Rapport de Conformité Légale

Groupe 5

Drago Mamadou, Fanise Soufiane, Hawat Paul, Otsoua Ibata Van Sorel, Hebert Clément, Lebourgeois Emilie

lycée FLAUBERT

Sommaire

Principes de base du RGPD:

Le Règlement Général sur la Protection des Données (RGPD) encadre strictement l'utilisation des données de santé.

Ces données sont considérées comme particulièrement sensibles, et leur traitement est en principe interdit (article 9.1). Cependant, il existe des conditions précises permettant de les utiliser légalement.

Tout traitement doit reposer à la fois sur une base légale (article 6 du RGPD), par exemple l'exécution d'une mission d'intérêt public dans le cas d'un hôpital, et sur une exception spécifique (article 9.2), adaptée au domaine de la santé.

Les exceptions les plus courantes sont : l'utilisation des données pour les soins ou la gestion des services de santé (article 9.2.h), leur traitement à des fins de recherche scientifique ou statistique avec les garanties nécessaires (article 9.2.j), ou bien le recours au consentement explicite du patient (article 9.2.a).

Il existe plusieurs principes à respecter pour traiter des données sensibles.

Tout d'abord, les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence). Par exemple, l'individu doit être informé de l'identité du responsable du fichier ou encore de la finalité du traitement des données.

Elles doivent être collectées pour des finalités déterminées et minimisées, c'est-à-dire pertinentes et limitées à ce qui est nécessaire au regard des finalités.

De plus, elles doivent être exactes et donc tenues à jour, mais aussi conservées pendant une durée ne dépassant pas celle nécessaire au regard des finalités.

Enfin, ces données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé, illicite, la perte, la destruction ou les dégâts d'origine accidentelle.

Le responsable du traitement, quant à lui, est responsable du respect des principes précédents et est en mesure de démontrer qu'ils sont respectés.

Obligation légale:

Droit des personnes :

Les obligations légales commencent par le respect des droits des personnes dans ce cas particulier les patients et leurs données personnelles. Tout d'abord l'utilisateur bénéficie d'un droit à la confidentialité et à la protection des données personnelles, les informations médicales sont des données sensibles. Leur traitement est donc strictement encadré et doit être limité aux personnes autorisées.
Ensuite, les patients doivent être informés et doivent bénéficier d'un consentement explicite, les patients doivent être clairement informés de l'utilisation de leurs données et donner leur consentement au préalable.
Enfin les patients ont le droit d'accès, de rectification et d'opposition, les patients peuvent à tout moment consulter leurs données, demander leur modification ou s'opposer à certains traitements comme des études par exemple.

Obligations de l'établissement :

l'établissement de santé est tenu de mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'assurer la sécurité et la conformité du traitement des données.

Tout d'abord l'établissement doit assurer la sécurité des données comme le fait de prévenir la perte, l'altération, l'accès non autorisé ou la divulgation des données de santé, notamment dans la gestion des documents papier et des fichiers excel.
Par conséquence pour la conformité et le secret médical : seules les personnes autorisées (médecins, chirurgiens et personnel administratif désigné) peuvent accéder aux données.
Ensuite pour la traçabilité des accès et les actions de consultation, modification ou transmission des données, les données doivent être enregistrées, afin d'assurer un suivi en cas d'audit ou de litige.
Enfin, l'établissement doit archiver et définir une durée de conservation des données doivent être conservée pendant une durée légale déterminée, puis détruite de manière sécurisée conformément aux dispositions du code de la santé publique et aux recommandations de la CNIL.

Responsabilités du personnel :

Pour le personnel administratif ils sont chargés de la manipulation des documents papier et des fichiers informatiques, il doit veiller au respect strict des règles de confidentialité et de sécurité.
Les médecins et chirurgiens doivent garantir la qualité et la pertinence des données, ils doivent s'assurer que les informations recueillies et utilisées sont exactes et conformes aux protocoles de recherche.
Pour finir l'établissement est responsable du traitement des données, il demeure juridiquement responsable de la conformité des pratiques. Tout manquement peut entraîner des sanctions administratives (notamment par la CNIL) et pénales.

