LA CONFIDENTIALITE DES DONNEES

TEC en COREVIH

Lyon – 18 et 19 juin 2015

« Admis dans l'intérieur des maisons, mes yeux ne verront pas ce qui s'y passe, ma langue taira les secrets qui lui seront confiés »

Hippocrate

COLLECTE DE DONNÉES DE SANTÉ

- Le principe est dicté par l'article 8 de la loi Informatique et Libertés :

  Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci

  Attention : Fichier Informatique ET Papier concernés

SAUF :

Consentement express de la personne, intérêt public, sauvegarde humaine…

(Alinéas 2 et 3 de l'art 8 de la Loi I&L)

CONFIDENTIALITE

La confidentialité des données médicales est régie par l'Article L1110-4 du Code de la santé publique, créé par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

CONFIDENTIALITE

Le secret médical

« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations le concernant.

Excepté dans les cas de dérogations expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne, venue à la connaissance du professionnel de santé, de tout membre du personnel de ses établissements ou organismes et de toutes autres personnes en relation, de part ses activités, avec ces établissements et organismes.

Il s'impose à tous les professionnels de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé (…) »

CONFIDENTIALITE

Le secret médical partagé

« Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible.

Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe »

CONFIDENTIALITE

Manquement au secret médical

Article 226-13 du Code Pénal : la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire

Article L 1110-4 CSP : : le fait d'obtenir ou de tenter d'obtenir des informations médicales en violation du droit au respect du secret

1 an d'emprisonnement et 15 000 € d'amende

CONFIDENTIALITE

Révélations autorisées du secret médical :

Lorsqu'une personne ou un médecin dans le cadre de sa exercice, informe les autorités de cas de mutilations ou de sévices, dont il a eu connaissance et qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger ;

Aux professionnels de la santé ou de l'action sociale qui informent le préfet de police du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une.

Dérogations obligatoires (entre autres) :

Les maladies contagieuses à déclaration obligatoire (art. L3113-1 CSP)

CONFIDENTIALITE

« En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part.

Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations. »

« Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. »

CONFIDENTIALITE ET SECURITE

Confidentialité et sécurité sont 2 notions liées.

Le responsable du traitement, est astreint à une obligation de sécurité. Il doit faire prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation :

- Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions (Gestion des habilitations)

- Le responsable du traitement doit prendre toutes mesures pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès. S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées.

- Les mesures de sécurité, tant physique que logique, doivent être prises. (par ex : Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe d'un minimum de 10 caractères.)

SECURITE DES FICHIERS

La sécurité des fichiers

- Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement.
- Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende.

MESURES INFORMATIQUES APPLICABLES

LOGICIELS

- Les applications doivent également être protégées par un mot de passe individuel, précédé d'un nom d'utilisateur unique
- Accès autorisé uniquement aux personnes qui y ont légitimement accès, dans le cadre de leur mission (profils d'habilitations). Droits d'accès décidés par le supérieur hiérarchique.

MOT DE PASSE

- Le mot de passe
  - Ne doit pas contenir de mot du dictionnaire, de nom propre, d'info personnelle (ex : date de naissance)
  - Ne doit pas être devinable
  - Doit contenir des chiffres, des lettres en minuscule et en majuscule, au moins un caractère spécial (&, %, *, $,…..)
  - Au moins 8 caractères
  - Renouvelé tous les 3 mois
  - Différent des 3 derniers
  - Ne doit pas être transmis, même à son/sa meilleure ami(e), ne doit pas être écrit
  - Ne doit pas être créé par quelqu'un d'autre que vous
  - Faire en sorte que le mot de passe ne soit pas mémorisé par les logiciels (ex : Navigateur internet)

MOT DE PASSE

- Construire un mot de passe et le retenir :

  Utiliser une proverbe, une phrase favorite, un vers de poésie, que vous retiendrez facilement

  Ex : Un Esprit Saint Dans Un Corps Saint !

  La première lettre de chaque mot + le caractère spécial donne : UeSdUcS!

  Ajoutez un incrément, cela donne : UeSdUcS!01

  Il ne vous reste qu'à changer l'incrément tous les 3 mois !

POSTE DE TRAVAIL

- Votre poste de travail doit être sécurisé
  - Verrouillage automatique au bout de 10 minutes maximum
  - Verrouillage manuel dès que vous quittez votre poste
  - Postes très sensibles : Désactiver ports USB
  - Utiliser un Antivirus
  - Effectuez régulièrement des sauvegardes sur des supports externes et conservez les dans un autre local, idéalement, dans un coffre ignifugé

POSTE DE TRAVAIL

Votre ordinateur doit être protégé au démarrage, par un mot de passe individuel

RESEAU

- En cas de connexion à Internet, prévoir des mesures de sécurités particulières comme la séparation physique des deux réseaux, la mise en place d'un firewall ou de barrières de protection logicielles.
- Lorsque des données de santé sont transférées via Internet, il convient de recourir au chiffrement de la communication

LOCAUX

- Les salles où sont hébergées les serveurs doivent faire l'objet d'une sécurisation accrue: Habilitations, fermeture à clé ou digicode, badge…

VIS-A-VIS DES PRESTATAIRES

- Le professionnel ou l'établissement de santé peut décider d'externaliser une partie du traitement des données des patients. Dans ce cas, le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité telles que prévues par la loi.

