Prorogé le 19/09/2022

Règlement de Confidentialité du CHU de Montpellier	**Document n°** CHRU/ 10.c/004/v4
	Page : 1/9
	Document(s) de référence :

Rédaction: BARBOTTE ERIC	**Vérification:** GARNIER EMMANUELLE, VALENTIN VIRGINIE **Vérification par DQGR**	**Approbation:** LE LUDEC THOMAS, BISMUTH MICHAEL **Date d'approbation : 03/09/2019 09:42:00**
Groupe de travail éventuel : MENEROUD MARIELLE, CUDENNEC AUDE, REQUENA-LAPARRA MARIE HELENE, HORVATH MARIA, YRIARTE CECILE, BOURGUE LAURENT, TEMPLIER VINCENT, EUVRARD JEROME, GANDIN GREGORY, RUBENOVITCH JOSH		

DESTINATAIRES

CHU-Hors-BALF Groupe réservé	Tout le personnel CHU (groupe CHU)

Cycle de vie du document

Version	Date d'application	Modifications/ Révisions
Version en cours	03/09/2019 09:42:00	Création

Article 1
PRINCIPES GENERAUX

1.1. Les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent (Article L1112-1-III du Code de la Santé Publique) et qu'ils emploient (article 9 du Code Civil).

Secret Professionnel

1.2. Le Secret Professionnel, incluant le Secret Médical, est institué dans l'intérêt des patients, des personnes accueillies et des professionnels exerçant au Centre Hospitalier Universitaire (CHU), il s'impose à tous les personnels travaillant pour le compte du CHU. Sa finalité est la protection de l'intimité et de la vie privée. Il couvre l'ensemble des informations venues à la connaissance des personnels travaillant pour le compte du CHU,

- par quelque mode que ce soit et notamment les moyens de communication numériques,
- que ces agents soient dépositaires d'une information par état, profession, fonction ou mission temporaire.

Ni l'accord du patient ni son décès ne délivrent le professionnel de son obligation au secret.

1.3. Toute personne physique ou morale exerçant une fonction pour le compte du CHU est soumise à ce règlement. Elle est appelée « utilisateur » dans l'ensemble de ce document.

1.4. Le Secret Professionnel s'impose à chaque utilisateur. Il implique l'interdiction de divulguer, hors cas de dérogation légale, des informations à caractère personnel dont l'utilisateur a pu avoir connaissance que ce soit durant ses heures de service ou en dehors de celles-ci.

1.5. L'utilisateur ne peut avoir accès, dans les limites de ses compétences, qu'aux informations strictement nécessaires à l'accomplissement de ses missions. Il doit protéger contre toute indiscrétion les informations et les documents qui lui ont été confiés.

1.6. Afin d'assurer la continuité de service et d'améliorer sa qualité, dans l'intérêt des patients et des professionnels, le partage de l'information entre utilisateurs peut être nécessaire. Les échanges doivent se limiter aux données nécessaires, pertinentes et non excessives, en rapport direct avec le domaine d'intervention de chaque professionnel, chacun d'entre eux étant tenu au respect du secret professionnel. La personne est dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant. Elle peut exercer ce droit à tout moment (Article L1110-4-IV du Code de la Santé Publique, Règlement Européen Général de Protection des Données (RGPD), loi n°78-17 du 6 janvier 1978 modifiée).

Article 2
Systèmes d'Information & Données

Système d'Information

2.1. Il est mis en place au sein du CHU un Système d'Information Hospitalier (SIH). Le SIH a pour but de faciliter, en l'automatisant, la gestion des informations et leur partage entre les utilisateurs lorsque ces informations relèvent de leur compétence.
Tous les traitements de données à caractère personnel font l'objet de procédures mentionnant :

- la nature des données transmises,
- la finalité du traitement des données,
- les personnes physiques ou morales destinataires des données,
- le droit d'accès, de rectification et de suppression des données,
- le droit d'opposition,
- la durée de conservation des données,
- la catégorie des données.

