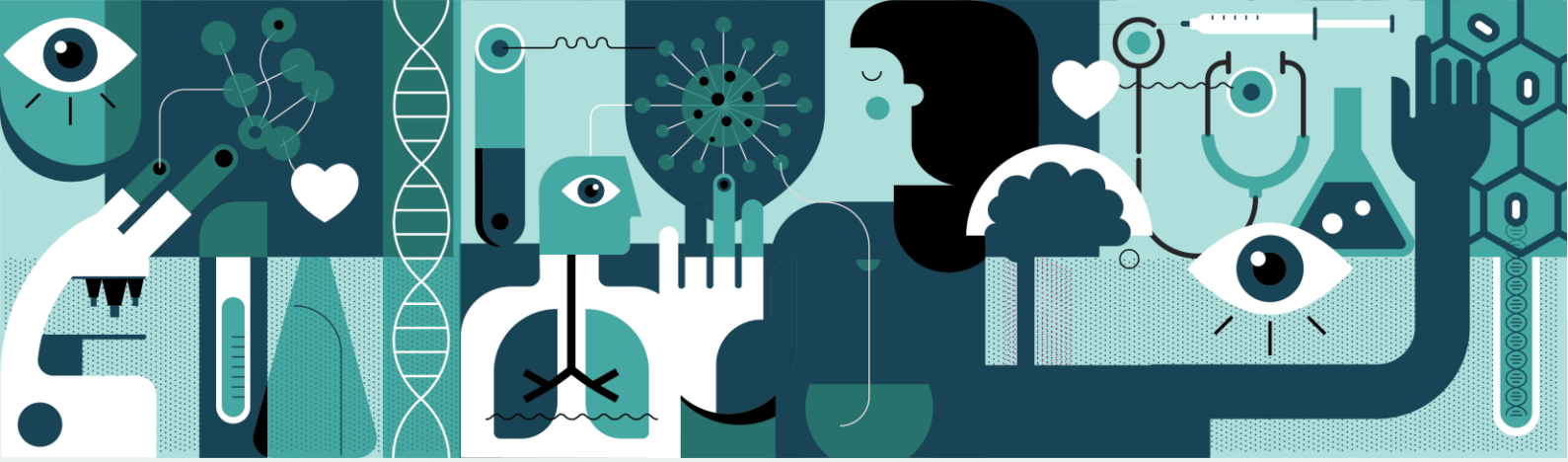


HÔPITAUX PUBLICS Grand Lille

Charte des Utilisateurs des Systèmes d'Information

Fiche de suivi du document

MODIFICATIONS APPORTEES

- 31/12/2024 Version 1.0 : document initial

Rédaction *(Nom et fonction)*	Visa
Cellule Conformité Numérique	

Vérification *(Nom et fonction)*	Visa
Thomas Aubin **Responsable Sécurité du Système d'Information GHT**	
Anthony Bouzidi **Délégué à la Protection des Données GHT**	
Mickaël Taine **Directeur des Système d'Information GHT**	

Approbation *(Nom et fonction)*	Visa
Frédéric Boiron **Directeur Général du CHU de Lille**	

Table des matières

1. Objet

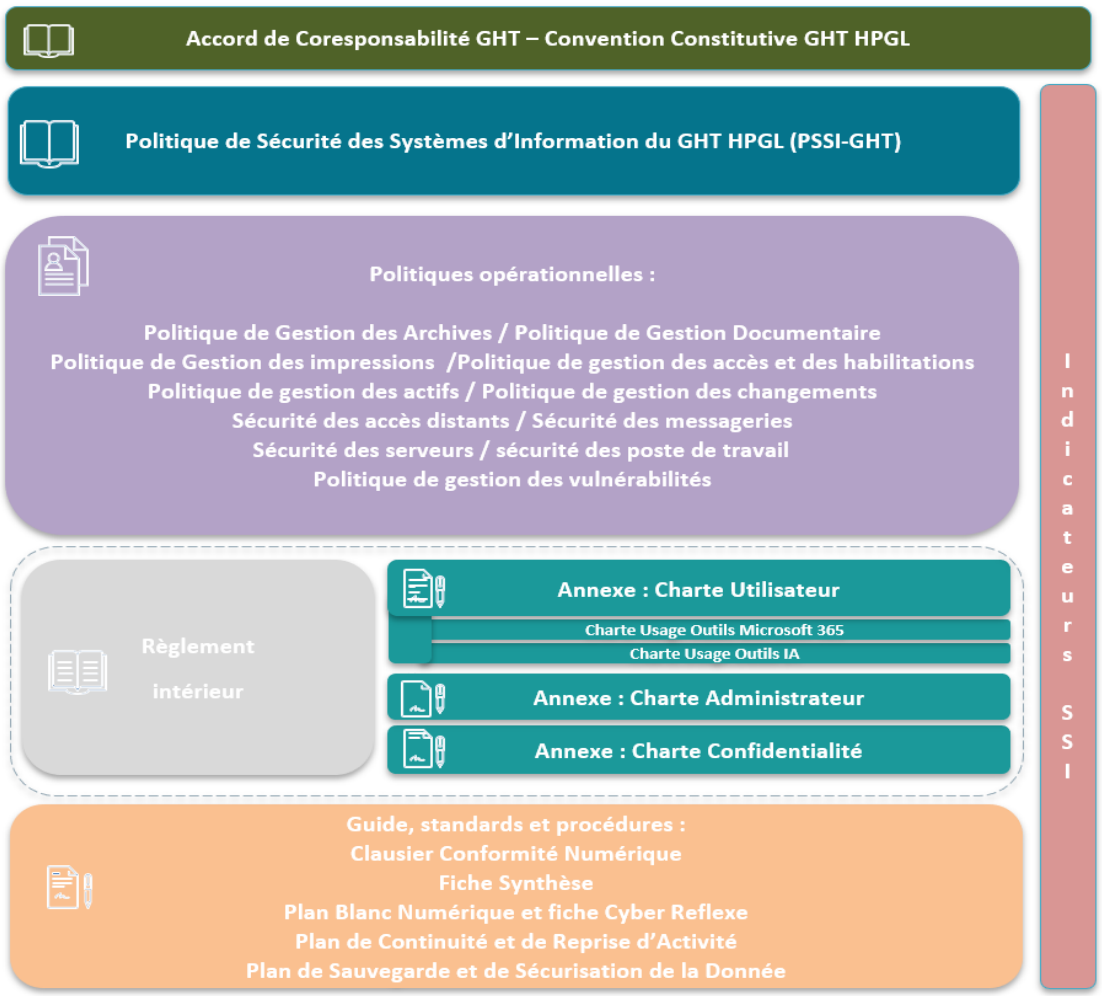
La présente charte a pour objet de formaliser les règles applicables à l'utilisation des Systèmes d'Informations et en particulier des Outils informatiques utilisés au sein des établissements membres du Groupement Hospitalier Hôpitaux Publics Grand Lille (GHT HPGL) (ci-après la « **Charte** »).

La présente Charte a également un objectif pédagogique et participe ainsi à la prise de conscience individuelle et collective des Utilisateurs, des enjeux de la sécurité des Systèmes d'Information à tous les niveaux au sein des établissements membres du GHT HPGL et de l'importance de protéger ces Systèmes d'Information.

