Politique de Protection des Données Personnelles	Document n° : CHRU/ 5.d/002/v2
	Page : 1/25
	Document(s) de référence :

Rédaction : MAS SANDRINE	Vérification : LENOIR FRANCOIS (Directeur(trice) de site / pôle / projets), EUVRARD JEROME (Directeur(e) des systèmes d'information (DSI)), BARRE SOPHIE (Directeur(e) d'établissement de santé - chef(fe) d'établissement), DELPUECH ANABELLE (Directeur(e) d'établissem[...]	Approbation : FERRER ANNE (Directeur(e) d'établissement de santé - chef(fe) d'établissement) Date d'approbation : 19/02/2026 09:03:00
Groupe de travail éventuel : KEBE DJEINABA, VERDAGUER VALERIE, PADOVANI ANGE, GARCIA DAMIEN, GIRAUD ISABELLE, GIMENO LINDA, David MORQUIN, CAGNIEUL JEROME, GAUTHIER SYLVIE, SICARD SCIACOVIELLO OLIVIER, MAKOUDI YANNIS	Vérification par DACQSS-PU	Classification : Public (C0)

DESTINATAIRES

Tout le monde

Cycle de vie du document

Version	Date d'application	Modifications/ Révisions
v2	20/02/2026	Corrections mineures (correction de fautes d'ortographe)
v1	19/02/2026	Création

Table des matières

1 Préambule : Déclaration de la Direction 3

2 Objet de la Politique de Protection des Données Personnelles (PPDP) 4

3 Champ d'application 5

4 Enjeux de la Politique de Protection des Données Personnelles (PPDP) 5

5 Cadre législatif et réglementaire 7

6 Responsabilités 7

7 Principes fondamentaux à respecter 8

7.1. Licéité et finalité du traitement 8

7.2. Loyauté, transparence 8

7.3. Minimisation des données personnelles 8

7.4. Exactitude et mise à jour 9

7.5. Sécurité et confidentialité 9

7.6. Limitation de la conservation 9

8 Les Bonnes pratiques à adopter au quotidien 9

8.1. Pour tous les collaborateurs internes 9

8.2. Pour les managers d'équipe du CHU de Montpellier 11

8.3. Pour les collaborateurs externes (partenaires, prestataires, sous-traitant, etc.) 11

9 Devoir de signalement des incidents sur les données personnelles 11

10 Information et droits des personnes concernées par le traitement de leurs données personnelles 12

11 Transfert de données personnelles 13

12 Réutilisation des données personnelles 13

13 Délégué à la Protection des données (DPO) 14

14 Information et Sensibilisation des collaborateurs 15

15 Sanctions et Recours 15

15.1. Sanctions internes 15

15.2. Sanctions administratives et pénales 16

15.3. Recours des personnes concernées 16

16 Mise à jour et Révision de la PPDP 16

17 Annexe 18

Annexe 1 – Supports internes liés à la PPDP 18

Annexe 2 - Définitions 19

Annexe 3 – Abréviations 25

1 Préambule : Déclaration de la Direction

Le Centre Hospitalier Universitaire (CHU) de Montpellier s'engage à offrir des soins de qualité et à protéger les données à caractère personnel traitées au sein de l'établissement (usagers, professionnels de l'établissement, collaborateurs, prestataires, etc.).

Pour garantir leur sécurité et leur confidentialité, le CHU de Montpellier a mis en place une Politique de Sécurité du Système d'Information (PSSI) et une stratégie de protection des données à caractère personnel spécifiée dans cette Politique de Protection des Données Personnelles (PPDP) de l'établissement.

Cette Politique définit des objectifs de sécurité et de confidentialités des données à travers les mesures, les règles, les processus, les procédures, les structures organisationnelles ainsi que les moyens matériels et logiciel mis en place au sein de notre établissement.

Pour atteindre les objectifs de protection des données personnelles, fixés au travers de la PPDP, ces mesures sont mises en œuvre, évaluées et améliorées selon une démarche continue d'amélioration et de qualité.

Pour répondre à ces exigences, le Délégué à la Protection des Données (DPD = DPO) contribue à la définition de la PPDP et assure la mise en place. Il informe et conseille l'établissement afin de se conformer au Règlement Général sur la Protection des Données (RGPD) et aux autres lois de protection des données. Le Responsable de la Sécurité du Système d'Information (RSSI) supervise la mise en œuvre opérationnelle de la PSSI. Il a un rôle de pilotage et de coordination dans sa mise en œuvre et mène des actions de prévention, de correction et de sensibilisation.

Nos professionnels et les personnels intervenant au sein de notre établissement sont sensibilisés à cette politique via diverses méthodes (règlement intérieur, sensibilisation, procédures, etc.).

Nous sommes tous contributeurs de la sécurité et de la confidentialité des données par notre vigilance, par le respect et l'application au quotidien des mesures mises en œuvre dans le cadre de cette PPDP et la PSSI. C'est pourquoi les managers de l'établissement sont mobilisés pour promouvoir et accompagner chacun dans une culture de la sécurité et la confidentialité au sein de leurs équipes.

En intégrant ces principes dans notre Politique de Protection des Données Personnelles, nous assurons la protection des données tout en soutenant nos missions de soins, d'enseignement et de recherche. Ensemble, nous pouvons garantir l'application quotidienne de la Politique de Sécurité de l'Information et la Politique de Protection des Données Personnelles au bénéfice de nos usagers, nos professionnels et les personnels intervenant au sein de notre établissement.

La Directrice Générale

Mme Anne FERRER

2 Objet de la Politique de Protection des Données Personnelles (PPDP)

La Politique de Protection des Données Personnelles définit les enjeux de la protection des données à caractère personnel, et établit les règles et les bonnes pratiques à respecter par l'ensemble des collaborateurs internes et externes du CHU de Montpellier.

Cette politique complète la Politique de Sécurité du Système d'Information (PSSI) de notre établissement.

