https://ressources.anap.fr/numerique/publication/2623-memento-rgpd

(DGOS)

Mémento RGPD

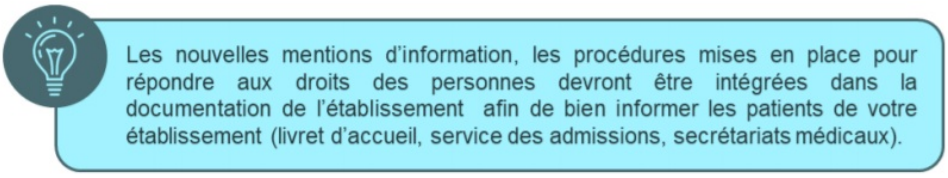
Sommaire

4. Contrôles et sécurité des données

Le RGPD renforce le contrôle par les usagers de leurs données personnelles

Le RGPD confirme les droits déjà prévus par la Loi Informatique et Libertés (LIL) et crée de nouveaux droits pour les citoyens. Le RGPD améliore la transparence en renforçant les exigences en terme d'information des usagers sur l'utilisation faite de leurs données et en leur facilitant l'accès à ces informations.

Confirmation des droits prévus par la LIL	Nouveautés
• Droit à l'information • Droit d'accès aux données • Droit de rectification • Droit à l'oubli • Droit d'opposition • Droit à la réclamation	• **Renforcement de l'information des usagers dont les données sont collectées (toutes les mentions de l'article 13 ne sont pas reprises)** ✓ Sur le droit d'exercer une réclamation ✓ Sur les coordonnées du DPO ✓ Sur l'intérêt légitime du responsable de traitement ✓ Sur le droit à l'effacement ✓ Sur le droit d'opposition de la personne • **Droit à la limitation du traitement (art.18)** • **Droit à la portabilité des données (art.20)** ✓ ce droit ne s'exerce que pour les traitements fondés sur le consentement ou l'exécution d'un contrat • **Elargissement des cas de notification des failles de sécurité (art.34)** • **Droit la réparation (art.82)**



Le RGPD renforce le contrôle par les usagers de leurs données personnelles

Le RGPD réaffirme également le droit à l'information et le droit d'accès des patients et de tout autre personne concernée par le traitement de données personnelles en établissement de santé (employés, fournisseurs, etc.)

Droit à l'information

Quiconque met en œuvre un fichier ou un traitement de données à caractère personnel est obligé d'informer la personne qui fait l'objet de ce traitement de données personnelles, notamment :

- De l'objectif de la collecte d'informations
- De son caractère obligatoire ou facultatif
- L'identité du responsable du traitement
- La durée de conservation
- Des destinataires des informations
- Des droits reconnus à la personne
- Des éventuels transferts de données vers un pays hors de l'Union européenne
- ...

L'information doit être claire et adaptée au public concerné.

Droit d'accès aux données

Les personnes concernées peuvent demander directement au responsable d'un fichier s'il détient des informations sur eux et demander à ce qu'on leur communique l'intégralité de ces données. L'exercice du droit d'accès permet de contrôler l'exactitude des données et si besoin de les faire rectifier ou effacer.

Il existe des dispositions spécifiques dans le code de la santé publique pour l'accès des usagers à leur dossier médical.

Modèles de mention d'informations : https://www.cnil.fr/fr/modeles/mention

Sécurisez les données personnelles en votre possession

Les mesures nécessaires doivent être prises pour assurer au mieux la sécurité des données à caractère personnel en votre possession afin de garantir au minimum les risques de pertes de données ou de piratage.

Les bonnes pratiques à avoir

Certains réflexes doivent être essentiels :

- Mises à jour de vos antivirus et logiciels
- Changement régulier et utilisation de mots de passe complexes
- Chiffrement des données dans certaines situations

En cas de perte ou vol d'un outil informatique, L'accès à son contenu en sera rendu plus difficile pour toute personne non autorisée à l'utiliser.

Les bonnes questions à se poser pour évaluer rapidement le niveau de sécurité de votre établissement, notamment :

- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?

- Une procédure de sauvegarde et de récupération de données régulièrement testée en cas d'incident a-t-elle été mise en place ?
- les règles de sécurité fixées par la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) sont-elles respectées ?

En cas de violation des données

En cas de violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées, etc.) vous devez le signaler à la CNIL, et à la personne concernée, dans les meilleurs délais (au maximum sous 72h) si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées : https://notifications.cnil.fr/notifications/index

Le signalement de tout incident de sécurité informatique est obligatoire et doit être déclaré sur : https://signalement.socialsante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

Glossaire

CNIL
Loi
personne
PGSSI-S
RGPD
risque

Date de parution : 25/06/2019

Télécharger la production