La présente Charte complète ainsi la charte de confidentialité du GHT HPGL mise en œuvre à travers le Système de Management de la Sécurité de l'Information (SMSI) et de la Politique de Sécurité des Systèmes d'Information (PSSI) du GHT HPGL. Leurs applications sont définies par des politiques opérationnelles régulièrement mises à jour.

2. Documentation

La présente Charte s'insère dans la politique globale du GHT HPGL en matière de sécurité des Systèmes d'information. Cette politique de sécurité à la fois globale et transverse s'organise comme suit :



Les règles ainsi définies sont destinées à assurer un niveau optimum de sécurité, de confidentialité et de performance d'usage des Systèmes d'Information et des Outils en conformité avec les dispositions légales et réglementaires applicables notamment aux établissements de santé, la jurisprudence des Cours et Tribunaux, ainsi que des recommandations de la Commission nationale de l'informatique et des libertés (CNIL), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Direction générale de l'offre de soins (DGOS) du Ministère des solidarités et de la santé, en fonction des besoins métiers, et dans le respect des libertés de chacun.

3. Définitions

Les mots suivants, débutant par une majuscule ou non, s'entendent de la définition qui leur est donnée :

Administrateur : désigne la ou les personnes ayant pour mission de s'assurer du fonctionnement normal du Système d'Information ainsi que de sa sécurité. Ces personnes comprennent notamment des agents des Directions des Systèmes d'Information des établissements membres du GHT.

BYOD : désigne le fait pour un Utilisateur d'avoir recours à un ou plusieurs Outil(s) Personnel(s) dans le cadre de ses fonctions ou interventions au sein des établissements membres du GHT HPGL et notamment de le(s) utiliser ou le(s) connecter avec les Outils et/ou au Système d'Information.

Données : désigne indifféremment les Données Confidentielles, les Données Très Confidentielles et les Données Secrètes.

Donnée(s) Confidentielle(s) : désigne les 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 qui est la propriété des établissements membres du GHT HPGL ou de tout autre organisme en lien avec la finalité du traitement. 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 (Il est rappelé que le partage et échange de la donnée de santé doivent respecter le cadre fixé par l'article L1110-4 CSP). L'Utilisateur est informé que la divulgation des Données Confidentielles est susceptible d'engager la responsabilité des établissements du GHT HPGL et du GHT HPGL lui-même.

Donnée(s) Très Confidentielle(s) : désigne les informations confidentielles sous la responsabilité particulière de chaque établissement de santé membre du GHT HPGL, diffusables par exception aux experts qualifiés (interne/externe) dans chaque établissement membre du GHT HPGL. Par exemple : les données d'authentification tels que les identifiants de connexion et les mots de passe. L'Utilisateur est informé que la divulgation des Données Très Confidentielles est susceptible d'aggraver la responsabilité des établissements du GHT HPGL et du GHT HPGL lui-même.

Donnée Secrète / Très Secrète : Information encore plus confidentielle que les Données Très Confidentielles, dont la diffusion et l'exploitation est interdite, et restant strictement limitée à un personnel spécifique identifié par leur nom au sein du GHT HPGL.

Outil(s) : désigne tous les moyens matériels et immatériels, physiques et logiques, mis à disposition des Utilisateurs par le GHT HPGL et ses établissements membres et qui comprennent notamment :

- Les **Matériels Informatiques :** désignent les matériels, y compris les programmes informatiques qui y sont installés et notamment les logiciels d'exploitation, les applications de toutes natures, et plus largement tous les dispositifs qui sont mis à la disposition des Utilisateurs par le GHT HPGL et ses établissements membres, tels que par exemple : les ordinateurs, les logiciels, les serveurs, les périphériques d'impression, les stations de travail, les portables, les abonnements à des services interactifs, etc.
- La **Téléphonie** : désigne l'ensemble des matériels permettant la télécommunication notamment par autocommutateur, VoIP, Internet, fixe ou mobile (voix, Visio et données), y compris les programmes informatiques qui y sont installés et notamment les logiciels d'exploitation, les applications de toute nature, et plus largement tous les dispositifs qui sont mis à disposition des Utilisateurs par le GHT HPGL et ses établissements membres, tels que par exemple : les téléphones fixes, mobiles, *smartphone* et bippers, etc. L'utilisation de la téléphonie est entendue de manière large dans la Charte et comprend notamment tous les appels, envois de données par voie de SMS/MMS, transferts de Fichiers, utilisation d'Internet, d'applications et de Messagerie électronique.
- Les **réseaux** : désigne les réseaux de télécommunications, y compris le réseau Wifi

Outils Personnels : désigne l'ensemble des moyens matériels et immatériels, physiques et logiques, qui ne sont pas mis à disposition des Utilisateurs par le GHT HPGL et ses établissements membres et qui sont utilisés au sein des établissements membres du GHT HPGL. Cela peut notamment désigner le matériel personnel des Utilisateurs (exemples : ordinateur portable, téléphone, tablette, tout dispositif de stockage…), y compris les programmes installés sur ces matériels et les programmes auxquels l'Utilisateur se connecte.

Système d'Information (SI) : désigne l'ensemble des matériel, logiciels et réseaux, y compris la télécommunication, mis en œuvre par les établissements du GHT HPGL permettant de collecter, stocker, traiter et distribuer de l'information, quel que soit les moyens mis en œuvre quel que soit le domaine d'activité quel que soit le moyen d'y accéder, incluant le BYOD. Il peut s'agir :

- De l'ensemble des matériels supportant les applications et services d'infrastructures du SI pour l'ensemble des environnements (production, développement, recette…) : serveurs physiques, serveurs virtuels, baies de stockage, dispositif de sauvegarde, équipements réseaux, … Ces matériels peuvent être fournis en mode Cloud et en mode hébergement « On premise » simple.
- De l'ensemble des activités de services (documentation, administration, exploitation, supervision, maintenance, sauvegarde/ restauration, renouvellement de matériels, …) nécessaire pour maintenir le SI en condition opérationnelle, de la couche matérielle jusqu'à la couche des applications, y compris réseau.
- Des éléments logiques (matériel, virtualisation, systèmes d'exploitation, middlewares, fichiers, bases de données, intranet, extranet…) nécessaires pour maintenir le SI en condition opérationnelle et les activités de services associées, de la couche matérielle jusqu'à la couche des applications, y compris réseau.
- Des réseaux permettant de connecter les sites répartis à travers le monde (dont les DataCenters) tels que par exemple les réseaux de types MPLS et VPN.

Utilisateur(s) : désigne toute personne, quel que soit son statut (salarié, personnel intérimaire, stagiaire, apprenti, interne, consultant externe, etc) autorisée à accéder à une ressource (matériel, logiciel ou réseau) du Système d'Information ou traiter une Donnée, y compris les Administrateurs.

4. Champs d'application

La présente Charte est applicable et opposable à l'ensemble des Utilisateurs.

Elle peut être précisée par des documents spécifiques pour certains usages (référencés en annexe de celle-ci), certaines

catégories, de professionnels ou d'Utilisateurs.

Elle s'applique quel que soit le lieu, la fréquence et la périodicité d'utilisation du Système d'Information.

5. Mise à jour de la Charte

La présente Charte est actualisée régulièrement, y compris sur proposition de la cellule Conformité Numérique et approbation du Directeur Général du CHU de Lille.

Les nouvelles versions de la Charte seront diffusées par les établissements membres du GHT HPGL aux Utilisateurs selon le mode de communication privilégié au sein de chaque établissement concerné.