Elle vise à garantir la conformité au Règlement Européen sur la Protection des Données Personnelles (RGPD) et à la Loi Informatique et Libertés (LIL), en protégeant les droits des personnes concernées et en réduisant les risques juridiques pour notre établissement dans l'exercice de nos missions :

- **Soins aux usagers :** Assurer des soins de haute qualité, contribuer à sa démarche d'amélioration continue qualité sécurité des soins (IQSS, EIG, etc.), favoriser l'utilisation d'outils à la pointe de la technologie, contribuer à la politique d'ouverture (coopération avec d'autres établissements, professionnels libéraux, etc.) ;
- **Enseignement :** Contribuer et former des professionnels avec une sensibilisation à la sécurité, la protection des données et à la confidentialité ;
- **Recherche :** Faire progresser la recherche afin d'améliorer les prises en charge, découvrir les médicaments de demain et de nouveaux dispositifs médicaux dans le respect de la réglementation ;
- **Organisme-employeur :** Recrutement et gestion du personnel (carrière, rémunération, organisation de travail, évaluation annuelle, formation, etc.).

Dans le cadre de nos missions, **nous réalisons de nombreux traitement de données à caractère personnel** (données personnelles) :

- **De nos usagers** ;
- **De nos collaborateurs internes et externes** (partenaires, prestataires, sous-traitants, etc.).

Ces informations représentent un élément stratégique et essentiel de l'activité de notre établissement. **A ce titre, il est fondamental d'en assurer la confidentialité et une protection adaptée.**

L'objectif du RGPD est de protéger les données personnelles des citoyens européens en leur garantissant des droits et de responsabiliser ceux qui sont amenés à traiter leurs données. **Il n'est pas possible de déroger aux dispositions du RGPD**, **sous peine de sanctions administratives, voire de sanctions pénales** pour les entreprises et les organismes établis sur le territoire de l'Union européenne (UE) ou dans des pays tiers à l'UE qui traitent des données personnelles des citoyens européen.

Développer notre activité en conformité avec le RGPD, c'est mettre en place des mesures techniques et organisationnelles appropriées afin de respecter les principes relatifs au respect de la vie privée, la confidentialité et à la protection des données (respect des droits des personnes, finalité explicite et légitime, durée de conservation, , mesures de sécurité adaptées, etc.) **et aussi (re)découvrir la richesse que constituent les données personnelles pour notre établissement et leur valorisation dans une démarche éthique.**

Les mesures prévues dans la présente Politique de Protection des Données Personnelles sont applicables au quotidien par l'ensemble de nos collaborateurs.

3 Champ d'application

Le périmètre de la Politique de Protection des Données Personnelles couvre l'ensemble des activités du CHU Montpellier traitant des données personnelles et en particulier :

- **Dossier patient ;**
- **Activités médicotechniques** (pharmacie, plateaux d'imagerie, laboratoires, biomédical, etc.) **;**
- **Dossiers des ressources humaines ;**
- **Gestion financière et comptable** ;
- **Activités supports transversales** (optimisation de l'activité hospitalière, amélioration continue qualité sécurité des soins, recherche, sécurité informatique, vidéosurveillance-vidéoprotection, etc.).

Cette politique s'applique :

- **À tout collaborateur interne** (salariés, intérimaires, stagiaires, etc.) **ou externe** (partenaires, prestataires, sous-traitants, consultants, etc.) **ayant accès à des données personnelles dans le cadre de ses fonctions** ;
- **À tous les traitements de données personnelles,** qu'ils soient automatisés ou non (fichiers papier inclus).

L'ensemble des collaborateurs du CHU de Montpellier sont les garants de la mise en œuvre de cette politique afin garantir le respect de la vie privée, du secret professionnel, la confidentialité et la protection des données personnelles, **et préserver ainsi la responsabilité de notre établissement.**

La PPDP est donc un document essentiel, validé par la Directrice générale. Elle est responsable de son application pour garantir la conformité au RGPD du CHU de Montpellier.

4 Enjeux de la Politique de Protection des Données Personnelles (PPDP)

La Politique de Protection des Données Personnelles est un enjeu majeur pour le CHU de Montpellier et nos collaborateurs.

Cette politique permet à notre établissement, au cours de son activité, à :

- **Respecter les droits fondamentaux** : Garantir la protection des données à caractère personnel (usager et collaborateur), le droit au respect de la vie privée, le droit à l'image, la confidentialité et le devoir de discrétion, le secret professionnel (Secret médical) et le partage et l'échange d'informations ;
- **Renforcer la confiance** : Instaurer un climat de confiance avec les collaborateurs internes et externes, en assurant la transparence et la sécurité des données traitées.
- **Sécuriser les activités** : Protéger les données sensibles contre les cyberattaques, les fuites ou les usages abusifs, afin de préserver la continuité et la réputation de l'entreprise.
- **Se conformer aux obligations légales** : Respecter les exigences du RGPD et de la LIL, ainsi que les réglementations spécifiques applicables.
- **Responsabiliser chaque acteur** : Impliquer tous les collaborateurs dans la protection des données, en leur fournissant les outils et les connaissances nécessaires.

- **Limiter les risques juridiques et financiers** : Éviter les sanctions administratives, les poursuites judiciaires et les préjudices d'image liés à une mauvaise gestion des données.

En plus de se conformer pleinement à la réglementation **(licéité[1]), le CHU de Montpellier informe**, en toute **transparence**, les personnes concernées sur les traitements des données personnelles mis en place par des notes d'information (site intranet/internet, livret d'accueil, Flyer, affiches, etc.). Cette information contribue à un **traitement loyal** des données traitées et permet d'instaurer une relation de confiance.

Le CHU de Montpellier cartographie, documente et suit les traitements des données personnelles réalisés au sein de l'établissement (registre des traitements, analyses d'impact sur la protection des données, encadrement des transferts de données, etc.).

