RECOURIR AU NUMÉRIQUE POUR MIEUX SOIGNER

La transformation de notre système de santé ne pourra avoir lieu sans un développement massif et cohérent du numérique en santé en France. Le numérique n'est pas une fin en soi. C'est un moyen pour mieux coordonner les professionnels de santé, pour développer des innovations thérapeutiques et organisationnelles, pour lutter contre la fracture sanitaire, pour repositionner le citoyen au cœur du système de santé, bref pour soigner mieux.

La politique de transformation numérique du secteur de la santé portée par la Délégation du numérique en santé repose sur un **engagement fort de sécurité des données de santé** énoncé dans la 2° orientation de la feuille de route « *Accélérer le virage numérique* ».

Pulsy décline cette politique en région Grand Est. Notre groupement d'intérêt public accompagne les acteurs de santé dans leurs projets de mise en place d'outils numériques. Nous garantissons la **conformité** de ces solutions aux **meilleurs pratiques en matière de sécurité** des systèmes d'information. C'est une attente forte de nos membres formalisée en **objectif stratégique dans notre feuille de route**.

Cet engagement se traduit par :

- Des solutions ergonomiques, facilement **accessibles** par les utilisateurs, professionnels du monde sanitaire, médico-social et social, qui peuvent s'appuyer sur nos équipes expertes pour répondre à leurs attentes, y compris **en dehors des heures ouvrées pour les services critiques** ;
- Des solutions robustes qui s'appuient sur une infrastructure **sécurisée à haut niveau de disponibilité** ;
- Un strict respect des utilisateurs par le recueil de leur **consentement** et la **confidentialité** totale des données personnelles recueillies dans le **coffre-fort numérique Pulsy** ;
- Une transparence sur l'ensemble de nos actions, garantie par notre gouvernance représentative, nos outils de pilotage, notre certification **HDS** et notre **démarche d'amélioration continue**.

Ces engagements d'éthique et de sécurité fondent notre action au service des professionnels, patients et usagers du Grand Est mais également des collaborateurs de Pulsy.

Il est donc primordial de **protéger les ressources et les informations** de nos systèmes d'information, de préserver la confiance de nos usagers et de veiller à la **continuité** de nos activités essentielles : nous devons nous employer à structurer et à mettre en œuvre une démarche globale de **Management de la Sécurité de nos Systèmes d'Information**, et de **conformité** vis-à-vis des référentiels et des réglementations applicables.

Afin de décliner concrètement ces principes de sécurité au sein de notre organisation, de nos systèmes d'information, de nos projets ainsi que dans nos réflexes au quotidien, il est essentiel de compter sur la **participation active de chacun de nos collaborateurs**.

Pulsy
6 Allée de Longchamp, 54600 Villers-lès-Nancy
03 83 97 13 70

POURQUOI PROTÉGER L'INFORMATION ?

La prise en charge d'un patient/usager nécessite le recueil de données à caractère personnel et tout particulièrement des données de santé. Ces données peuvent être partagées entre professionnels de santé ou provenir d'autres sources (DMP, autres professionnels de santé, institutions ou structures médicalisées...) dans le respect du secret professionnel.

La mise en œuvre de système d'information de santé doit prendre en compte **les droits fondamentaux du patient/usager**, en garantissant notamment la **confidentialité**, la **traçabilité** et la **pérennité** des données de santé à caractère personnel tout au long du cycle de vie des données (de leur création ou saisie à leur archivage et destruction).

Quatre niveaux de sécurité :

- **Disponibilité : un niveau contextualisé et encadré** en fonction des besoins et des contraintes métier.
- **Intégrité : une fiabilité maximale** des données de santé à tous les stades de leur cycle de vie.
- **Confidentialité : un accès maîtrisé** aux données de santé en cohérence avec leur nature et la nécessité pour un individu d'y accéder. Seule l'équipe de soin impliquée dans la prise en charge du patient doit pouvoir accéder à ses données de santé, dans le respect du secret professionnel. Le principe est qu'au-delà de ce périmètre, tout accès ne peut être accordé qu'avec l'accord du patient (et tous les droits qui en découlent).
- **Traçabilité : des traces à valeur de preuve** face au détournement de finalité.