L'Utilisateur s'engage à prendre connaissance de chaque mise à jour et à relire régulièrement les dispositions de cette Charte si nécessaire.

6. Les conditions d'utilisation des Outils

6.1 Usage professionnel

L'ensemble des dossiers, fichiers, Données et informations créés, consultés, modifiés, stockés, envoyés ou reçus transitant ou traités au travers du Système d'Information sont présumés avoir un caractère professionnel.

Il appartient à tout Utilisateur de contribuer à la protection :

- Des Outils, des équipements et des Données contre toute perte, destruction, atteintes à l'intégrité, falsification des sources, perturbation du fonctionnement, augmentation indue des coûts de fonctionnement…,
- Des accès au Système d'Information et aux Données pour s'assurer que seules les personnes autorisées accèdent au SI,
- De la confidentialité des Données et des Informations Confidentielles de toute nature notamment en termes de divulgation desdites Données et/ou informations,
- Contre l'utilisation du SI, des Outils, des Données à toutes autres fins que celles prévues pour le traitement de ces données ou à des fin répréhensibles ou illégales, contre la violation des droits des tiers, les détournements à des fins personnelles, l'usurpation ou le masquage d'identité…

Les Outils mis à la disposition des Utilisateurs par un établissements membres du GHT HPGL, sont destinés à un usage professionnel. Aux termes de la jurisprudence, sont ainsi présumés avoir un caractère professionnel, notamment :

- Les fichiers créés grâce à ces moyens par un utilisateur, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant personnel ;
- Les connexions établies par un utilisateur sur des sites internet pendant son temps de travail grâce à un moyen informatique ou de communication électronique, pour l'exécution de son travail.

L'Utilisateur est informé que chaque établissement du GHT HPGL peut accéder aux données produites par les utilisateurs placés sous sa responsabilité ou agissant pour son compte, en dehors de la présence de l'Utilisateur

L'utilisation des Outils mis à disposition, à des fins autres que professionnelles peut présenter un caractère fautif.

L'adresse de courrier électronique professionnelle ne doit donc pas être utilisée dans un autre contexte, notamment sur des sites internet (chats, forums de discussion, blogs, etc.), sans rapport avec l'activité professionnelle.

6.2 Usage non professionnel

Bien que les moyens informatiques et de communications électroniques soient destinés à un usage professionnel, leur utilisation à des fins non professionnelles est tolérée uniquement de manière exceptionnelle, raisonnable, et socialement admise, tels que :

1. *La création d'un répertoire informatique non professionnel, c'est-à-dire privé, à la condition qu'il soit clairement identifiable en tant que tel. Il peut être identifié par le terme « PRIVE » suivi des initiales des nom et prénom de l'utilisateur pour le stockage de documents personnels ;*
2. *L'utilisation de l'adresse de courrier électronique à des fins non professionnelles, c'est-à-dire privées, afin de répondre à des besoins à caractère d'urgence et à titre exceptionnel. La confidentialité attachée à la correspondance professionnelle implique la notion du terme « PRIVE » dans la zone « objet du message ». La perspective d'une réponse impose d'informer le tiers destinataire du message de cet usage.*

Un tel usage ne doit notamment pas :

1. *Perturber le bon fonctionnement des Outils et Système d'Information des établissements du GHT HPGL en général ;*
2. *Compromettre ses activités ou la continuité de ses services ;*
3. *Porter atteinte ou être susceptible d'engager la responsabilité du GHT HPGL et de ses établissements membres ;*
4. *Affecter le travail de l'Utilisateur ni d'autres Utilisateurs ou tiers ;*
5. *Permettre de télécharger et/ou stocker de fichiers à des fins personnelles et n'ayant pas de rapport avec l'activité du GHT HPGL, quels qu'en soient la nature (exemples : photos, vidéos, films, musiques, etc …) ;*
6. *Poursuivre un but lucratif ou même ludique.*

L'usage des Outils à des fins non professionnelles relève de la seule et entière responsabilité de l'Utilisateur, qui dégage en conséquence les établissements du GHT HPGL de toute responsabilité. La protection et la sauvegarde régulière de ces dossiers non professionnels incombent à l'Utilisateur.

Le caractère non professionnel/privé du répertoire ou des courriers électroniques échangés, ne fait pas obstacle :

- A ce que les établissements du GHT HPGL puissent accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour l'établissement en termes de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;
- A ce que ces éléments fassent l'objet de conservations techniques dans le cadre des procédures de back up ou de plans de continuité ou reprise d'activité mis en œuvre au sein des établissements du GHT HPGL ;
- En cas de détection ou de suspicion de la présence d'un code malveillant, à la mise en quarantaine ou, s'il y a lieu, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;
- A ce que chaque établissement du GHT HPGL, y compris un Administrateur ou toute personne habilitée, puisse dans tous les autres cas et pour des motifs légitimes, accéder aux éléments en présence de l'Utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisé par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie,douanes, Commission Nationale de l'Informatique et des Libertés (CNIL), Membres de l'équipe conformité numérique, etc.).

7. Les conditions d'accès au Système d'Information

7.1 Principes

Chaque Utilisateur est doté d'un ou de plusieurs identifiants permettant l'accès aux Outils ainsi qu'à la partie du Système d'Information qui lui est autorisée en fonction de son profil.

Ces identifiants peuvent prendre diverses formes (identifiant/mot de passe, biométrie, signature électronique, carte avec ou sans contact, OTP, etc.), et restent personnel.

Il est dès lors interdit à l'Utilisateur de :

- *Procéder à la moindre divulgation, même intra-service, de son ou de ses identifiants ;*
- *Utiliser un identifiant autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;*
- *Supprimer, masquer ou modifier son identité ou son identifiant ;*
- *User de ses habilitations pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.*

L'Utilisateur s'engage à respecter les politiques opérationnelles en matière de gestion des accès et des habilitations qui lui seront mis à disposition par les établissements membres du GHT HPGL. L'Utilisateur doit notamment :

- *Renouveler ses identifiants selon la procédure mise en place par les établissements du GHT HPGL, notamment si ses identifiants ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, ou s'ils ont été oubliés ;*
- *Modifier ses mots de passe selon une fréquence déterminée par les établissements du GHT HPGL ;*
- *Utiliser, à l'exclusion de tout autre, les moyens techniques d'authentification qui lui sont remis pour se connecter à distance ;*
- *Aviser sans délai l'/les Administrateur(s) de la perte ou du vol des moyens d'authentification à distance. Il devra également, selon les cas, soit assister les établissements du GHT HPGL, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.*

Sauf à être en mesure de démontrer le contraire, tout usage des Outils est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès qui en assume toutes conséquences, notamment juridiques et financières.

Les établissements du GHT HPGL se réservent, quelle qu'en soit la raison, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer tout ou partie du droit d'accès de toute personne aux Outils et/ou Système d'Information.

7.2 Interdiction de recourir à la sous-traitance

Tout Utilisateur est notamment informé du danger résultant de la transmission de Données par tout moyen de communication (messagerie, site web, téléphone, etc.).

Outre les cas autorisés par les établissements du GHT HPGL, l'Utilisateur s'interdit de recourir à des tiers, qui peuvent notamment être en freelance afin de réaliser les missions qui peuvent lui être confiées dans le cadre de l'exercice de ses fonctions au sein des établissements du GHT HPGL.