Il met en place une procédure pour gérer les demandes de droits (Procédure d'Exercice des droits). Ceci lui permet de démontrer son engagement en matière de conformité dans le domaine de la protection des données **(accountability).**

Le CHU de Montpellier s'engage à intégrer la protection des données personnelles dès la conception de tout projet, service ou outil lié au traitement des données personnelles, conformément au concept de **« protection des données dès la conception et par défaut[2] »**.

De plus, CHU de Montpellier veille à ce que les procédures respectent les principes de **minimisation des données personnelles,** de **limitation des finalités** de la collecte et de conservation imposées par le code de la santé publique (**limitation des durées de conservation**).

Le principe de l'**exactitude** et de l'**intégrité** revêt une importance primordiale lorsqu'il s'agit de données de santé, que ce soit dans le contexte des soins médicaux ou de la recherche. Ces principes sont mis en application par le biais de mesures techniques et organisationnelles pour protéger les données (politique de sécurité du système d'information, Gestion du registre des traitements et des analyses d'impact, etc.).

L'exigence de **confidentialité** imprègne chacune des démarches entreprises. Le CHU de Montpellier assure que seules les personnes autorisées aient accès aux données personnelles, tout en veillant à ce qu'elles ne divulguent pas ces informations sans autorisation, conformément aux principes de confidentialité, de respect du secret professionnel et au devoir de discrétion (politique de gestion des habilitations, comité des traces d'accès au dossier patient informatisé, etc.).

Adopter une politique de protection des données personnelles n'est pas uniquement une obligation réglementaire. Elle s'inscrit dans :

- **But pédagogique :** expliquer les enjeux permet de mieux faire comprendre l'importance de cette politique et d'encourager son application par l'ensemble de nos collaborateurs.
- **Engagement stratégique et une démarche de responsabilité** : protéger les personnes, anticiper les risques et renforcer la conformité, créer un climat de confiance, respect de la confidentialité, etc.

[1] Règlement général sur la protection des données – RGPD, Article 6
[2] Règlement général sur la protection des données – RGPD, Article 25

5 Cadre législatif et réglementaire

La présente Politique de Protection des Données Personnelles (PPDP) de notre établissement s'inscrit dans le respect et l'application des textes légaux et réglementaires en vigueur. De plus, elle rend compte des avis, lignes directrices, décisions de l'autorité compétente en la matière et des normes internes mise en place :

- Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;
- Vu la loi n°78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Vu le code de la Santé Publique ;
- Vu le code Pénal ;
- Vu le Code Civil ;
- Vu le Code de la fonction publique ;
- Vu les Codes de la déontologie des ordres professionnels (médecin chirurgien-dentiste, pédicure-podologue, infirmier, sage-femme, masseur-kinésithérapeute, pharmacien) ;
- Vu les lignes directrices, recommandations, délibérations, décisions, référentiels, avis adopté par la CNIL ;
- Vu le lignes directrices, recommandations, bonnes pratiques du Comité européen de la protection des données (CEPD) ;
- Vu le référentiel de Certification des établissements de santé pour la qualité des soins – HAS.
- Vu les normes internes :
  - Règlement intérieur
  - Politique de Sécurité du Système d'Information
  - Charte des bons usages du Système d'Information

Toute évolution législative entraînera une mise à jour de la présente Politique.

6 Responsabilités

L'activité de notre établissement génère quotidiennement des centaines de circuits de données, entre différentes applications. **Le CHU de Montpellier, en qualité de « responsable du traitement des données personnelles »,** est donc tenu à diverses obligations prévues par le RGPD et doit être en mesure de démontrer, à tout moment, sa conformité à ce règlement en retraçant toutes les démarches entreprises :

- Collecter des données personnelles uniquement nécessaires à des finalités déterminées ;
- Informer de manière transparente les personnes concernées, organiser, faciliter et respecter leurs droits et le respect de leur vie privée ;
- Fixer des durées de conservations des données personnelles ;
- Mettre en place des mesures relatives à la traçabilité des traitement effectués (registre de traitement) et évaluer les risques engendrés par le traitement (analyse d'impact) ;
- Sécuriser et protéger les données personnelles (mesures techniques et organisationnelles) ;

- Désigner un délégué à la protection des données (DPO) à la CNIL[3] ;
- etc.

La Directrice Générale, en tant que responsable légal de l'établissement, représente l'établissement dans sa qualité de « Responsable de traitement » des données personnelles. Dans ce cadre, elle est tenue de s'assurer et être en mesure de démontrer que les traitements sont effectués conformément à la présente Politique de Protection des Données Personnelles. **Elle veille donc avec l'appui du DPO, à son application par l'ensemble des collaborateurs qui accèdent et traitent des données personnelles.**

Tout collaborateur accédant ou traitant des données personnelles s'engage à :

- **Respecter les règles de cette Politique** ;
- **Garder une confidentialité absolue ;**
- **Ne pas détourner l'usage des données à des fins personnelles ou non autorisées ;**
- **Signaler toute violation ou risque.**

Tout collaborateur s'engage à en prendre connaissance et à en relire régulièrement les dispositions, si nécessaire. **Cette politique est applicable et opposable à toute personne accédant et traitant des données personnelles tenues par notre établissement. Tout non-respect de cette politique est constitutif de faute, ce que la personne reconnait et accepte**. Tout acte qui serait non conforme à la présente sera présumé avoir été accompli par la personne identifié, sauf à ce que cette dernière en apporte la preuve du contraire.

La Direction générale veille donc à ce que le CHU de Montpellier respecte scrupuleusement les lois et réglementations en vigueur avec l'appui de la Direction des Affaires juridiques et internationales (DAJ). La DAJ permet d'identifier les opportunités et les risques juridiques. Elle a donc un rôle essentiel pour assurer la conformité légale des activités et protéger les intérêts de notre établissement.