Ces traitements sont soumis à l'avis du Délégué à la Protection des Données (DPO) dans le cadre du RGPD. Ils sont répertoriés dans le registre prévu par le RGPD.

2.2. Le SIH repose physiquement sur un réseau mettant en communication un ensemble d'ordinateurs. Tout ordinateur faisant partie du réseau est identifié logiquement (adresse IP sur le réseau). Lorsque le réseau

emprunte des réseaux publics, les données personnelles de santé issues du SIH y transitant sont cryptées (article L 1110-4-1 du Code de la Santé Publique).

2.3. Le SIH conserve l'historique des accès de chaque utilisateur. Ce système de contrôle et de traçabilité des accès doit enregistrer tout accès au système d'information hospitalier avec ses dates et heures de début et de fin de session, les identifiants du professionnel et de la machine, ainsi que les actions réalisées.

Typologie des Données

2.4. Le SIH véhicule et gère des informations à caractère personnel directement identifiantes et des informations anonymes, anonymisées, pseudonymisées nécessaires au bon fonctionnement et à la gestion de l'établissement.

Informations à caractère personnel

2.5. Constitue une information à caractère personnel toute information relative à une personne identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Notamment, sont à caractère personnel :

- Toutes les informations du dossier du patient ou de l'agent,
- Les Résumés de Sortie du PMSI,
- Tout ensemble de données obtenu par requête et au sein duquel il est possible d'accéder, même indirectement, à l'identité d'au moins un patient ou un agent.

2.6. Une information à caractère personnel dans le SIH est définie par :

- Un Identifiant Permanent du Patient (IPP) ou de l'agent (matricule) ou un ensemble d'informations permettant son identification,
- Un auteur de l'information (professionnel, service, unité fonctionnelle ou département).

2.7. Afin de regrouper les informations, il est défini pour chaque patient ou agent un dossier informatisé ou matérialisé dont le but est la communication rapide de données utiles à la prise en charge du patient ou le suivi et la gestion de la carrière de l'agent

Le dossier informatisé :

- Regroupe des informations à caractère personnel du patient ou de l'agent,
- Est ouvert à tous les professionnels participant à la prise en charge du patient, de l'agent ou de leur dossier, selon des modes d'accès particuliers définis dans les textes d'application de ce règlement,
- Est disponible sur le SIH.

Tout personnel :

- Ne doit consulter le dossier que pour les besoins de la prise en charge du patient ou la gestion de l'agent et dans son seul intérêt,
- Doit protéger contre toute indiscrétion les documents concernant les personnes prises en charge ou les professionnels, quels que soient le contenu et le support de ces documents,
- Est averti qu'une trace est gardée de toutes ses consultations du dossier informatisé.

2.8. En dehors des cas où la loi oblige l'établissement à exploiter des données à caractère personnel,

- La personne concernée peut s'opposer au recueil et à l'utilisation de ces données.
- Elle peut retirer son consentement ou demander la suppression ou la limitation de leur recueil ou de leur utilisation ;
- Aucune information à caractère personnel ne peut être transmise si la personne s'y oppose.

Les modalités de l'information ainsi que celles liées à l'exercice des droits issus du RGPD et de la loi n°78-17 du 6 janvier 1978 modifiée sont précisées :

- Dans le livret d'accueil du nouveau recruté,
- Dans le livret d'accueil patient fourni lors de chaque séjour en hospitalisation,
- Dans le livret d'accueil patient consultant fourni lors de chaque consultation,
- Dans les halls d'entrée des différents établissements du CHU par affiche,
- Dans les documents d'information individuelle obligatoires préalablement à toute mise en œuvre de traitement.

Informations anonymes, anonymisées ou pseudonymisées

2.9. Sont définies comme anonymes ou anonymisées, les informations agrégées ou toute information obtenue par suppression de toutes les indications permettant, directement ou non, l'identification du patient ou du professionnel travaillant pour le compte du CHU.

2.10. Sont définies comme pseudonymisées les informations qui ne peuvent plus être rattachées à un individu sans être recoupées avec d'autres informations, qui sont conservées séparément.

