RGPD : un référentiel pour le cabinet dentaire

Outre la réalisation d'un référentiel adapté à la pratique de ville pour la protection des données de santé, la Commission nationale de l'informatique et des libertés (Cnil) a tranché sur l'obligation de désigner un délégué à la protection des données, qui concernera peu de cabinets dentaires.

La Commission nationale de l'informatique et des libertés (Cnil) aura donc entendu le message du Conseil national de l'Ordre et de sa commission numérique. Dans l'une des deux délibérations en date du 18 juin concernant la protection des données à caractère personnel dans les cabinets de ville, la Cnil suggère que **la réalisation d'une analyse d'impact ainsi que la désignation d'un délégué à la protection des données ne devraient être nécessaires que pour les seuls cabinets de groupe dépassant le seuil annuel de 10 000 patients**. Peu de cabinets dentaires sont donc impactés par cette suggestion de la Cnil, qui n'a certes pas valeur de réglementation, mais dont la portée n'est pas négligeable notamment en cas de contentieux. L'objectif de la Cnil, dans ses deux délibérations n° 2020-081 et n° 2020-076 du 18 juin, consistait à faciliter l'application de nos obligations en matière de *« traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux »*. On sait en effet que le traitement des données à caractère personnel, dans le champ médical et de la santé, est considéré à juste titre comme très sensible. La Cnil conforte donc les différents outils que le Conseil national avait mis à la disposition des confrères au moment de l'entrée en vigueur du RGPD. Elle fait même mieux puisque, en appui du guide qu'avait édité l'Asip santé pour assurer la sécurité de ces données, elle en propose une synthèse sous la forme du tableau que nous publions ci-dessous.

CATÉGORIES	MESURES
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel du cabinet accédant aux données.
	Pour un cabinet mutualisant des ressources informatiques, rédiger une charte informatique et lui donner force contraignante.
Authentifier les utilisateurs	Définir un identifiant (« login ») propre à chaque utilisateur.
	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la Cnil.
	Pour les utilisateurs accédant aux données de santé, utiliser une authentification forte via leur carte de professionnel de santé (CPS) ou tout moyen alternatif à deux facteurs.
	Maintenir la CPS au niveau strictement personnel, sans communication du code secret au personnel du cabinet (p. ex. : secrétaire médical).
Gérer les habilitations	Attribuer un profil d'habilitation adapté à chaque utilisateur (distinguant notamment les données administratives et les données médicales).
	Supprimer les permissions d'accès obsolètes.
	Informer les utilisateurs de la mise en place du système de journalisation.
	Prévoir les procédures pour les notifications de violation de données à caractère personnel.

CATÉGORIES	MESURES
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de la session informatique.
	Permettre la mise à jour régulière des antivirus.
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste.
	Limiter le stockage d'informations d'ordre médical sur une tablette ou un ordiphone (en raison des conséquences pour les patients en cas de vol ou de perte du matériel). Si ces équipements sont utilisés, leur niveau de sécurisation des données doit être équivalent à celui des autres équipements (chiffrement, codes d'accès, etc.).
	Exiger un secret pour le déverrouillage des ordiphones ou des tablettes.
	Protéger les écrans des regards indiscrets (orientation, filtre optique).
	Limiter l'utilisation de supports de stockage amovibles (clés USB, disques durs externes) et chiffrer systématiquement les données sensibles qui y sont conservées.
	Ne pas prêter un ordiphone ou une tablette à usage professionnel.
Protéger le réseau informatique interne	Limiter les connexions d'appareils non professionnels sur le réseau.
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées.
	Permettre l'installation sans délai des mises à jour critiques.
Sauvegarder et prévoir la continuité d'activité	Effectuer ou permettre l'exécution des sauvegardes régulières.
	Stocker les supports de sauvegarde dans un endroit sûr.
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées.
	Détruire les archives obsolètes de manière sécurisée.
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable du cabinet les interventions par des tiers.
	Effacer les données de tout matériel avant sa mise au rebut.
Gérer la sous-traitance	Prévoir des clauses spécifiques dans les contrats des sous-traitants.
	Prévoir des conditions de restitution et de destruction des données.
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.).
Sécuriser les échanges avec d'autres professionnels de santé et avec les patients	S'assurer qu'il s'agit bien du bon destinataire.
	Utiliser une messagerie électronique sécurisée de santé pour les échanges entre professionnels de santé.
	Pour les échanges avec d'autres professionnels intervenant dans la prise en charge du patient ou avec les patients eux-mêmes : - procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard et transmettre le secret par un envoi distinct et via un canal différent ; - utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ; - choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes.
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées.
	Installer des alarmes anti-intrusion et les vérifier périodiquement.
	Sécuriser le stockage des dossiers au format papier (locaux sécurisés, armoire fermant à clé).
	Récupérer les documents imprimés contenant des données immédiatement après leur impression ou effectuer, lorsque c'est possible, une impression sécurisée.
	Détruire les documents papier contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié (certifié au minimum classe 3 de la norme DIN 32757105).