Le non-respect de cette Politique peut donc entraîner des sanctions et des recours, ainsi qu'un préjudice pour notre établissement et les personnes concernées.

7 Principes fondamentaux à respecter

Tout collaborateur (interne et externe) accédant ou traitant des données personnelles doit respecter les principes suivants :

7.1. Licéité et finalité du traitement

- Le **traitement doit être autorisé par la loi** (reposer sur une base légale) ;
- Les données doivent être collectées uniquement pour des **finalités légitimes, déterminées et explicites** ;

7.2. Loyauté, transparence

Les personnes concernées doivent être informées de manière clair et transparente **sur l'utilisation de leur données personnelles et les droits associés.**

7.3. Minimisation des données personnelles

Ne collecter que les **données strictement nécessaires** à la finalité du traitement.

[3] Règlement général sur la protection des données – RGPD, Article 37

7.4. Exactitude et mise à jour

- S'assurer que les données sont **exactes, complètes et à jour** ;
- Corriger ou supprimer toute information inexacte, si nécessaire.

7.5. Sécurité et confidentialité

- Prendre toutes les précautions nécessaires pour **protéger les données contre tout accès non autorisé, perte ou divulgation** ;
- **Avoir une vigilance accrue avec les données sensibles** telles que les données de santé ;
- **Documenter les incidents sur des données personnelles.**

Notre établissement met en place des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque (mots de passe, antivirus, pare-feu, accès restreint aux fichiers contenant des données personnelles, etc.).

7.6. Limitation de la conservation

- Conserver les données **uniquement pendant la durée strictement nécessaire à la finalité** de leur traitement, sauf obligation légale de conservation plus longue ;
- Supprimer ou rendre les données anonymes/anonymisées lorsqu'elles ne sont plus nécessaires.

8 Les Bonnes pratiques à adopter au quotidien

L'ensemble des collaborateurs (interne et externe) sont responsables, en tout lieu, de l'usage qu'ils font du système d'information mis à leur disposition par le CHU de Montpellier. Chacun a une obligation de réserve, de devoir de discrétion et de confidentialité à l'égard des données confidentielles auxquelles il accède. Cette obligation implique le respect du secret professionnel, de la déontologie et de la protection des données à caractère personnel. Pour toute question ou de doute sur la protection des données, ils peuvent se rapprocher du DPO du CHU de Montpellier.

8.1. Pour tous les collaborateurs internes

- **Ne pas partager ses identifiants** (mot de passe ou badge) ou **sa session ;**
- **Ne pas utiliser ces codes d'accès pour accéder à d'autres applications ou d'autres données que celles strictement nécessaires à l'exercice des missions confiées ;**
- **Ne pas user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur ;**
- **Ne jamais laisser trainer des documents contenant des données personnelles** (bureau, imprimante, etc.) ;
- **Ne pas divulguer, reproduire, transmettre ou utiliser les données confidentielles pour des fins personnelles** ou **étrangères à l'objectif initial de leur collecte** ou **à l'extérieur de notre établissement sans autorisation explicite** (signature d'un contrat ou d'un accord de confidentialité si nécessaire) ;
- **Ne pas stocker de données personnelles** sur des supports non sécurisés (clé USB personnelle, cloud non autorisé, etc.) ;
- **Ne pas partager des données personnelles en dehors l'équipe de soins sans l'autorisation préalable de la personne concernée** ;

- **Ne pas traiter des données personnelles d'une manière incompatible avec les finalités pour lesquelles elles ont été recueillies (**s'assurer de l'existence d'un lien entre les finalités initiales de la collecte des données personnelles et les finalités envisagées ultérieurement).

- **Utiliser des mots de passe complexes ;**
- **Verrouiller sa session** lors de chaque absence, même courte ;
- **Consulter les données personnelles conformément aux missions confiées.** La consultation hors de ce cas sera qualifié d'illégitime et sera sanctionné **;**
- **Respecter la confidentialité, le devoir de discrétion et le secret professionnel** ;
- **Transmettre des données qu'aux personnes autorisées et vérifier les destinataires** avant d'envoyer un email ou un fichier contenant des données personnelles et **ne jamais envoyer de données sensibles non chiffrées par email (**utiliser une messagerie sécurisée**)** ;
- **Utiliser des systèmes sécurisés pour le partage de fichiers autorisés par le CHU de Montpellier** ;
- **Supprimer les fichiers contenant des données personnelles dès qu'ils ne sont plus utiles ;**
- **Suivre les règles d'archivage sécurisées** (armoires fermées à clé pour les documents papier, etc.) ;
- **Prévenir tout comportement à risque** (sécurité ou violation) impliquant des données personnelles ;
- **Informer immédiatement tout comportement à risque et signaler toute anomalie** (email suspect, perte de matériel, accès non autorisé, etc.) au service dédié (Securite-Informatique@chu-montpellier.fr) et au DPO dans le cadre d'un incident sur des données personnelles (dpo@chu-montpellier.fr) ;
- **En cas de cessation de fonctions, restituer intégralement les données, fichiers informatiques et tous supports d'information relatifs aux données ou informations** ainsi que tous documents, codes, moyens d'accès, ou matériels et **ne pas en conserver de copie** sous quelque forme que ce soit. ;
- **Respecter la confidentialité même après la fin de la relation de travail.**

Le collaborateur est **le premier maillon de la chaîne de traitement des données personnelles**. Chacun, à son niveau, contribue à la sécurité et à la confidentialité des données, et du respect de la vie privée par sa vigilance et l'application au quotidien des mesures mises en œuvre dans le cadre de la PSSI et de la présente Politique. En effet, la capacité de protection et de réaction est souvent déterminante.