2.11. Les comptes rendus d'activité synthétiques dans lesquels les données d'état civil ont été supprimées, sont anonymisés.

2.12. Dans le cadre du PMSI, toute exploitation particulière des Résumés de Sortie Anonymes, autre que la transmission aux autorités de tutelle prévue dans le code de la Santé Publique, doit être effectuée sous contrôle médical.

2.13. Les données à caractère personnel qui font l'objet d'un traitement en vue de l'Evaluation des Pratiques Professionnelles (EPP) ne peuvent être communiquées que sous la forme de statistiques agrégées ou de données constituées de telle sorte que les personnes concernées ne puissent être identifiables.

Article 3

Accès & Exploitation des données

3.1. Le Système d'Information n'est accessible qu'aux utilisateurs autorisés, dans l'exercice de leurs missions et dans les strictes limites de leurs compétences à l'exclusion de toute autre.

A l'intérieur du CHU

3.2. La fonction et les missions de chaque utilisateur sont définies dans une fiche de poste réglementaire en lien avec la fiche métier, une fiche de mission réglementaire ou une lettre de mission. Dans ce cadre réglementaire, tout utilisateur reste seul à même d'évaluer la stricte nécessité de consulter les données personnelles. Cette consultation sera faite dans le respect des règles du secret professionnel.

3.3. Dans le cadre de la prise en charge collective des patients ou de la gestion personnelle ou collective du personnel, il peut être utile, dans leur intérêt, de permettre la consultation de données à caractère personnel à des utilisateurs autres que l'auteur ou le destinataire de ces données. Le partage de données personnelles se fait dans le respect du secret professionnel.

3.4. L'accès d'un utilisateur est limité aux données personnelles relevant de son état, sa profession, sa fonction ou ses missions, considérées comme strictement nécessaires à la meilleure efficience dans la gestion du dossier de l'agent ou la prise en charge du patient, à l'exclusion de tout autre. Cet accès est délivré au regard d'une matrice d'habilitation.

3.5. Par principe, conformément à la loi (article L1110-4 du Code de la Santé Publique) et à leur statut, les personnels non soignants ne sont pas autorisés à accéder aux données à caractère personnel relatives aux patients, quels que soient le contenu et le support de ces données.
Toutefois pour les actions relevant de leur mission et autorisées par la loi, nécessaires à la continuité du service public hospitalier, pour lesquelles l'accès aux données à caractère personnel de santé est requis, cet accès est autorisé aux agents hospitaliers chargés de ces missions et à l'exclusion de toute autre. Ces agents sont alors soumis à l'article 1.4 du présent règlement.

3.6. Par principe, conformément à la loi et à leur statut, le personnel n'assurant pas la gestion administrative du personnel n'a pas accès aux données à caractère personnel relatives à ces professionnels, quels que soient le contenu et le support de ces données.
Toutefois pour les actions relevant de leur mission, nécessaires à la continuité du service public hospitalier, pour lesquelles l'accès aux données à caractère personnel est requis, cet accès est autorisé aux agents hospitaliers chargés de ces missions et à l'exclusion de toute autre. Ces agents sont alors soumis à l'article 1.4 du présent règlement.

3.7. Dans le strict cadre du contrôle de la qualité des données du PMSI, les Techniciens d'Information Médicale (TIM) du Département de l'Information Médicale (DIM) ont accès à l'ensemble des données médicales à caractère personnel par délégation du médecin DIM (Article R6113-5 du Code de la Santé Publique).

3.8. Les traitements automatisés de données à caractère personnel dont la finalité est ou devient la recherche, les études dans le domaine de la santé, l'analyse ou l'évaluation des pratiques ou des activités de soins ou de prévention, sont soumis aux dispositions liées à la protection des données à caractère personnel et, le cas échéant, aux méthodologies de référence correspondantes.

3.9. L'utilisation des résultats de ces traitements ne peut se faire sans l'accord de la personne, physique ou morale, ayant réalisé les traitements.