Une telle communication externe de Données engage la responsabilité de l'Utilisateur seul et dégage toute responsabilité des établissements du GHT HPGL sur les conséquences de cet acte.

8. Règles applicables à l'usage nomade et à la BYOD

L'usage nomade définit l'accès aux SI du GHT HPGL en situation de mobilité sur un Outil qui peut être maitrisé ou non par la DSI de l'établissement.

Dans le cadre du télétravail et de ses déplacements professionnels, l'Utilisateur assure la garde et la responsabilité des Outils qui lui ont été remis.

Cet usage des Outils dits « nomades » impose à l'Utilisateur un niveau de surveillance et de confidentialité renforcé.

L'Utilisateur doit notamment :

- *Adopter une attitude de prudence et de réserve au regard des informations et des ressources des Systèmes d'Information des établissements du GHT HPGL, qu'il pourrait être amené à manipuler ou à échanger ;*
- *Veiller à ce que des tiers non autorisés ne puissent pas accéder à ces moyens, à les utiliser ou à accéder à leur contenu ;*
- *Aviser sans délai l'/les Administrateurs en cas d'incident avéré ou de doute ;*
- *Utiliser un filtre de confidentialité à minima lorsqu'il se situe en dehors des établissements du GHT HPGL ;*
- *Ne pas connecter les Matériels Informatiques à un équipement personnel ou professionnel non sécurisé, inconnu ou nonfiable, qui pourrait compromettre ceux-ci ;*
- *Ne se connecter qu'à des réseaux de confiance (Réseau des établissements du GHT HPGL, réseau personnel via solution sécurisée de typeVPN, bastion, ou solution « zero-trust » en télétravail).*

L'Utilisateur est informé que dès lors qu'un Outil Personnel est connecté à un Outil ou au Système d'Information il est pleinement responsable des conséquences liées à une telle connexion et utilisation.

Afin d'assurer un minimum de sécurité des Outils et du Système d'Information, l'Utilisateur s'engage notamment à :

- Obtenir l'autorisation préalable de l'établissement concerné du GHT HPGL et la validation par l'Administrateur de l'Outil Personnel, avant d'avoir recours au BYOD au sein de l'établissement concerné du GHT HPGL. Ainsi, aucun Outil Personnel ne devra être connecté aux Outils et au Système Informatique sans cette autorisation et vérification ;
- Respecter l'ensemble des règles de la présente Charte lors de l'utilisation des Outils Personnels, en particulier les règles applicables aux Outils ;
- Garantir que les Outils Personnels disposent d'une protection suffisante et s'assurer du maintien de cette protection pendant toute la durée de leur utilisation au sein du GHT HPGL (Mise à jour du système d'exploitation, mise à jour de l'antivirus, pare-feu activé, ...) ;
- Procéder à un cloisonnement des données et des applications personnelles et professionnelles au sein des Outils Personnels, par exemple par l'usage de sessions dédiées, avec usage d'un mot de passe fort ;
- Respecter les règles de classement, d'archivage, de sauvegarde, de conservation et de suppression des fichiers fixés par l'établissement concerné du GHT HPGL pour les fichiers stockés sur les Outils Personnels, afin notamment de permettre leur accès par les autres Utilisateurs autorisés à tout moment ;
- Rester vigilant sur le risque de divulgation/publication des fichiers stockés sur les Outils Personnels. A ce titre, chaque Utilisateur est responsable du respect du secret professionnel et de la confidentialité des fichiers qu'il est amené à stocker sur les Outils Personnels et particulièrement en dehors des locaux des établissements du GHT HPGL. Il est d'ailleurs vivement recommandé de supprimer régulièrement tous les fichiers et toutes les données professionnelles des Outils Personnels, après les avoir sauvegardés dans le Système d'Information ;
- À la fin de son contrat de travail ou de son intervention pour les établissements du GHT HPGL l'Utilisateur devra :

- Restituer tous les fichiers conservés sur son ou ses Outils Personnels ;
- Supprimer immédiatement tous les fichiers de son ou ses Outils Personnels ;
- Permettre l'accès par l'Administrateur aux Outils Personnels afin que ce dernier puisse s'assurer de l'effectivité de la restitution et de la suppression des données.

9. Sécurité des postes de travail

Afin de sécuriser les Données protégées et de réduire le risque de fraude ou de faille de sécurité, l'Utilisateur doit :

- *Ne pas mettre à la vue de tous des Données Confidentielles ;*
- *Ne rendre accessible les Données Confidentielles qu'aux personnes ayant le besoin d'en connaitre ;*
- *Stocker de manière sécurisée les Données Confidentielles ;*
- *Détruire les supports papier dont l'usage n'est plus nécessaire en respectant les procédures en vigueur dans l'établissement concerné ;*
- *Ne pas noter sur papier les identifiants, mots de passe ou tout autre moyen d'identification ;*
- *Retirer des postes de travail en cas d'absence et stocker dans un lieu sécurisé tous médias sur lesquels sont enregistrées des Données Confidentielles ;*
- *Effacer les tableaux à la fin de chaque réunion et/ou supprimer les feuilles papier du tableau avec annotations – supprimer les fichiers de présentation et de travail sur les postes disponibles en salle de réunion en fin de session ;*
- *Retirer immédiatement toute impression contenant des données Confidentielles de l'imprimante ;*
- *Verrouiller les ordinateurs et les terminaux laissés sans surveillance, ou dès lors qu'il quitte sa session de travail.*

10. Gestion des absences et des départs

10.1 Absence

Chaque Utilisateur doit veiller à ce que la continuité du service soit assurée conformément aux modalités d'organisation définies par les établissements du GHT HPGL notamment que l'information nécessaire au bon fonctionnement de son service ou à la prise en charge des patients ait bien été partagée au sens du code de la santé publique (L1110-4 CSP).

En cas d'absence imprévue de l'Utilisateur ou de non-respect de la consigne précédente, chaque établissement du GHT HPGL se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques, aux codes administrateurs systèmes et plus généralement, à tous documents à caractère professionnel de l'Utilisateur, ayant recours en tant que de besoin.

10.2 Départ

A l'annonce du départ d'un Utilisateur d'un des établissements du GHT HPGL, et pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation des moyens informatiques et de communication électronique pourront être modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

Lors de son départ, l'Utilisateur doit :

- *Faire le tri dans les messages de sa boite aux lettres électronique en supprimant ceux à caractère privé ou non nécessaires à la continuité de service. Le contenu résiduel pourra être transmis au responsable hiérarchique N+1 qui pourra avoir accès aux messages entrants postérieurement au départ de l'Utilisateur ;*
- *Restituer l'ensemble des Outils qui lui ont été remis ;*
- *Supprimer le répertoire nommé « PRIVE » suivi des initiales des nom et prénom de l'Utilisateur, ainsi que tous les documents de même nature, au plus tard la veille de son départ.*

Sauf nécessité liée à la continuité du service pour un temps défini dans les politiques opérationnelles, le compte de messagerie de l'Utilisateur est désactivé le jour de son départ.

Ses identifiants sont également immédiatement désactivés, sauf besoins légitimes. Toute exception devra être motivée, tracée, suivie, et bornée dans le temps.

L'Utilisateur est informé que conformément à la règlementation et à ses obligations, l'employeur conserve les traces de ses activités dans le cadre des fonctions qui lui avaient été confiées pendant une durée définie par la loi.