8.2. Pour les managers d'équipe du CHU de Montpellier

- **Appliquer les bonnes pratiques de protection des données personnelles** dans la gestion de l'équipe ;
- **Sensibiliser et accompagner** ses équipes aux risques et aux bonnes pratiques ;
- **Relayer les règles et la culture de sécurité, de protection des données, de confidentialité et du respect de la vie privée** ;
- **Être vigilant sur les traitements réalisés** par ses équipes **;**
- **Prévenir tout comportement à risque** (sécurité ou violation) impliquant des données personnelles ;
- **Informer immédiatement tout comportement à risque et signaler les anomalies** (email suspect, perte de matériel, accès non autorisé, etc.) au service dédié (Securite-Informatique@chu-montpellier.fr) et au DPO dans le cadre d'un incident sur des données personnelles (dpo@chu-montpellier.fr).

Le manager est un **acteur de terrain**, un **relais opérationnel** et un **ambassadeur de la présente politique** pour ses équipes.

8.3. Pour les collaborateurs externes (partenaires, prestataires, sous-traitant, etc.)

- **Respecter les règles internes** du CHU de Montpellier **(**PSSI, PPDP, etc.) **;**
- **Respecter les clauses** relatives à la protection des données mises en place ;
- **Ne pas réutiliser les données** en dehors du cadre prévu par le contrat ou tout acte juridique ;
- **Respecter la confidentialité des données personnelles traitées ;**
- **Utiliser les outils et accès fournis de manière responsable ;**
- **Informer immédiatement tout comportement à risque** (sécurité ou violation) impliquant des données personnelles partagées **et signaler toute anomalie** (email suspect, perte de matériel, accès non autorisé, etc.) au service dédié (Securite-Informatique@chu-montpellier.fr) et au DPO dans le cadre d'un incident sur des données personnelles (dpo@chu-montpellier.fr).
- **Agir en partenaire de confiance** (professionnalisme, discrétion, collaborer activement à la conformité RGPD, respecter l'image et les valeurs de notre établissement en matière d'éthique numérique, etc.).

Les collaborateurs externes jouent un rôle tout aussi **important** que les collaborateurs internes **dans l'application de la présente Politique**. Il est soumis aux mêmes obligations que les collaborateurs internes et doit adopter une posture responsable tout au long des missions confiées par le CHU de Montpellier.

9 Devoir de signalement des incidents sur les données personnelles

Tout collaborateur doit signaler immédiatement ou au maximum dans les 24H au DPO du CHU de Montpellier tout :

- Perte ou vol de matériel contenant des données personnelles (ordinateur, clé USB, etc.) ;
- Envoi par erreur d'un e-mail à un mauvais destinataire contenant des données personnelles ;
- Accès non autorisé à des données personnelles ou suspicion d'intrusion ;
- Comportement suspect lié au traitement de données personnelles.

En effet, notre établissement a l'obligation de documenter l'incident de violation des données personnelles (nature de la violation, nombre approximatif de personnes concernées, nombre approximatif d'enregistrements de données à caractère personnel concernés, conséquences probables de la violation de données, mesures prises ou envisagées, etc.). Si la violation constitue un risque au regard de la vie privée des personnes concernées, le CHU de Montpellier est dans l'obligation de notifier l'incident à la CNIL sous 72H. Lorsque la violation est suffisamment grave pour porter atteinte à la vie privée, les personnes concernées doivent être informées par notre établissement de la violation de leurs données personnelles dans les meilleurs délais.

10 Information et droits des personnes concernées par le traitement de leurs données personnelles

Le CHU de Montpellier informe de manière claire, concise et transparente toutes les personnes du traitement de leurs données personnelles conforment aux dispositions prévues aux articles 13 et suivants du RGPD :

- Usagers ;
- Collaborateurs internes (salariés, stagiaires, etc.) ;
- Collaborateurs externes (prestataires, partenaires, sous-traitant, etc.) ;
- Etc.

L'information ainsi que celles liées à l'exercice des droits sont précisées sur :

- Les livrets d'accueil / flyers des usagers / affiches / documents d'information individuelle obligatoires dans certains cas en application de la réglementation (élaboration du projet de soin, entrepôt de données de santé, projet de recherche, etc.) ;
- Support de communication en ligne (portail patient, site internet et intranet, etc.) ;
- Dans le document de contractualisation avec les collaborateurs externe ;
- Etc.

NB : Le consentement des personnes n'est pas systématiquement recueilli sauf dans les cas encadrés par des dispositions légales spécifiques (partage d'information, projet de recherche, cookies non essentiels, prospection commerciale, etc.).

Toute personne concernée par le traitement de ses données personnelles peut exercer son droit :

- **D'accès** (obtenir la communication de son dossier pour en vérifier le contenu et connaître le traitement dont font l'objet ses données personnelles) ;
- **De rectification** (demander la correction des informations inexactes ou incomplètes la concernant) ;
- **D'opposition** (s'opposer à tout moment à l'utilisation de certaines ces données) ;
- **D'effacement ou droit à l'oubli** (demander la suppression de ces données) ;
- **A la portabilité des données** (récupérer ses données dans un format lisible par machine) **;**
- **A la limitation du traitement** (suspendre l'utilisation de ses données) ;
- **A ne pas faire l'objet d'une décision automatisée** (refuser les décisions prises uniquement par des algorithmes ou des systèmes automatisés (sans intervention humaine)).

Ces droits sont applicables dans la limite de la réglementation applicable imposée au CHU de Montpellier (obligation légale, mission d'intérêt publique, etc.) **et peuvent s'exercer auprès du DPO du CHU de Montpellier**.

11 Transfert de données personnelles

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données personnelles en France, en UE et hors de l'UE ne cesse de croître.

Les transferts de données personnelles à l'extérieur de notre établissement doivent être conformes au respect de la sécurité, la protection et de la confidentialité des données personnelles.