3.10. Une gestion médicalisée reposant sur des données à caractère personnel plus précises que les données anonymes est indispensable pour assurer les missions de gestion de l'établissement, comme l'organisation des services de soins et de leur logistique, le suivi, la négociation et la modélisation du budget général du CHU et des budgets particuliers, le suivi de l'évolution des activités, notamment dans le cas de coopérations (réseaux de soins internes au C.H.U., réseaux ville-hôpital, réseaux de soins).
Les agents en charge de ces fonctions ont, dans le cadre de coopération d'étude et d'analyse avec le DIM, accès aux données à caractère personnel nécessaires.
La lecture de ces données doit se faire sous autorisation de la Commission des Habilitations.
S'il s'agit de données de soin, la lecture est effectuée sous le contrôle d'accès et la validation des résultats des études et analyses de ces accès par le DIM et le DPO dans le cadre de l'Autorité de Contrôle des Accès.

3.11. Dans le cadre des travaux et recherches intra hospitalières, les articles 3.13, 3.14 et 3.16 s'appliquent.

A l'extérieur du CHU

3.12. Des données médicales peuvent être transmises à l'extérieur du C.H.U dans le cas de réseaux de soins. Ces transmissions doivent se faire dans le strict cadre des Méthodes de Référence (MR) publiées par la CNIL et de la Loi 78-11 « Informatique et Liberté » modifiée. Hors cadre de référence, les transmissions sont soumises à autorisation de la CNIL.

3.13. Hors situation de soins du patient, la transmission de données médicales à des personnes physiques ou morales extérieures à l'hôpital doit :

- Faire l'objet d'un protocole écrit, préalable, précisant les données, buts poursuivis et modalités d'utilisation, adressé à l'Institutinonal Review Board (IRB) via le formulaire mis en place conjointement par l'IRB et le DIM. L'IRB et le DPO statueront sur la validité de cette demande. Ils pourront s'opposer à cette demande et formuler des recommandations en cas d'études, recherche et évaluations.
- Respecter les règles relatives au secret professionnel,
- Ne pas aller à l'encontre de l'intérêt du patient,
- Etre conforme aux formalités préalables prévues par la loi du 6 janvier 1978, aux recommandations de la CNIL et des Méthodologies de Référence (MR).

Ces données médicales, même anonymes ou anonymisées, ne pourront être utilisées à des fins de promotion ou de prospection commerciale, dès lors qu'elles sont associées à l'identification du professionnel de santé.

3.14. Les traitements automatisés de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé doivent être conformes à une Méthodologie de Référence. Toute personne a le droit de s'opposer à ce que des données nominatives la concernant fassent l'objet d'un traitement ayant pour fin la recherche dans le domaine de la santé.

3.15. La transmission vers un Etat n'appartenant pas à l'Union Européenne de données à caractère personnel faisant l'objet d'un traitement n'est autorisée que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet (RGPD).

3.16. Dans les cas où la transmission des données de santé s'effectue par moyens informatiques, seules des messageries de santé sécurisées (MSS) recourant au cryptage des données peuvent être utilisées. A défaut, il sera recouru au cryptage de la totalité des données, dans le cadre de la réglementation française et européenne en vigueur

3.17 Dans les cas où la transmission des données à caractère personnel (hors données de santé) s'effectue par moyens informatiques, celle – ci, éventuellement effectuée entre professionnels de santé ou organismes tiers, sera réalisée dans des conditions garantissant de façon effective la confidentialité des données. En particulier il sera recouru, selon leur sensibilité, au cryptage de tout ou partie des données, dans le cadre de la réglementation française et européenne en vigueur.

3.18. Sauf conditions légales particulières, un agent investi d'une mission ou d'une expertise demandée par un organisme extérieur à l'hôpital, tel que Justice, Agence Régionale de Santé, Caisse Primaire d'Assurance Maladie, Compagnie d'Assurance, … n'est plus dans l'exercice de sa fonction hospitalière. L'accès au système d'information médicale lui est interdit par principe. L'accès peut néanmoins lui être autorisé dans le strict cadre de sa mission.
Si la consultation d'informations à caractère personnel est indispensable à cette mission, elle ne pourra se faire que dans le cadre de la mission et de la réglementation correspondante.

