1. Objectif

Cette politique définit les principes appliqués par l'organisation pour assurer la **protection des données à caractère personnel**, en particulier des données de santé, en conformité avec le RGPD, la loi Informatique et Libertés, et le référentiel HDS. Elle s'articule avec les politiques SSI associées (classification, accès, journalisation, sauvegardes, cryptographie).

2. Périmètre

Cette politique s'applique à l'ensemble des traitements de données à caractère personnel réalisés par l'organisation, quels que soient les supports et les systèmes (applications métiers, SI de santé, solutions cloud, sauvegardes, journaux, etc.), y compris ceux couverts par la certification HDS. Elle s'applique à tous les collaborateurs, prestataires et sous-traitants qui interviennent sur ces traitements dans le cadre de leurs fonctions.

3. Principes de protection des données

L'organisation applique les principes suivants, conformes à l'article 5 du RGPD :

a) **Licéité, loyauté et transparence :**
- Les données personnelles sont collectées de manière licite et transparente.

Les personnes sont informées des finalités, des bases juridiques, des destinataires, des durées de conservation et de leurs droits via les mentions d'information et politiques de confidentialité appropriées.

b) Limitation des finalités :
- Les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de façon incompatible avec ces finalités

c) Minimisation des données :
- Seules les données nécessaires au regard des finalités sont traitées et collectées.

d) Exactitude :
- Les données doivent être exactes, complètes et mises à jour. Des mécanismes permettent la rectification ou la mise à jour à la demande des personnes ou des services métiers

e) **La limitation de la conservation**
- Les données sont conservées pour une durée ne dépassant pas celle nécessaire au regard des finalités en tenant compte des obligations légales ou réglementaires applicables (notamment en matière de santé).

- Les durées sont définies dans le registre des traitements et les référentiels internes (plan de classement, politique d'archivage).

f) Intégrité et confidentialité :

- Les données sont traitées de manière à garantir leur sécurité, y compris la protection contre le traitement non autorisé ou illicite, la perte, la destruction ou les dommages d'origine accidentelle.
- Les mesures de sécurité mises en œuvre s'appuient sur le SMSI et les politiques SSI (accès, cryptographie, journalisation, sauvegardes, sécurité des postes, télétravail, sécurité physique), avec un niveau renforcé pour les données de santé.

4. Engagement de la direction

La direction s'engage à :

- Respecter la réglementation sur la protection des données
- Mettre en place les ressources nécessaires
- Intégrer la protection des données dans le SMSI.

5. Responsabilités

Fonction	Rôle
CEO	Valide la politique, alloue les ressources nécessaires et veille à son application dans le cadre du SMSI et de la démarche HDS.
DPO	Conseille et contrôle la conformité RGPD, tient le registre des traitements, pilote les analyses d'impact (PIA/AIPD) et est l'interlocuteur de l'autorité de contrôle.
CTO	Met en œuvre les contrôles de sécurité.
RSSI	Met en œuvre et pilote les mesures de sécurité techniques et organisationnelles du SMSI, en lien avec les politiques SSI, pour assurer la sécurité des données personnelles.
Responsables métiers	S'assurent que les traitements de leur périmètre respectent les principes et procédures définis (finalités, base juridique, minimisation, durées de conservation).
Employés et prestataires	Respectent les règles de sécurité et de confidentialité, ainsi que les procédures internes relatives aux données personnelles.

6. Sécurité des données

Les mesures de sécurité appliquées aux données personnelles sont définies et mises en œuvre dans le cadre du SMSI et des politiques SSI existantes, notamment :

- SSI-POL-03 – Classification de l'information : classification des données personnelles (dont données de santé) et mesures associées.
- SSI-POL-04 / SSI-POL-12 – Gestion des accès et des identités : contrôle des accès, gestion des habilitations et des moyens d'authentification.
- SSI-POL-05 – Contrôle cryptographique : chiffrement des données au repos et en transit, gestion des clés.
- SSI-POL-09 – Journalisation et surveillance : traçabilité des accès et actions sur les données personnelles et de santé.
- SSI-POL-10 – Sauvegarde et récupération : continuité, sauvegardes et tests de restauration des systèmes contenant des données personnelles.
- SSI-POL-06, 07, 08, 13, 14, 15 – Incidents, développement sécurisé, vulnérabilités, télétravail, postes de travail, sécurité physique, etc.

Les exigences HDS (journalisation renforcée, contrôle fin des accès, sauvegardes externalisées sécurisées, sécurité physique des locaux d'hébergement, supervision, localisation des données) sont appliquées de manière spécifique aux traitements de données de santé concernés.

7. Localisation et transferts de données

Les données personnelles, et en particulier les données de santé hébergées dans le cadre HDS, sont hébergées dans des environnements conformes au référentiel HDS et aux exigences de souveraineté (EEE ou pays offrant un niveau de protection adéquat, ou encadrement contractuel approprié).

Tout transfert hors de ces zones fait l'objet d'un encadrement juridique approprié (clauses contractuelles types, garanties supplémentaires) documenté dans le registre des traitements.

8. Droits des personnes

Les personnes concernées disposent des droits suivants, dans les limites prévues par les textes applicables :

- Droit d'accès à leurs données.
- Droit de rectification.
- Droit d'effacement (droit à l'oubli, lorsque applicable).
- Droit à la limitation du traitement.
- Droit à la portabilité des données lorsque les conditions sont réunies.

- Droit d'opposition au traitement, notamment pour certains traitements fondés sur l'intérêt légitime.

Impact Healthcare met en place des procédures internes pour traiter les demandes d'exercice de droits dans les délais réglementaires et en assurer la traçabilité.

9. Registre des traitements et analyses d'impact

L'organisation tient à jour un registre des traitements de données personnelles, incluant pour chaque traitement : finalités, base juridique, catégories de données, destinataires, durées de conservation, mesures de sécurité principales, transferts éventuels.

Pour les traitements susceptibles d'engendrer un risque élevé (notamment en santé), une analyse d'impact relative à la protection des données (PIA/AIPD) est réalisée et actualisée.

10. Gestion des incidents impliquant des données personnelles

Tout incident de sécurité impliquant des données personnelles doit être :

- signalé immédiatement selon la Politique de gestion des incidents (SSI-POL-06)
- analysé et documenté
- traité avec des mesures correctives adaptées

Lorsque les conditions réglementaires sont réunies, l'organisation :

- notifie la violation à l'autorité de contrôle compétente dans les délais requis
- informe les personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

11. Révision

La présente politique est revue au moins une fois par an, et à chaque évolution significative du contexte réglementaire, du référentiel HDS, des traitements de données personnelles ou du SI.