11. Accès à Internet

Les établissements du GHT HPGL mettent à la disposition de l'Utilisateur un accès internet chaque fois que cela est nécessaire dans le cadre de l'exercice de sa fonction.

Internet est un outil de travail ouvert à des usages professionnels (administratifs, pédagogiques, recherches, etc.).Il peut aussi constituer le support d'une communication privée.

Au regard des dispositions légales et déontologiques applicables, l'Utilisateur ne doit pas consulter des contenus illicites ou ne répondant pas à la déontologie du GHT HPGL.

Les établissements du GHT HPGL filtrent, d'administrent, d'interdisent l'accès à certains sites internet, assurent une traçabilité des accès, et procèdent au contrôle a priori ou a posteriori des sites internet visités et des durées d'accès correspondantes.

Il est rappelé que les Utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts des établissements du GHT HPGL, y compris sur Internet.

Les établissements du GHT HPGL se réservent le droit d'interdire certains accès, protocoles de communication, programmes ou modules pouvant porter atteinte à la sécurité.

Pour des raisons de continuité de service, le GHT HPGL peut interdire la consultation de site « non essentiels » à son activité.

12. Utilisation de la messagerie électronique

La mise à disposition de la messagerie électronique professionnelle par les établissements du GHT HPGL suppose que l'Utilisateur doit :

- *Sauf autorisation expresse, utiliser la messagerie comme un outil de communication et d'information, et s'interdit de s'en servir pour conclure des contrats ou réaliser des actes juridiques ;*
- *S'assurer de l'exactitude des données des destinataires ;*
- *Limiter l'envoi de messages aux destinataires concernés ;*
- *Ne pas contourner les dispositifs de sécurité ou les limitations mises en œuvre par l'établissement ;*
- *Apurer régulièrement et classer en fonction des consignes éventuelles les messages émis et reçus ;*
- *Ne pas mettre en place de règles de redirections automatiques de ses mails professionnels vers une boîte mail extérieure, et inversement.*

- *Ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;*
- *Ne communiquer aucune donnée sensible par mail sur simple demande, notamment des identifiants/mots de passe ;*

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. En cas de dysfonctionnement du dispositif de filtrage ou de réception d'un message électronique d'un expéditeur ayant vraisemblablement réalisé une erreur de destinataire, l'Utilisateur doit :

- *Eviter dans la mesure du possible de prendre connaissance des contenus et ne jamais ouvrir les éventuelles pièces-jointes ;*
- *Prévenir immédiatement l'expéditeur dudit message pour l'en informer ;*
- *Supprimer, après en avoir informé l'expéditeur, les messages qui ne lui sont pas destinés.*

Les données de santé ne peuvent apparaitre en clair dans des messages ; elles doivent être échangées au travers de mécanismes sécurisés (Messageries sécurisées de santé MS Santé ou équivalent), et chiffrées.

Si l'utilisation des moyens précités n'est pas possible, les données permettant l'identification des personnes (Nom, prénom, date de naissance, ou tout autre donnée directement ou indirectement identifiante…) doivent être masquées avant leur envoi par une messagerie professionnelle standard de façon à ne pas pouvoir réidentifier le patient.

L'Utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation applicable et notamment relative au droit de propriété intellectuelle, au secret des correspondances, aux données personnelles, aux systèmes de traitement automatisé de données et au droit à l'image des personnes.

Pour faire face aux risques d'hameçonnage et de rançongiciel, l'Utilisateur prend toutes les précautions nécessaires pour s'assurer de la légitimé de la correspondance reçue avant l'ouverture du message et de la pièce jointe.

13. Gestion des connaissances, des espaces collaboratifs et des réseaux sociaux internes.

Le GHT HPGL privilégie le partage et la capitalisation des connaissances, et peut être ainsi amené à mettre en place des espaces collaboratifs de travail :

- *Les données à caractère professionnel doivent impérativement être sauvegardées dans les espaces disques partagés ;*
- *Les disques locaux sont dédiés au fonctionnement des systèmes et non pas au stockage et à la sauvegarde de données personnelles.*

La qualité des informations ainsi disponibles est un objectif important et chaque Utilisateur doit :

- *Être attentif à la pertinence des informations diffusées au sein de ces espaces et à travers les outils de gestion des connaissances mis à sa disposition ;*
- *Respecter les normes de classification, de nommage et de diffusion.*

Par souci de qualité, de responsabilité et de protection du patrimoine informationnel du GHT HPGL, l'utilisation de ces mêmes espaces et outils peut faire l'objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

Aux mêmes fins, le GHT HPGL pourra mettre en place des outils de marquage de tout ou partie des éléments des bases de données constituées dans ce cadre, pour éviter toute extraction. Les Utilisateurs seront avertis de la présence de tels outils.

Les établissements du GHT HPGL autorisent l'usage des réseaux sociaux internes, dédiés aux personnels de chaque établissement, qui leur permettent de partager des informations utiles à l'amélioration du service fourni et à l'innovation.

14. Réseaux sociaux externes

Dans l'éventualité où l'accès aux réseaux sociaux serait nécessaire pour l'Utilisateur dans le cadre de ses fonctions, ce dernier devra respecter les règles suivantes. Le service responsable de la communication de chaque établissement du GHT HPGL est le seul compétent pour déterminer les conditions d'utilisation des réseaux sociaux.

L'Utilisateur devra :

- *S'abstenir de diffuser toutes Données Confidentielles relatives aux établissements du GHT HPGL et détenues par eux ;*
- *S'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein des établissements du GHT HPGL ;*
- *Répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image demarque des établissements du GHT HPGL ;*
- *Respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables, notamment s'abstenir de publier et diffuser des publications à caractère injurieux, raciste, diffamatoire et pornographique ;*
- *S'abstenir de publier tout contenu, notamment sur les réseaux sociaux, pouvant nuire à la réputation et à l'image (y compris l'e-réputation) du GHT HPGL, de ses établissements membres, ou de toute personne (exemples : employé, dirigeant, prestataire ou partenaire ou tout tiers) ;*
- *Utiliser uniquement les outils de communication validés par les établissements du GHT HPGL ;*
- *Prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour lesSI des établissements du GHT HPGL.*

Il est en outre rappelé que les personnels des établissements du GHT HPGL, qui sont soumis au secret professionnel et/ou au secret médical, ont un devoir de réserve, ainsi qu'un devoir de loyauté vis-à-vis des établissements du GHT HPGL. Il est notamment strictement interdit de diffuser des documents ou des informations non validés comme « public » par chaque établissement. L'Utilisateur a conscience et est ainsi informé que de tels agissements peuvent notamment engager sa responsabilité et justifier une sanction disciplinaire.

15. Protection de la propriété intellectuelle

L'utilisation des Outils des établissements du GHT HPGL implique le respect des droits de propriété intellectuelle et de la législation en vigueur.