3.19. Le SIH reposant sur des matériels informatiques dont certains sont sous télémaintenance, les contrats de maintenance ou de télémaintenance ou les contrats relatifs à des prestations extérieures devront être conformes au présent règlement et au RGPD.

3.20. Les accès des agents hospitaliers aux réseaux extérieurs (internet, DMP, DCC, réseau ville - hôpital,…) ne peuvent contrevenir à la « Charte des Bons Usages du Système d'Information ».

Article 4

Droits des Patients et des Professionnels

4.1. Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :

- de la nature des données transmises,
- de la finalité du traitement des données,
- des personnes physiques ou morales destinataires des données,
- du droit d'accès, de rectification et de suppression des données,
- du droit d'opposition,
- de la durée de conservation des données,
- de la catégorie des données.

4.2. Hors les cas où la transmission de données à caractère personnel est imposée par la loi, le consentement de la personne examinée ou soignée doit être recherché dans tous les cas. Lorsque le malade, en état d'exprimer sa volonté, refuse le stockage sur dossier numérisé des données à caractère personnel qui le concernent, demande leur anonymisation ou une admission discrète, les personnes en charge du SIH doivent respecter ce refus après avoir informé le malade des conséquences. Lorsque le patient persiste dans son refus du support numérisé, un dossier papier doit être constitué.

4.3. Le patient et le professionnel du CHU ont le droit d'obtenir confirmation que des données à caractère personnel le concernant font l'objet d'un traitement, d'obtenir des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires auxquels les données sont communiquées.

4.4. Le patient du CHU a le droit de connaitre l'identité des personnels ayant consulté son dossier.
Le professionnel du CHU a le droit de connaitre l'identité des personnels ayant consulté son dossier administratif.
Pour mettre en œuvre ce droit, ils en font la demande au DPO, qui saisit l'Autorité de Contrôle des Accès.
Cette Autorité apportera les éléments de réponse conformément à la « Procédure de vérification des traces d'accès réalisés au dossier patient informatisé » pour les patients, et à la procédure de vérification des accès aux dossiers administratifs pour le personnel.
Le DPO apportera une réponse au demandeur.
En complément, l'Autorité de Contrôle peut réaliser des contrôles de sa propre initiative.

4.5. Le patient ou le professionnel du CHU peut exiger que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel le concernant pour des raisons tenant à sa

situation particulière (RGPD et Loi 78-11 du 6 janvier 1978 modifiée). Après avis du DPO, le CHU lui apporte une réponse.

Article 5
Identification

Cette partie est décrite dans la « Charte des Bons Usages du Système d'Information ».

Article 6
Publication

6.1. Les règles de confidentialité contenues dans le Règlement de Confidentialité du CHU de Montpellier et les sanctions encourues en cas d'atteinte à la confidentialité et de détournement des fichiers sont communiquées à tous les utilisateurs.
Lors de l'attribution de son identifiant, le professionnel devra attester qu'il a pris connaissance du Règlement de Confidentialité du CHU de Montpellier et s'engager à la respecter.

6.2. Le présent Règlement est publié sur le site Intranet du CHU de Montpellier.

6.3. Il est annexé au Règlement Intérieur du CHU et s'impose à tout utilisateur.

6.4. Lors de chaque renouvellement ou de toute mise à jour du Règlement de Confidentialité du CHU de Montpellier, l'utilisateur dispose d'un délai de 30 jours pour notifier sa prise de connaissance et son engagement, période durant laquelle il est invité quotidiennement à le faire. L'utilisation du SIH est conditionnée à l'attestation de prise de connaissance et d'engagement de chaque professionnel à respecter le Règlement de Confidentialité du CHU de Montpellier.

