STRATEGIE NUMERIQUE

Ce document complète le projet d'établissement 2023-2028.

L'objectif de l'EHPAD est de développer un environnement numérique sécurisé, performant et adapté aux besoins des résidents, des professionnels et des parties prenantes.

La stratégie

L'établissement s'engage à :

- Assurer la maintenance, l'évolution et la sécurisation continue des équipements et infrastructures numériques
- Garantir la confidentialité, l'intégrité et la disponibilité des données relatives aux résidents et au fonctionnement de l'établissement
- Assurer un accès sécurisé aux systèmes d'information par un investissement adapté
- Protéger les données de santé et les données personnelles conformément à la réglementation en vigueur
- Mettre à disposition des professionnels des outils numériques à jour
- Favoriser une communication numérique accessible et adaptée avec les résidents, les familles, les professionnels et les parties prenantes.
- Prendre en compte et évaluer le risque numérique dans le plan de gestion de crise
- Développer les compétences numériques des professionnels par des actions régulières d'information et de sensibilisation

Les outils et la mise en œuvre de la stratégie numérique

Afin de mettre en œuvre cette stratégie, l'établissement déploie les actions suivantes :

Protection du système d'information

- Les données sont sauvegardées régulièrement grâce à un système de double sauvegarde garantissant leur restauration en cas d'incident ;
- Les équipements informatiques bénéficient de mises à jour régulières et de dispositifs de protection adaptés ;
- Le prestataire informatique spécialisé Tekinova assure la maintenance des équipements, la sécurisation du réseau, le suivi des infrastructures et l'accompagnement technique de l'établissement.
- Le plan de gestion de crise contient un paragraphe « Sécurité du Système d'information / Prévention Cyberattaque »

Sécurisation des accès et des données

- Le Prestataire Tekinova a mis en place un système de réseau sécurisé
- Chaque professionnel dispose d'un identifiant personnel et d'un mot de passe strictement confidentiels ;
- Les identifiants et mots de passe sont individuels et ne peuvent être ni partagés, ni communiqués, ni affichés ;
- Les droits d'accès aux logiciels sont définis selon les missions et les responsabilités de chaque professionnel ;
- Les sessions informatiques sont automatiquement verrouillées en cas d'inactivité et doivent être fermées après chaque utilisation ;
- Les connexions et les actions réalisées dans les logiciels métiers sont tracées afin de garantir la sécurité et la traçabilité des informations ;
- Les mots de passe répondent aux exigences de complexité définies par la politique de sécurité informatique et sont renouvelés régulièrement.

Accompagnement des professionnels

- Les équipes sont régulièrement sensibilisées aux bonnes pratiques numériques, notamment en matière de confidentialité, de cybersécurité, de phishing et de fraude informatique ;
- Les professionnels disposent d'outils numériques facilitant l'organisation du travail, la gestion administrative et la coordination des accompagnements.

Développement des services numériques

L'établissement s'appuie sur différents outils numériques permettant d'améliorer la qualité de fonctionnement et la coordination avec les partenaires :

- Logiciels internes de gestion des ressources humaines et de planification (Octime, Staffelio, Silae) ;
- Plateformes nationales et sectorielles facilitant les parcours et les échanges (ViaTrajectoire, CNSA) ;
- Outils de communication institutionnelle tels que le site internet et l'application Illiwap . Le site internet est géré par un prestataire spécialisé afin qu'il soit toujours à jour de la réglementation
- Réseau Wi-Fi sécurisé accessible aux professionnels et aux résidents selon les modalités définies par l'établissement.