Sans que cette liste soit exhaustive, l'Utilisateur doit :

- *Utiliser les logiciels ou applications, dans les conditions de la licence souscrite par les établissements du GHT HPGL ;*
- *Ne pas effectuer de copies illicites de logiciels, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels les établissements du GHT HPGL ne possèderaient pas un droit d'usage ;*
- *Ne pas reproduire et utiliser les bases de données, pages web ou autres créations des établissements du GHT HPGL ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;*
- *Ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur internet ;*
- *Ne pas copier et remettre à des tiers des créations appartenant à des tiers ou aux autres établissements duGHT HPGL sans s'assurer de l'autorisation du titulaire de droits qui s'y rapporte ;*
- *Ne pas solliciter l'envoi par des tiers, en pièces jointes, de fichiers, programmes, logiciels, ou progiciels en violation des droits d'auteurs et des contrats de licence conclu par les établissements du GHT HPGL.*

16. Préservation du secret et de la confidentialité

16.1 Principes applicables

Le respect de la confidentialité de l'ensemble des Données qu'elles soit Confidentielles, Données Très Confidentielles et Données Secrètes/Très Secrètes sont protégées et explicitées dans la charte de confidentialité, disponible au sein de chaque établissement du GHT HPGL.
La classification d'une information est directement applicable au Matériel Informatique qui sert à la traiter, à la stocker ou à la communiquer. C'est la classification la plus élevée des informations contenues dans le média qui s'applique à celui-ci dans sa totalité.

Les Utilisateurs sont dans tous les cas informés que seules les personnes désignées et habilitées par la loi peuvent lire et échanger les données de santé des patients. Les Utilisateurs s'interdisent de consulter des informations pour lesquelles ni leur rôle ni leur champ de compétence ne leurs donnent de droits particuliers.

Le secret professionnel est une obligation à laquelle est soumis l'ensemble du personnel des établissements du GHT HPGL ainsi, l'Utilisateur est tenu à un devoir de vigilance sur le risque de divulgation/publication des informations qu'il utilise dans l'exercice de ses fonctions ou de l'utilisation des Outils et ce même en dehors des locaux des établissements du GHT HPGL.

Afin de respecter cette obligation, l'Utilisateur doit :

- *Communiquer de telles informations uniquement aux tiers autorisés ayant besoin d'en connaitre ;*
- *N'accéder qu'aux informations en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres Utilisateurs ;*
- *Respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein des établissements du GHT HPGL.*

La diffusion de toute donnée ne peut être réalisée qu'aux conditions suivantes :

- Habilitation de l'émetteur ;
- Désignation d'un destinataire autorisé ;
- Respect d'une procédure sécurisée.

Les échanges avec les partenaires extérieurs aux établissements du GHT HPGL ne doivent comporter aucune donnée sensible au sens du RPGD. Si un transfert est absolument nécessaire dans le cadre de leurs fonctions, une solution sécurisée doit être mis à disposition par la Direction des Systèmes d'Information de l'établissement.

16.2 Protection des Données sensibles et Chiffrement

La gestion de la confidentialité des Données est explicitée dans la charte de confidentialité, disponible au sein de chaque établissement du GHT HPGL.

De manière générale, tout utilisateur s'engage notamment à protéger contre toute indiscrétion les documents médicaux concernant les patients qu'il a soignés ou examinés, quel que soit le contenu et le support de ces documents.

16.3 Recours au chiffrement

L'utilisation de procédés de chiffrement requis pour préserver la confidentialité des Données est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés.

Il est interdit d'utiliser des moyens de chiffrement autres que ceux expressément autorisés par les établissements du GHT HPGL, sur validation du RSSI de GHT.

Le chiffrement est obligatoire :

- *Pour la diffusion d'informations confidentielles à des tiers extérieurs à l'établissement n'ayant pas accès aux espaces collaboratifs mis à disposition des employés et des partenaires ;*
- *Tout transport et transfert via média de stockage amovible.*

Le chiffrement n'est pas autorisé dans les espaces de stockage et de sauvegarde des établissements sans autorisation explicite obtenue auprès de la Direction des Systèmes d'Information de l'établissement et/ou le Responsable de la Sécurité du Système d'Information du GHT HPGL.

17. Protection des données à caractère personnel

17.1 Traitement des données de l'Utilisateur par l'établissement

Au travers du Système d'Information et des Outils mis à disposition des Utilisateurs, le GHT HPGL peut collecter les données personnelles des Utilisateurs dans le cadre de leurs fonctions à des fins légitimes ainsi que pour les finalités suivantes :

- La rémunération et les déclarations sociales obligatoires ;
- La gestion administrative du personnel (exemple : type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence) ;
- L'organisation du travail (exemple : photographie de l'employé pour les annuaires internes et organigrammes ; numéros de téléphone en cas de garde, d'astreinte ou de plan blanc) ;
- L'action sociale prise en charge par l'employeur (exemple : les informations concernant les ayants-droit de l'employé) ;
- Le suivi de l'utilisation des Outils, du Système d'Information et des connexions au travers des Outils, à des fins de sécurité et de contrôle de l'usage ;
- Le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- La gestion de la sécurité des biens et des personnes ;
- Le respect de la présente Charte.

Le GHT HPGL doit garantir la confidentialité et la sécurité des données qu'il possède sur chacun. Seules les personnes habilitées doivent en prendre connaissance et ces accès doivent être tracés.

Ces données sont traitées pendant la durée d'accomplissement des finalités indiquées ci-dessus et pourront être conservées postérieurement à leur départ de l'établissement si des durées sont légalement prévues.

Pour chaque traitement de données à caractère personnel, le personnel doit être informé, du responsable de traitement, des finalités, de la durée de conservation de vos données, des différents destinataires, ou encore **des droits sur ces données :**

Droit d'information : lors de la collecte de données personnelles, certaines informations doivent être transmises :la raison pour laquelle les données sont collectées, leur durée de conservation, les destinataires des informations,les coordonnées du responsable du traitement, etc. (*Par exemple lors d'une embauche ou lors de la collecte des pièces nécessaires au recrutement*) ;

Droit d'accès : à tout moment, il est possible de demander à consulter les données personnelles recueillies (*Par exemple l'accès au dossier professionnel*) ;

Droit de rectification : si certaines données personnelles sont inexactes ou incomplètes, il est possible de demander leur rectification (*Par exemple un changement d'adresse, de numéro de téléphone, de nom, etc.)* ;

Droit à l'effacement (« droit à l'oubli ») : droit d'obtenir l'effacement des données personnelles notamment si celles-ci ne sont pas ou plus nécessaires au regard des objectifs pour lesquelles elles ont été initialement collectéesou traitées ou si celles-ci sont conservées au-delà de la durée qui aura été indiquée ;

Droit à la limitation du traitement : possibilité de demander de geler l'utilisation de données si jamais l'exactitudeest contestée le temps de procéder aux vérifications nécessaires. Concrètement, le Centre hospitalier ne devra plusutiliser les données mais devra les conserver. Inversement, il est possible de demander au Centre hospitalier de conserver des données qu'il souhaiterait lui-même effacer ;

Droit à la portabilité : possibilité de demander à récupérer les données personnelles et les transmettre à un tiers ; (*Par exemple : un agent pourra le cas échéant demander à récupérer les données qu'il a fournies dans le cadre de l'embauche (données d'identification, données relatives à la protection sociale, à sa formation professionnelle, etc.),voire à demander la transmission directe de ces informations à son futur employeur.*)

Droit d'opposition : si cela n'entrave pas le bon fonctionnement de l'établissement, et pour des motifs légitimes, ilest possible de demander que certaines des données personnelles ne soient pas collectées ou utilisées sauf si ce traitement répond à une **obligation légale** ou lors qu'il est nécessaire à **l'exécution de votre contrat de travail** ou s'il est fondé sur votre **consentement** ;

Droit de retirer votre consentement : si le traitement en question a requis celui-ci.