Article 7
Sanctions

7.1. Violation du secret professionnel

La révélation d'informations à caractère secret par une personne qui en est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, hormis les cas où la loi l'impose ou l'autorise, est punie d'un an d'emprisonnement et de 15 000 euros d'amende (article 226-13 du Code Pénal).
Le délit de violation du secret professionnel est constitué dès lors que la révélation est effective, même si son objet est de notoriété publique, même si elle n'entraîne aucun préjudice pour celui qu'elle concerne, même si elle n'est pas intentionnelle.

7.2. Violation du secret professionnel à l'occasion d'un traitement de données à caractère personnel
Article 326-22 du Code Pénal
Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

7.3. Traitement de données à caractère personnel hors cadre légal

Le fait, y compris par négligence, de procéder ou faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-16 du Code Pénal).
Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement correspond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes est puni de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-18-1 du Code Pénal)
Sont interdites, sous peine de sanctions pénales, "la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés à partir de données issues directement ou indirectement des prescriptions médicales ou des informations médicales mentionnées à l'article L 161-29 du code de la sécurité sociale, dès lors que ces fichiers permettent d'identifier directement ou indirectement le professionnel prescripteur" (article L 4113-7 du Code de la Santé Publique)

7.4. Collecte indue de données à caractère personnel

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code Pénal).
Les données, même rendues anonymes à l'égard des patients, ne peuvent être utilisées à des fins de promotion ou de prospection commerciale, dès lors qu'elles sont associées à l'identification du professionnel de santé (article L4113-7 du code de la santé publique)

7.5 Accès non autorisé aux données à caractère personnel

Article 323-1 du Code Pénal
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

7.6. Détournement de la finalité du traitement de données à caractère personnel
Article 326-21 du Code Pénal
Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

7.7. Le CHU, représenté par son Directeur Général, portera à la connaissance de la justice toute violation du présent Règlement de Confidentialité du CHU de Montpellier susceptible d'être pénalement sanctionnée.

7.8. Le CHU, représenté par son Directeur Général, portera à la connaissance des instances ordinales toute violation du présent Règlement de Confidentialité du CHU de Montpellier susceptible d'être considérée comme un manquement déontologique.

7.9. Sans préjuger de la responsabilité pénale ou ordinale individuelle des professionnels, tout manquement aux règles du présent Règlement est passible de sanction disciplinaire décidée par le Directeur général selon les procédures en vigueur.

7.10. S'il est résulté de la violation du présent Règlement de Confidentialité du CHU de Montpellier un préjudice pour le patient, le professionnel ou l'établissement, le versement de dommages-intérêts peut être demandé par la victime.

LES DIX PRINCIPES DE LA CONFIDENTIALITE :

1. Le secret professionnel est une règle qui s'impose à tout agent public, pendant et en dehors du temps de travail. Je dois le respecter et le défendre.

2. Le secret professionnel couvre tout ce qui est venu à ma connaissance dans mon exercice professionnel, c'est-à-dire non seulement ce qui m'a été confié, mais aussi ce que j'ai vu, entendu ou compris concernant un patient ou un agent.

3. Quel que soient les formes ou les outils de communication (réseaux sociaux, messageries interne ou externe, communication scientifique, smartphone et autres objets connectés), je dois respecter le secret professionnel.

4. Je dois protéger les données des patients et des agents de mon établissement.

5. Je ne peux consulter ou partager avec mes collègues que les données utiles à la prise en charge des patients ou au suivi de la carrière des agents.

6. Je sais que mon utilisation du Système d'Information Hospitalier (SIH) est tracée.

7. Mon identifiant est personnel et mon mot de passe strictement confidentiel ; Je n'utilise aucun autre matricule que le mien et je ne communique jamais mon mot de passe.

8. Je dois changer régulièrement mon mot de passe.

9. Je ne dois pas utiliser mes propres matériels (smartphone, tablettes, appareils photo, etc…) pour traiter ou échanger des données concernant des patients ou agents, hors procédure validée par la Délégation à l'Usage du Numérique.

10. La violation du secret professionnel engage ma responsabilité et m'expose à des sanctions disciplinaires, ordinales, civiles et pénales.