Sources utilisées : Code de la santé publique : Article L1110-4 : secret médical et respect de la vie privée. CNIL : règlement (UE) 2016/679 du 27 avril 2016 : article 32, 15 à 21

Actions à entreprendre :

Concernant la base légale et la documentation, l'on va s'appuyer sur l'article 6 et l'article 9 de la RGPD qui nous informe que l'on doit Identifier clairement la finalité de chaque traitement**.** L'on va devoir également tenir un registre des traitements selon les instructions de l'article 30. et si l'on traite à grande échelle des données à caractère correspondant au domaine de la santé l'on devra réaliser une AIPD (information provenant de l'article 35 + liste du CNIL)

Concernant les principes fondamentaux, l'on devra selon l'article 12 informer très clairement les patients si l'on affiche, notifient ou mentionnent leurs présence en ligne. L'on devra aussi limiter les données collectés à ce qui est strictement nécessaire ; vérifier et mettre à jour les données des patients ; fixer et appliquer des durée de conservation limitées ; anonymiser ou pseudonymiser les données quand l'identification n'est pas nécessaire et mettre en place un processus pour démontrer la conformité. Toutes ces consignes proviennent de l'article 5 de la RGPD.

Concernant le droit des patients, l'on devra mettre en place un canal de contact ; garantir l'accès, la rectification, l'effacement, la limitation, la portabilité ou l'opposition ; prévoir des procédures internes pour traiter les demandes dans des délais légaux et informer sur les cas ou certains droit peuvent être restreints tel que des recherches médicales. (article 12-22)

Concernant la sécurité & organisation, Privacy by design / default : limiter les données et protéger dès la conception ; contrôles d'accès : accès seulement au nécessaire; séparer pro/perso ; chiffrement, sauvegardes, journalisation des accès ; former et sensibiliser le personnel. (article 25 et 32)

Concernant la gouvernance et la conformité, nommé un Délégué à la production des données si l'organisme et public ou si celui-ci traite une grande quantité de données sensibles ; documenter les politiques de sécurité et de confidentialité ; mettre en place une procédure de notification de violation de données (article 33-34)

Quelques actions techniques à tenir, séparer outils pro/perso ; tenir un registre clair ; anonymiser les données inutiles (remplacer les nom par des id aléatoire) ; cloisonner les accès chaque agent voit ce qui le concerne.

Propositions Techniques pour la sécurité des données (solutions pour assurer la sécurité du réseau/données)

Il faudrait sensibiliser et former le personnel sur les bonnes pratiques à avoir pour conserver la confidentialité des données.

Aussi, il pourrait être intéressant de faire un audit des droits d'accès dont dispose chaque utilisateur qui a besoin de traiter des données personnelles.

De plus, l'authentification est un point important pour protéger la confidentialité des données personnelles. Il est alors primordial de ne jamais communiquer les identifiants, d'avoir un mot de passe robuste et d'utiliser la double authentification.

Nous pouvons aussi mettre en place un système de pseudonymisation. Ce système consiste à remplacer les données directement identifiantes des patients (noms, prénoms,..) par des données indirectement identifiantes commes des alias ou des séquences de numéros qui sont appelés des "pseudonymes".

On peut également mettre en place le principe de minimisation qui consiste à ne collecter et ne traiter que les données strictement nécessaires à l'objectif annoncé.

Une solution pour sécuriser les transmission entre postes clients et le serveur de base de données doit être mise en place. Par exemple, la solution de connexion sécurisée à MySQL avec SSL.

Pour les solutions qui touchent à l'installation réseau, il est possible de mettre en place des VLANs pour permettre un cloisonnement du site de la clinique, afin que les employés puissent avoir accès uniquement aux données auxquelles ils doivent avoir accès.

Si un employé souhaite faire une demande de droits, il devra contacter son service informatique via un ticket GLPI, afin que le DPO puisse prendre connaissance de cette demande et déterminer si, oui ou non, l'employé peut obtenir ces droits exceptionnels.

Les utilisateurs seront aussi organisés en groupes afin que les droits soient respectés conformément à la consigne du moindre privilège et au RGPD.