Ces transferts doivent être encadrer en utilisant les différents outils juridiques (contrat ou tout acte juridique) permettant identifier les acteurs impliqués, leurs rôles (responsable, sous-traitant ou responsable conjoint du traitement) et les obligations de chacun en vertu du RGPD. Dans ce cadre, le CHU de Montpellier a mis en place une politique de transfert de l'information. De plus, le Comité européen de la protection des données (CEPD) a dégagé certains critères permettant de déterminer si un organisme intervient en qualité de responsable, de responsable conjoint ou de sous-traitant dans son diagramme pour l'application pratique des notions de responsable du traitement, de sous-traitant et de responsables conjoints du traitement.

Avant tout transfert au sein de notre établissement, il est donc essentiel de définir la responsabilité du CHU de Montpellier dans ce cadre (rôle et obligation).

12 Réutilisation des données personnelles

Il est possible de réutiliser certaines données personnelles collectées initialement pour d'autres finalités **si la réutilisation repose sur une base légale clairement définie**, notamment :

- ✓ **Le consentement explicite de la personne concernée**, lorsque cela est requis (recherche, etc.) ;
- ✓ **L'exécution d'une mission d'intérêt public ou obligation légale** (planification ou évaluation des politiques de santé publique, amélioration de la qualité des soins, réutilisations imposées par les autorités sanitaires, etc.) ;
- ✓ **Intérêt légitime de l'établissement** (améliorer l'organisation des soins et la gestion des ressources internes, etc.), sous réserve de ne pas porter atteinte aux droits et libertés des personnes.

Toute réutilisation doit être encadrée, documentée et conforme au RGPD et à la LIL, ainsi aux dispositions spécifiques applicables au secteur public de la santé et garantir le respect des droits des personnes concernées (nouvelle information et son consentement obtenu si requis par la loi). Toute réutilisation fait l'objet d'une évaluation préalable des risques pour la vie privée et **est soumise à l'approbation du CHU de Montpellier.**

Il est interdit :

- De réutiliser les données personnelles à des fins commerciales ;
- Aucune communication ou publication de données identifiantes.

Dans le cadre de réutilisations de données à des fins de recherche scientifique, médicale ou en santé publique, il faut informer la Direction de la Recherche et d'Innovation au service dédié (accueil-recherche@chu-montpellier.fr) afin de respecter les procédures réglementaires applicables (avis d'un comité d'éthique, autorisation de la CNIL si nécessaire, etc.).

13 Délégué à la Protection des données (DPO)

Le DPO du CHU de Montpellier est le « Chef d'orchestre » de la conformité en matière de protection des données, en étroite collaboration avec la Direction du Numérique en Santé et Cyber sécurité (DNS), le pilote du Système de Management de la Sécurité de l'Information (SMSI) et le Responsable de la Sécurité du Système d'Information (RSSI). Il effectue ses missions en toute indépendance et sans conflit d'intérêts.

Le DPO doit donc être impliqué dans toutes les questions relatives à la protection des données mise en place au sein de l'établissement. Il n'est pas tenu comme responsable en cas de non-respect du RGPD et il rend compte de son activité à la Direction Générale. **Il conseille sur le contenu et la mise en œuvre de l'information auprès des personnes** concernées par le traitement de leurs données personnelles **et il est le garant de l'application de l'exercice des droits.**

En cas de question ou de doute, vous pouvez contacter :
Délégué à la Protection des Données (DPO)
Centre Administratif André Bénech
191 avenue Doyen Gaston Giraud, 34295 MONTPELLIER CEDEX 5
dpo@chu-montpellier.fr
04 67 33 54 50

14 Information et Sensibilisation des collaborateurs

Des actions d'information et de sensibilisation sont régulièrement organisées pour vous aider à **comprendre pourquoi la protection des données personnelles est essentielle au sein de notre établissement** et ainsi maintenir un niveau élevé de conformité RGPD**.** Elles vous expliquent les enjeux, les raisons de notre engagement, et en quoi chacun d'entre nous est concerné.

Chaque collaborateur est responsable de :
- Se tenir informé des règles en vigueur ;
- Participer aux sensibilisations mise en place ;
- Appliquer les consignes dans sa pratique quotidienne.

Notre établissement met également à la disposition de ces collaborateurs internes une formation proposée par le GRADeS e-santé Occitanie permettant de s'exercer et de renforcer ses connaissances en cybersécurité et protection des données.

La sensibilisation et la formation sur les bonnes pratiques sont essentielles pour réduire les risques d'attaques (rançongiciels, etc.) et les violations de données personnelles.

15 Sanctions et Recours

En cas de manquement avéré à la présente PPDP, des sanctions proportionnelles à la gravité de la faute pourront être appliquées, conformément aux règles internes du CHU de Montpellier et à la réglementation en vigueur. **Le CHU de Montpellier ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un collaborateur qui ne se sera pas conformé aux règles décrites dans la présente PPDP.**

15.1. Sanctions internes

1- Pour tous les collaborateurs internes
- **Avertissement écrit** pour les manquements mineurs ou les négligences ;
- **Sanctions disciplinaires** pouvant aller jusqu'au licenciement pour faute grave en cas de violation grave ou répétée (accès non autorisé à des données personnelles, divulgation ou utilisation frauduleuse de données, notamment, non-respect des procédures de sécurité ou de signalement d'incidents sur les données personnelles, etc.).

2- Pour les collaborateurs externes (partenaires, prestataires, sous-traitant, etc.)

- **Résiliation du contrat** pour manquement grave ou non-respect des clauses de protection des données ;
- **Exclusion des appels d'offres futurs** en cas de violation répétée ou de non-coopération lors d'un incident ;
- **Pénalités financières si prévues contractuellement**, notamment en cas de non-respect des délais de signalement d'une violation de données.

15.2. Sanctions administratives et pénales

La Loi prévoit des poursuites pénales pour les infractions les plus graves (atteinte à la vie privée[4], accès ou maintien frauduleux dans un système de traitement automatisé de données[5]), destruction, altération ou divulgation non autorisée de données[6]).

