridictionnel effectif contre l'autorité
- le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant (article 450 CNB)
- le droit à réparation et à responsabilité (article 451 CNB)

III. LA GARANTIE DE LA PROTECTION DE LA VIE PRIVÉE DANS LA PRATIQUE DE LA TÉLÉMÉDECINE

A. L'INFORMATION PRÉALABLE ET LE CONSENTEMENT
B. LA PROTECTION CONTRE L'ACCÈS AU DOSSIER MÉDICAL
   - ❖ Patient en situation de vulnérabilité et de détresse morale

La protection du patient en situation de vulnérabilité passe d'abord par les droits qui lui sont reconnus par le code numérique du Bénin.

Plus spécifiquement, en France tout le monde n'accède pas de façon équitable au système de santé. Isolement, précarité, complexité des démarches ou mauvaise maîtrise de la langue sont autant de barrières qui compliquent l'accès aux soins. Reconnus par la loi de modernisation du système de santé, **la médiation et l'interprétariat sont deux moyens permettant de réduire ces inégalités en santé**. Dans ce contexte, la Haute Autorité de Santé (HAS) a publié deux référentiels qui en précisent le cadre d'intervention et les bonnes pratiques.

IV. CONCLUSION

Les nouvelles pratiques et les nouvelles technologies utilisées dans la santé permettent de générer de plus en plus de données qui transitent en ligne.

Cela représente un attrait, notamment pour les personnes malveillantes. En effet, les données de santé sont très valorisées par les hackeurs (revente, divulgation, rançon…) .

Par exemple, le 22 août 2022, un hôpital du département de l'Essonne en FRANCE a subi une cyberattaque par un groupe de hackers. Ces derniers ont commencé à diffuser des données piratées de près de 1,5 million de personnes, patients ou agents de l'hôpital.

IV. CONCLUSION

Le secteur de la santé compte parmi les secteurs les plus touchés par des attaques malveillantes. De plus en plus, nous entendons parler d'attaques et de compromission des données détenues par les organismes de santé.

En conséquence, les professionnels de la santé doivent mettre en œuvre les dispositifs prévus par le législateur pour éviter la perte, le vol ou l'altération des données afin de créer les conditions d'une protection efficace de la vie privée et des données sensibles de leurs patients.

Avec le code du numérique du Bénin, toute fuite ou altération de données engage la responsabilité du responsable du traitement et peut donner lieu à des sanctions et poursuites judiciaires.

L'Autorité de Protection des Données à caractère personnel est l'autorité administrative indépendante compétente pour garantir cette protection et dont l'autorisation préalable doit être sollicitée avant tout traitement de données de santé, de données sensibles.

IV. CONCLUSION

Par ailleurs, nous recommandons à l'Etat d'encourager l'usage approprié des technologies numériques pour la santé pour un meilleur suivi des patients et pour combler le vide des déserts médicaux.

JE VOUS REMERCIE