Pour exercer ces droits, il est possible de contacter le délégué à la protection des données du Centre Hospitalier en joignant une pièce d'identité à la demande à l'adresse suivante : dpo@chru-lille.fr

S'il est estimé, après avoir contacté le délégué à la protection des données du Centre Hospitalier, que les droits Informatique et Libertés ne sont pas respectés ou que le dispositif de contrôle d'accès n'est pas conforme aux règlesde protection des données, il est possible d'adresser une réclamation à la CNIL (cf. www.cnil.fr).

17.2 Devoirs de l'Utilisateur

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel. Ces dispositions figurent pour l'essentiel dans le Règlement Général sur la Protection des Données (loi n° 2018-493 du 20 juin 2018) et la loi Informatique et Libertés (loi n° 78-17). Dans ce cadre, les Utilisateurs devront se conformer à la procédure en cas de mise en œuvre d'un traitement de données à caractère personnel.

Toute nouvelle constitution de fichiers ou de bases de données comprenant des données à caractère personnel doit faire l'objet de formalités préalables auprès du Délégué à la Protection des Données (DPO), sauf dérogations légales ou réglementaires. Dans ce cadre, l'Utilisateur doit respecter les finalités des traitements de données à caractère personnel objets de ces formalités préalables et aucun Utilisateur ne peut de son propre chef mettre en œuvre un tel traitement.

L'Utilisateur reconnait avoir été alerté et s'engage à respecter le fait que, conformément au Règlement Général sur la Protection des Données et à la loi Informatique et Libertés, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un tel traitement impliquent que les données à caractère personnel doivent être :

- Traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
- Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément

à l'article 89, paragraphe 1 du Règlement Général sur la Protection des Données, comme incompatible avec les finalités initiales (limitation des finalités) ;
- Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- Exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;
- Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1 du Règlement Général sur la Protection des Données, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;
- Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

18. Sécurité

Les Outils sont exclusivement installés, configurés et paramétrés par le personnel habilité des établissements du GHT HPGL. Les Utilisateurs non autorisés s'interdisent d'installer, de configurer ou de paramétrer ou de modifier les configurations ou paramétrages, de tout ou partie des Outils

A des fins de précaution, certaines configurations peuvent être verrouillées par les établissements du GHT HPGL (poste de travail, accès internet, etc.).

La mise en place d'outils de sécurité par les établissements du GHT HPGL ne doit pas dispenser les Utilisateurs de leur obligation de vigilance à cet égard.

En effet, tout Utilisateur a la charge, à son niveau, de contribuer à la sécurité des Outils mis à sa disposition, principalement par exemple en évitant l'introduction de codes malveillants susceptibles d'endommager les Systèmes d'Information des établissements du GHT HPGL et en respectant la politique de sécurité du GHT HPGL.

Cette vigilance passe notamment par le respect des règles de conduite suivantes :
- *Détruire les messages du type « chaîne de solidarité » ;*
- *Ne pas stocker et router des gadgets reçus ou trouvés sur internet ;*
- *Ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la Direction des Systèmes d'Information par les moyens en place dans l'établissement (mail, outil de tickets informatisés, centre d'appels…).*

En cas de réception de messages non sollicités (pourriels, hameçonnages, rançongiciels, …), l'Utilisateur veille à :

- *Ne pas l'ouvrir ;*
- *Ne pas y répondre ;*
- *Ne pas le transférer ;*
- *Informer la cellule ou le Responsable en charge du traitement des risques informatiques (Equipe de sécurité opérationnelle, équipe informatique, …) ;*
- *Agir sur instruction de cette dernière ou ce dernier.*

L'Utilisateur s'interdit également de :

- *Modifier les moyens mis à sa disposition notamment par l'ajout de logiciels, progiciels, même gratuits, ou de matériels pour quelque raison que ce soit ; si ces logiciels ou matériels lui semblent nécessaires pour l'exercice de*

sa mission, il en fait part à sa Direction du Système d'Information, qui analysera la demande, notamment au regard des aspects sécurité ;

- *Modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit,en particulier les fichiers contenant des informations comptables ou d'identification ;*
- *Charger, stocker, publier, diffuser ou distribuer des documents, informations, images, vidéos :*
  - *À caractère violent, pornographique ou contraires aux bonnes mœurs,*
  - *Susceptibles de porter atteinte au respect de la personne humaine et à sa dignité, ainsi qu'à la protection des mineurs,*
  - *À caractère diffamatoire,*
  - *À caractère sexiste ou discriminatoire,*
  - *Susceptibles de porter atteinte à la vie privée des personnes,*
  - *Ou de manière générale prohibés par la loi et / ou sanctionnés pénalement*
- *Mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les Matériels Informatique dont il a usage ;*
- *Utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués, ou masquer son identité ;*
- *Effectuer des opérations pouvant nuire aux relations internes ou externes des établissements du GHT HPGL.*

D'une manière générale, l'Utilisateur doit :

- *N'installer et n'utiliser que du Matériel Informatique expressément autorisé par la Direction du Système d'Information de l'établissement ;*
- *Informer, sans délai, la Direction du Système d'Information de son établissement de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique ;*
- *Signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus selon la procédure en vigueur.*

Le GHT HPGL met à disposition des modules de sensibilisation à la sécurité du système d'information. L'Utilisateur doit les consulter. Tout non-respect de ces règles sera considéré comme une négligence de sa part.

19. Traçabilité et filtrage

Pour satisfaire aux obligations légales qui leur incombent, tenant à leur capacité à :

- Apporter la preuve du bon usage des Outils mis à la disposition des Utilisateurs ;
- Prévenir tout usage illicite de ces mêmes moyens,

les établissements du GHT HPGL procèdent à la mise en place :

- D'outils de traçabilité (journaux de connexions) de l'ensemble des moyens informatiques et de communications électroniques, permettant de détecter les écarts, abus et comportements suspects sur les Systèmes d'Information ;
- D'outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre ou d'interdire l'accèsà internet ou à certaines catégories de sites internet.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

20. Mesures d'urgence et plan de continuité d'activité

L'Utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, les établissements du GHT HPGL peuvent mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'Utilisateur pourra être amené, à la demande d'un établissement, à prendre des mesures d'urgence et de sécurité spécifiques qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure notamment une dégradation de service sur tout ou partie des ressources des Systèmes d'Information concernés (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources des Systèmes d'Information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou aux Systèmes d'Information, télétravail, déplacement sur des sites de secours tiers, etc.).

L'Utilisateur est informé que dans le cadre des Plans de Continuité et de reprise d'Activité, les Systèmes d'Information bénéficient de sauvegardes régulières, selon un Plan de Sauvegarde défini suivant la criticité des données à traiter. Il lui appartient en conséquence d'enregistrer tout fichier et tout autre document, données ou message ou information nécessaire à l'activité des établissements du GHT HPGL dans l'emplacement dédié sur le Système d'Information afin de permettre sa sauvegarde et donc sa sécurisation.

21. Maintenance

La mise à disposition des Outils des établissements du GHT HPGL, implique des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

L'objectif de ces opérations est d'assurer le bon fonctionnement et la sécurité des Systèmes d'Information concernés. Ces opérations se distinguent des opérations de contrôle et d'audit expliquées ci-après.