Les peines encourues peuvent aller jusqu'à **5 ans d'emprisonnement et 300 000 € d'amende pour les personnes physiques,** et jusqu'à **1 500 000 € pour les personnes morales.**

15.3. Recours des personnes concernées

Toute personne (usager, collaborateur, etc.) estimant que ses droits en matière de protection des données n'ont pas été respectés dispose des recours suivants :

1-Recours interne

- **Réclamation auprès du DPO** ;
- **Demande de médiation interne** pour tenter de résoudre le litige à l'amiable.

2- Recours externe

- Saisir **la Commission Nationale de l'Informatique et des Libertés** (CNIL) pour faire une réclamation. La CNIL est chargée de surveiller l'application des règles relatives à la protection des données (https://www.cnil.fr/plaintes ou CNIL - Service des Plaintes - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07). **La CNIL peut mener une enquête et, le cas échéant, prononcer des sanctions à l'encontre de l'établissement.**
- **Action en justice** : La personne concernée peut saisir les tribunaux compétents pour faire valoir ses droits et obtenir réparation (dommages et intérêts, injonction de faire ou de ne pas faire, etc.).

16 Mise à jour et Révision de la PPDP

Cette politique respecte le processus de gestion documentaire mis en œuvre au CHU de Montpellier, au travers du logiciel Qualidoc, sous la responsabilité de la Direction Qualité, Sécurité des Soins et Partenariat en Santé selon la procédure de gestion des documents à caractère transversaux.

La Politique de Protection des Données Personnelles est diffusée à l'ensemble des professionnels concernés par sa mise en application.

[4] Article 226-1 et suivants du code pénal
[5] Article 323-1 et suivants du code pénal
[6] Article 323-3 du code pénal

Elle est révisée régulièrement pour être en conformité avec la réglementation et refléter les évolutions de la technologie, tout en prenant en compte du principe d'amélioration continue.

17 Annexe

Annexe 1 – Supports internes liés à la PPDP

- Gestion du Registre de traitement et des analyses d'impact (AIPD) du CHU de Montpellier.
- Note d'information sur le traitement des données personnelles des usagers et des collaborateurs internes et externes du CHU de Montpellier.
- Procédure d'exercice des droits de la personne concernées par le traitement de leurs données.
- Gestion des demandes d'analyse des traces d'accès au dossier patient informatisé.
- Gestion des violations de données personnelles.
- Procédure de traitement des données des données personnelles par les collaborateurs externes.
- Politique de Gestion des Habilitations.
- Politique de Gestion des Incidents de sécurité du Système d'Information.

Annexe 2 - Définitions

Accountability : Obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Analyse d'impact (AIPD) sur la protection des données : Etude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. L'AIPD se décompose en trois parties : une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels, l'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques et l'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Base légale d'un traitement : Ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de collecter ou d'utiliser des données personnelles.
On peut également parler de « **fondement juridique** » ou de « **base juridique** » du traitement.
Six bases légales sont prévues par le RGPD :

- Le consentement ;
- Le contrat ;
- L'obligation légale ;
- La sauvegarde des intérêts vitaux ;
- L'intérêt public ;
- Les intérêts légitimes.

Confidentialité : Définie par l'Organisation internationale de normalisation (ISO) comme « le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé ». Elle s'articule autour de deux éléments :

- D'une part, le droit à la protection de la vie privée, afin d'empêcher la divulgation de tout ce qui pourrait permettre d'identifier les personnes ;
- D'autre part, le devoir de discrétion et le secret professionnel incombant aux professionnels.

Consentement : Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Devoir de discrétion : Obligation de ne pas divulguer les informations concernant l'activité, les missions et le fonctionnement de la structure dans laquelle on exerce une activité.

Donnée à caractère personnel (Données personnelles) : Toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.
Il s'agit de l'ensemble des données collectées et produites dans le cadre du parcours de soins au sein du CHU de Montpellier qu'elle soit recueillie directement ou indirectement et/ou conservée en dossier patient

(papier et/ou informatisé). Mais aussi, des données personnelles de nos professionnels, des personnels intervenant au sein de notre établissement, des collaborateurs, prestataires, etc.

Donnée à caractère personnel concernant la santé : Données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique, qui révèlent des informations sur l'état de santé de cette personne. Cela comprend notamment :

- Les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de services (numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé) ;
- Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;
- Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédicale de la personne concernée.

Donnée à caractère personnel sensible : Catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Données anonymes/anonymisées : Informations agrégées ou toute information obtenue par suppression de toutes les indications permettant, directement ou non, l'identification d'une personne (usager ou collaborateur). L'anonymisation est donc un traitement de données qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible.

Données confidentielles : Toutes informations et données de toute nature, notamment à caractère personnel, technique, scientifique, économique, financière, comptable, étude, prototype, matériel, audit, données expérimentales et de tests, spécifications, savoir-faire, expérience, logiciels et programmes, quels qu'en soient la forme, le support ou le moyen, incluant, sans limitation, les communications orales, écrites ou fixées sur un support quelconque, ainsi que tout document, information, fichier, création liés à l'activité d'une entreprise. Ces données peuvent par exemple correspondre à des données sensibles au sens du RGPD, des données de santé, des données de recherche ou des données spécifiques telles que les alertes sanitaires et épidémiologiques.

Dossier patient (Dossier médical) : Traitement des données à caractère personnelles collectées à l'occasion d'une prise en charge sanitaire, médico-sociale ou des activités nécessaires à la coordination de ces prises en charge. Le terme dossier patient informatisé (DPI) renvoie aux traitements mis en œuvre sur support numérique.

Données pseudonymisées : Informations qui ne peuvent plus être rattachées à un individu sans être recoupées avec d'autres informations, qui sont conservées séparément. La pseudonymisation est le

traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Dossier ressources humaines : Traitement des données à caractère personnelles collectées à l'occasion des recrutements et pour la gestion des professionnels.