- En cas d'hébergement par un tiers, le professionnel ou l'établissement de santé devra s'assurer que le prestataire met en œuvre des mesures de sécurité suffisantes, et qu'il est agréé par le ministère

- Si intervention d'un prestataire sur une base de données, quelqu'un doit être présent à ses côtés. L'intervention doit également être consignée dans un registre.

TRANSFERT DE DONNEES

TOUT TRANSFERT DE DONNEES PAR UN CANAL NON SECURISE NE DOIT PAS AVOIR LIEU…

TRANSFERT DE DONNEES

- Dans l'intérêt direct du patient (assurer son suivi médical, faciliter sa prise en charge par l’assurance maladie obligatoire…) ou pour les besoins de la santé publique, des transferts peuvent être nécessaires par :
  - Transfert par support externe
  - Transfert par email
  - Surtout pas par messagerie instantanée

SUPPOTS EXTERNES

- Il s’agit des clés USB, des ordinateurs portables, des tablettes/smartphones

- Si des données sensibles doivent y être enregistrées, les fichiers les contenant doivent être chiffrés

CHIFFREMENT

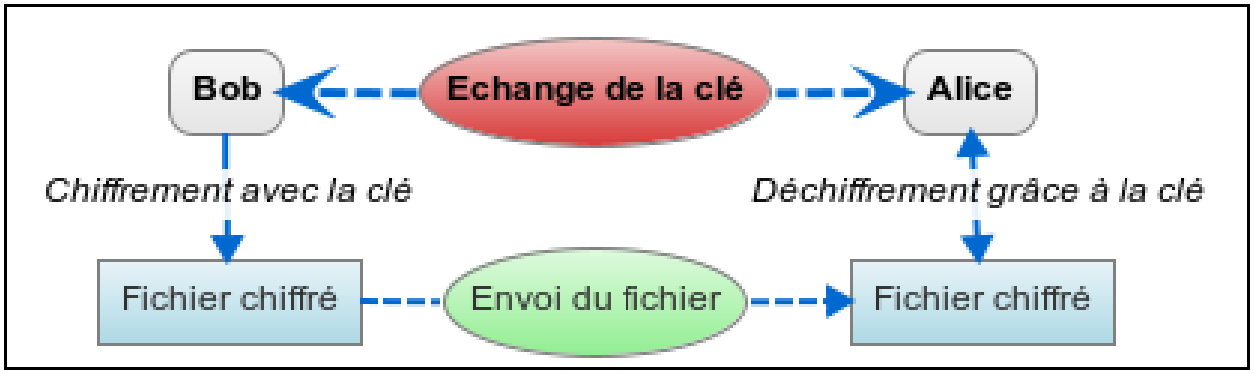
- Chiffrer, c’est rendre la lecture d’un fichier impossible à toute personne ne possédant pas la clé de déchiffrement.

- Plusieurs logiciels existent : AXCrypt, Veracrypt (remplaçant de TrueCrypt)

AXCrypt

- Permet de chiffrer un fichier / un dossier
- Gratuit et sûr
- Utilisation d'un fichier contenant une clé (plus sécurisé) et/ou d'un mot de passe
- Le fichier clé, créé séparément, est lié au fichier chiffré au moment du chiffrement.
- Lors du déchiffrement, il vous faudra bien sûr le mot de passe et le fichier clé, afin d'ouvrir l'original.
- Ne stockez pas le fichier clé et le fichier chiffré au même endroit.
- Possibilité de créer un exécutable : Le destinataire n'est pas obligé d'installer le logiciel.

SCHEMA CHIFFREMENT



EMAIL

- Première faille : Le mot de passe du compte email : Utiliser les règles vues précédemment

- Possibilité de chiffrer les messages et les pièces jointes envoyés avec Outlook, par exemple. Vous devez auparavant envoyer votre certificat (identité numérique) à votre destinataire. Il vous aura ensuite ajouter à ses contacts, et il pourra lire votre message.

- MSSANTE : Messagerie nationale sécurisée accessible aux professionnels de santé. Déjà disponible.

SERVEUR DE FICHIERS

Services de stockage et de partage de copies de fichiers sur internet (ex : Dropbox) :

FORMELLEMENT INTERDIT !!!

Sauf si agréé Hébergeur de données de santé

MESSAGERIE INSTANTANEE

FORMELLEMENT INTERDIT !!!