Ces opérations peuvent nécessiter l'intervention d'une personne habilitée soit sur site, soit à distance.

Il est rappelé que, dans ce cadre, la personne habilitée peut être amenée à prendre connaissance de l'ensemble des éléments présents sur le poste de l'Utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage professionnel ou privé.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable est identifié, les établissements du GHT HPGL pourront engager les procédures appropriées.

22. Assistance et prise en main à distance

Au préalable de la prise en main à distance dans le cadre d'une assistance, l'Utilisateur sera amené à autoriser le technicien à accéder à son poste de travail.

Pendant toute la durée de la prise en main à distance un visuel informe l'Utilisateur que l'ensemble des actions effectuées et pages consultées sont visibles par le technicien. À tout moment l'Utilisateur peut interrompre la prise en main à distance.

Dans le cas de l'assistance de prise en main à distance, **l'Utilisateur ne doit jamais communiquer son identifiant et son mot de passe.**

Il est rappelé que, dans ce cadre, la personne habilitée peut être amenée à prendre connaissance de l'ensemble des éléments présents sur le poste de l'Utilisateur, ainsi que des données de connexion, qu'il s'agisse d'un usage

professionnel ou privé.

Si, à l'occasion d'opérations de prise en main à distance, une utilisation anormale et/ou un contenu illicite ou pré-judiciable est constaté par l'assistance, un signalement pourra être effectué. Les établissements du GHT HPGL pourront engager les procédures appropriées.

L'assistance a le devoir de secret concernant les autres informations dont il aurait pu avoir connaissance dans le cadre de ses missions.

23. Contrôle et audit

Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des Outils. Elles sont réalisées dans le respect de la politique opérationnelle de contrôle et d'audit du système d'information.

Ces opérations de contrôle et d'audit incombent aux établissements du GHT HPGL, dans le cadre de leur obligation générale de sécurité, en application des dispositions du Code pénal relatives aux atteintes aux systèmes de traitements automatisés de données, et de la loi Informatique et libertés modifiée.

Chaque établissement du GHT HPGL, en tant qu'employeur, dispose également d'un pouvoir de contrôler l'activité des Utilisateurs et, en particulier, le respect par eux de la présente Charte.

L'utilisation des Outils pourra faire l'objet d'une surveillance, afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques, ce à quoi l'Utilisateur consent expressément.

Les établissements du GHT HPGL se réservent ainsi le droit, notamment de :

- Vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- Diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources des Systèmes d'Information ;
- Contrôler l'origine licite des logiciels installés ;
- Conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque Système d'Information ;
- Transmettre aux autorités judiciaires et/ou policières sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, de quelque nature qu'il soit, les établissements du GHT HPGL se réservent notamment le droit de :

- Surveiller le contenu des informations qui transitent sur les Systèmes d'Information ;
- Vérifier le contenu des disques durs des ressources des Systèmes d'Information attribuées aux utilisateurs ;
- Procéder à toutes copies utiles pour faire valoir ses droits ;
- Réutiliser les données de traçabilité exploitables.

En cas de perturbations induites par l'apparition intempestive d'alertes à la suite de tentatives d'infection des systèmes à l'aide de virus informatiques, elle est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

Les Utilisateurs sont toutefois informés que les Administrateurs sont conduits, de par leur fonction, à avoir accès à l'ensemble des informations relatives des Utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

Néanmoins, les Administrateurs sont tenus au secret professionnel et ne peuvent utiliser leurs droits

d'Administrateurs qu'à des fins strictement professionnelles.

En cas de faisceau d'indices laissant supposer qu'un Utilisateur met en cause les intérêts et la sécurité des établissements du GHT HPGL, en ne respectant pas les règles instituées par la présente charte, le RSSI de GHT ou l'équipe Conformité Numérique du GHT, ou la Direction du Système d'Information de l'établissement se réserve le droit de fournir à la Direction des Ressources Humaines (DRH), sur sa demande écrite et motivée, les traces individuelles des connexions incriminées sur la période juridique admise au moment de l'enquête.

En cas de non-respect de la présente Charte par un Utilisateur, le RSSI de GHT ou l'équipe Conformité Numérique, ou la Direction du Système d'Information de l'établissement se verra dans l'obligation d'avertir le supérieur hiérarchique de l'Utilisateur pour que celui-ci décide de la suite à donner.

Tout Matériel Informatique installé illicitement sera supprimé ou désactivé par les intervenants du service compétent dès le constat de leur présence sur le poste de travail.

24. Consommations des abonnements data et téléphoniques

Pour la bonne gestion des ressources de Téléphonie :

- Un autocommutateur ou un PABX enregistre, à partir de chacun des postes téléphoniques fixes, les éléments de la communication (date, heure, durée, coût et numéros appelés) ;
- Pour les Outils nomades (téléphone portable, *smartphone*, etc.), les mêmes informations sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations data et téléphoniques, peuvent être utilisées pour démontrer toutes utilisations contrevenantes aux termes de la présente charte ou pour servir de preuve d'un fait illicite.

En cas d'abus ou d'utilisation répondant à un usage privé l'employeur pourra notamment être amené à demander le remboursement de la consommation effectuée.

L'enregistrement des conversations téléphoniques est par principe interdit. Seuls peuvent être réalisés les enregistrements mis en place par l'employeur dont la nécessité est reconnue, proportionnés aux objectifs poursuivis, ayants faire l'objet d'une information à destination des agents concernés et après cadrage par l'équipe Conformité Numérique.

25. Responsabilité et sanctions

Toute accès au Système d'Information, toute utilisation des Outils, des Données et plus largement toutes ressources mises à disposition par le GHT HPGL engage la responsabilité de l'Utilisateur.

Dans le cadre de son activité professionnelle et des usages personnels tolérés, l'Utilisateur se doit de respecter la présente Charte, le règlement intérieur, y compris ses annexes ainsi que la politique du système d'information et ses déclinaisons opérationnelles (Politiques opérationnelles applicables à l'utilisateur).

Tout non-respect par l'Utilisateur de la Charte est constitutif de faute, ce que l'Utilisateur reconnait et accepte.

Le GHT HPGL rappelle que certains agissements (cas de malveillance, non-respect des différentes lois relativesà la confidentialité des informations) peuvent engager la responsabilité personnelle civile et/ou pénale de l'Utilisateur il en est ainsi également chaque fois que l'Utilisateur agira hors de ses fonctions.

Le non-respect de ses dispositions par les agents les expose à des sanctions disciplinaires en particulier celles définies dans le règlement intérieur. Concernant les extérieurs missionnés au GHT HPGL, le non-respect de ces dispositions pourra notamment engendrer une rupture du contrat les liants au GHT.

L'absence de sanction prononcée par les établissements du GHT HPGL, ne pourra être interprétée comme une renonciation de cette dernière à s'en prévaloir ultérieurement ni comme une autorisation implicite ou une tolérance à accomplir de tels actes.

Tout acte qui serait non conforme à la présente Charte sera présumé avoir été accompli par l'Utilisateur identifié, sauf à ce que ce dernier en apporte la preuve du contraire.

Signature :

Annexe 1. Charte Utilisateurs des outils « Microsoft 365 »

GHT HPGL - Charte Utilisateurs - M365_v

Annexe 2. Charte des Utilisateurs des Systèmes d'intelligence artificielle

GHT HPGL - Charte Utilisateurs Système I