PROTÉGER l'information et PÉRENNISER la sécurité des services

MAINTENIR l'activité et FIABILISER les systèmes D'INFORMATION

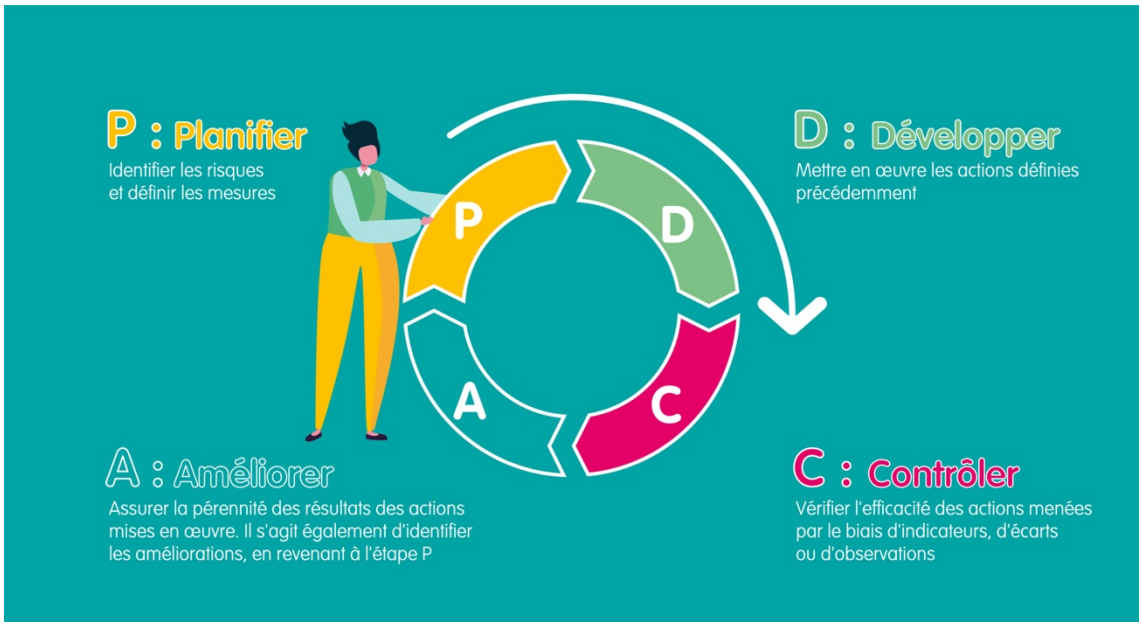
AMÉLIORER la qualité de l'organisation de Pulsy

Pulsy
6 Allée de Longchamp, 54600 Villers-lès-Nancy
03 83 97 13 70

LE SYSTÈME DE MANAGEMENT DE SÉCURITE DE L'INFORMATION ?

Afin d'assurer la maîtrise de la sécurité des systèmes d'information de Pulsy, la démarche repose sur la mise en œuvre d'un Système de Management de la Sécurité de l'information (SMSI), qui s'appuie sur le cadre défini par la norme ISO 27001 et son annexe A.

Ce système de management s'inscrit dans une **démarche d'amélioration continue** :



L'objectif de cette démarche est d'apporter des résultats concrets, mesurables et proportionnés aux risques. Ainsi les risques sont appréciés et les mesures définies en conséquence **(Planifier)**, puis elles sont mises en œuvre **(Développer)**, et ensuite elles sont contrôlées **(Contrôler)**. Enfin, des actions correctives sont mises en place en fonction des écarts observés **(Agir)**.