Droit au respect de la vie privée : Elément juridique qui vise à protéger le respect de la vie privée des individus. La vie privée renvoie à la sphère personnelle d'un individu, celle qui est protégée des regards indiscrets et qui concerne son intimité. Le droit au respect de la vie privée implique :

- Le respect de l'intimité, du secret médical, du droit à l'image, etc. ;
- Des limites aux pratiques d'espionnage et d'enquête (comme les écoutes téléphoniques) ;
- La mise en place de nouvelles règles et instances visant à limiter les risques liés au développement des outils numériques.

Finalité d'un traitement : Objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial. Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur.

Loi Informatique et Libertés (LIL) - Officiellement loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) : Loi française qui réglemente le traitement des données personnelles. La LIL est destinée à garantir la protection de la vie privée des citoyens face aux moyens de traitement automatisés de données numériques. La LIL a amené à la création de Commission nationale de l'informatique et des libertés (CNIL). Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. La CNIL est une autorité administrative indépendante (AAI), c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

Partage et échange d'informations : Notion qui permet à des professionnels de partager entre eux des informations couvertes par le secret professionnel dans le but d'assurer la qualité et la continuité des soins d'un usager dans le respect de ses droits et la confidentialité de leurs données. Le partage d'informations nécessaires à la prise en charge d'un usager entre des professionnels ne faisant pas partie de la même équipe de soins, requiert en revanche son accord préalable et doit être tracé dans son dossier médical.

Politique de Sécurité du Système d'Information (PSSI) : Plan d'action défini pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, État, union d'États…) en matière de sécurité des systèmes d'information (SSI).

La PSSI du CHU de Montpellier définit les enjeux de la sécurisation du système d'information (SI) et établit les règles de sécurité nécessaires. C'est un document essentiel, validé par la direction, qui doit être respecté par tous les utilisateurs du SI.

Registre des activités de traitement : Ce qui permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier :
- les parties prenantes ;
- les catégories de données traitées ;
- à quoi servent ces données, qui y accède et à qui elles sont communiquées ;
- combien de temps les données personnelles sont conservées ;
- comment elles sont sécurisées.

Règlement Général sur la Protection des Données (RGPD) - Officiellement appelé règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : Règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Responsable du traitement (RT) : Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Responsable conjoint du traitement : Lorsque deux responsables du traitement, ou plus, déterminent ensemble les finalités et les moyens du traitement, ils sont responsables conjoints du traitement.
Cette responsabilité conjointe peut se traduire par :
- Une décision prise en commun ;
- Ou des décisions séparées mais complémentaires, qui aboutissent à un traitement commun.

Secret professionnel (secret médical) : Implique l'interdiction de divulguer, hors cas de dérogation légale, des données à caractère personnel (privées ou professionnelles, situations financière et sociale, données de santé, etc.) dont le professionnel a pu avoir connaissance que ce soit durant ses heures de service ou en dehors de celles-ci. Il couvre tout ce qui est venu à la connaissance des professionnels, qu'ils l'aient vu, lu, entendu ou compris. Ni l'accord de la personne ni son décès ne délivrent de l'obligation au secret. Le seul à qui le secret n'est pas opposable est la personne concernée elle-même.

Sécurité des systèmes d'information (SSI) : Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais

usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Sous-traitant (ST) : Personne physique ou morale (entreprise ou organisme public) qui traite des données pour le compte d'un autre organisme (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation.
Les sous-traitants ont des obligations concernant les données personnelles, qui doivent être présentes dans le contrat/convention avec la Responsable de traitement :

- Une obligation de transparence et de traçabilité ;
- La prise en compte des principes de protection des données dès la conception et par défaut ;
- Une obligation de garantir la sécurité des données traitées ;
- Une obligation d'assistance, d'alerte et de conseil (par exemple, une procédure de notification des violations de données personnelles doit être notifiée).

Système d'information (SI) : Système d'information recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par le CHU de Montpellier ou par des tiers au service de ces utilisateurs. Il est aussi constitué des dispositifs numériques nomades connectés au SI du CHU de Montpellier.

Système de management du système d'information (SMSI) : Ensemble de politiques visant la gestion de la sécurité de l'information. Le SMSI vise à identifier, évaluer, traiter et surveiller les risques liés à l'information, qu'elle soit stockée sur un serveur, en transit sur un réseau ou manipulée par des collaborateurs. Son périmètre peut couvrir des systèmes d'information, des bases de données RH, des secrets industriels, des services cloud ou encore des processus métiers stratégiques. Cette approche globale permet de protéger aussi bien les actifs techniques que les ressources humaines et organisationnelles.

Traitement : Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Transfert de données : Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Violation de données : une violation de la sécurité entraînante, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles. Les obligations des responsables du traitement concernant les violations de données

personnelles, et notamment leur notification à la CNIL et aux personnes concernées, sont prévues dans le RGPD.

Annexe 3 – Abréviations

CHU	Centre Hospitalier Universitaire
CNIL	Commission Nationale de l'Informatique et des Libertés
DACQSS-PU	Direction Qualité, Sécurité des Soins et Partenariat Usagers
DNS	Direction du Numérique en Santé et Cyber sécurité
DAJ	Direction des Affaires juridiques et internationales
DPD/DPO	Délégué à la Protection des Données (« Data Protection Officer »)
EIG	Evénements indésirables graves
IQSS	Indicateurs de Qualité et de Sécurité des Soins
LIL	Loi Informatique et Liberté
PPDP	Politique de Protection des Données Personnelles
PSSI	Politique de Sécurité du Système d'Information
RGPD	Règlement Général sur la Protection des Données Personnelles (Règlement (UE) n°2016/679)
RSSI	Responsable de la Sécurité de Système d'Information
RT	Responsable de Traitement
SI	Système d'Information
SMSI	Système de Management de la Sécurité de l'Information
ST	Sous-Traitant
UE	Union Européenne