Le Dossier Usager Informatisé (DUI) : Netsoins

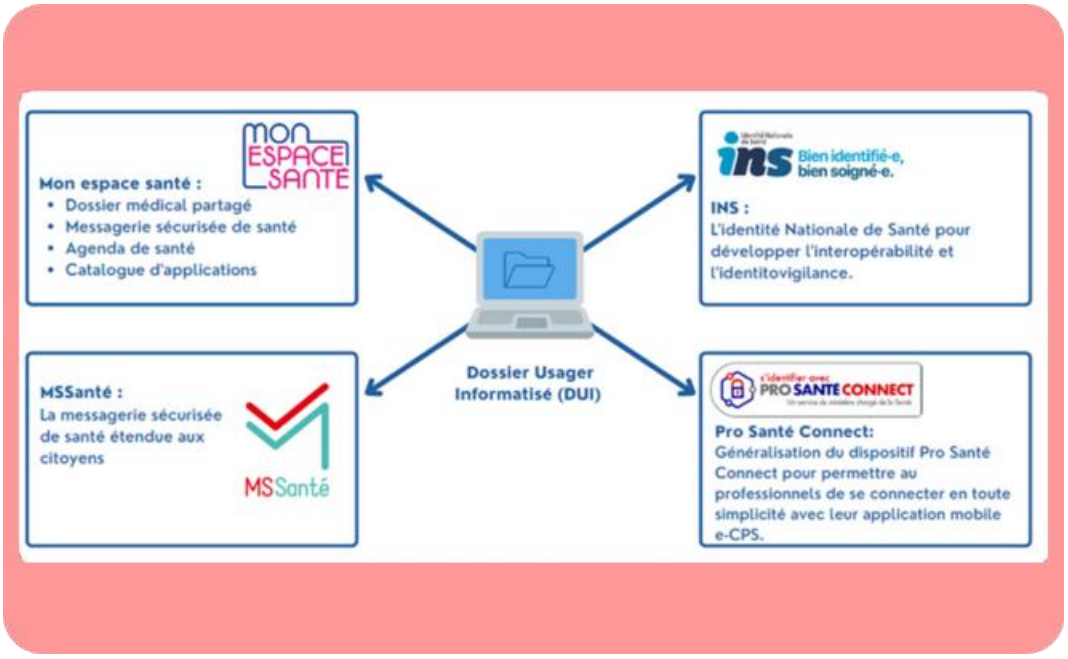
Depuis 2019, le ministère chargé de la Santé porte une stratégie nationale du numérique en santé. Annoncé en juillet 2020, le Ségur du numérique en santé vise à accélérer les actions de la feuille de route « Ma Santé 2022 » concernant le partage des données sensibles, afin d'améliorer la santé des citoyens, le quotidien des professionnels et l'efficience du système de santé.
Dans le cadre de l'amélioration de la coordination des soins et de la sécurisation des pratiques, notre établissement a mis en œuvre une stratégie structurée de déploiement des outils numériques en santé (MSS, e-CPS, DMP), notamment en s'équipant d'un logiciel, Dossier Usager Informatisé (DUI), référencé Ségur.
Celui-ci permet de généraliser le partage fluide et sécurisé des données afin d'améliorer la coordination autour des usagers et les replacer au cœur de leur accompagnement.

La démarche mise en œuvre repose sur les objectifs opérationnels suivants :

- Sécuriser les échanges d'informations médicales et paramédicales, avec la création d'une adresse MSS (Messagerie Sécurisée de santé), pour les professionnels concernés (infirmiers, médecins coordonnateurs, cadres…). Cet outil est utilisé prioritairement pour les transmissions médicales (comptes rendus, prescriptions, échanges avec hôpitaux, médecins traitants).

- Améliorer la coordination avec les professionnels de santé libéraux, les établissements sanitaires et les partenaires du territoire, avec l'alimentation du DMP (Dossier Médical Partagé) par les équipes. Bientôt, la consultation du DMP pour améliorer la continuité des soins sera développée en sus (par ex, lors des admissions et des retours d'hospitalisation),

- Renforcer l'appropriation des outils numériques par les professionnels (MSS et DMP).



AGEVAL : outil de gestion de la qualité

L'ensemble des données de la solution AGEVAL est hébergé dans les datacenters (localisés en France) de son partenaire SIGMA INFORMATIQUE. Ce dernier est un hébergeur agréé par ASIP SANTÉ (hébergement agréé de données de Santé) garantissant fiabilité, rentabilité, sécurité et qualité de service.

Les sauvegardes sont réalisées par AGEVAL sur un serveur géré SIGMA INFORMATIQUE. La politique de sauvegarde des données de la solution AGEVAL suit : 2 sauvegardes quotidiennes (12h et 24h) et une rétention des sauvegardes à J-7 sur 2 emplacements distincts.

De plus, une sauvegarde des documents qualité de référence intégrés dans le logiciel AGEVAL est en place dans le dossier « Qualité » du serveur local de l'établissement.