CHARTE
d'accès et de bon usage des technologies de communication du groupe UNEOS

CHAPITRE 1

OBJET DU DOCUMENT

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du Groupe UNEOS et rappelle à ses Utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information du Groupe UNEOS, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux Utilisateurs, conformément à la politique de sécurité du système d'information définie par le Groupe UNEOS.

Cette Charte a été validée par le Conseil d'Administration. Préalablement, elle a été notifiée à sa mise en œuvre au Comité Social et Économique. Elle constitue une annexe au Règlement Intérieur de l'établissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance. La Charte est mise à leur disposition sur l'Intranet et affichée dans les locaux des établissements du Groupe.

CHAPITRE 2

CHAMP D'APPLICATION

⌘ *2-1 : système d'information et de communication*

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du Groupe UNEOS, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Le système d'information et de communication du Groupe UNEOS est notamment constitué des éléments suivants :

- Ordinateurs (fixes, portables, terminaux), périphériques, assistants personnels (Smartphones…), tablettes, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs.

- Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'établissement.

⌘ *2-2 : Utilisateurs concernés*

Sauf mention contraire, cette Charte s'applique à l'ensemble du personnel des établissements de santé et des EHPAD tous statuts confondus, et concerne notamment les personnels permanents ou temporaires (stagiaires, étudiants, internes, prestataires, fournisseurs, sous-traitants, intérimaires…) utilisant les moyens informatiques de l'établissement et les personnes auxquelles il est autorisé d'accéder au système d'information à distance directement ou à partir du réseau administré par l'établissement.

Dans la présente Charte, sont désignés sous les termes suivants :

- Ressources informatiques : les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité.
- Outils de communication : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, Intranet, etc).
- Utilisateurs : les personnes ayant accès ou utilisant les ressources informatiques et les services internet de l'établissement.

CHAPITRE 3

CADRE RÉGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :
  - Le traitement de données à caractère personnel et le respect de la vie privée
  - Le traitement de données personnelles de santé
- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données médicales ;
- Le secret professionnel et le secret médical ;
- La signature électronique des documents ;
- Le secret des correspondances ;
- La lutte contre la cybercriminalité ;
- La protection des logiciels et des bases de données et le droit d'auteur.

La présente Charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux Utilisateurs.

CHAPITRE 4

CRITÈRES FONDAMENTAUX DE LA SÉCURITÉ

⌘ *4-1 : PRINCIPES*

Le Groupe UNEOS héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médico-techniques…) et sur les personnels de l'entité (paie, gestion du temps, accès à Internet et à la messagerie…).
L'information se présente sous de multiples formes :

- stockée sous forme numérique sur des supports informatiques,
- imprimée ou écrite sur papier, imprimée sur des films (images),
- transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone, FAX...

La **sécurité de l'information** est caractérisée comme étant la préservation de :

- **Sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin.
- **Son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie.

⌘ *4-2 : UNE MISSION SÉCURITÉ*

Le service informatique en charge du système d'information du Groupe UNEOS fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont bien au service de la production de soins. Elle doit donc définir et empêcher les abus.

⌘ *4-3 : UN ENJEU TECHNIQUE ET ORGANISATIONNEL*

Les enjeux majeurs de la sécurité sont la qualité et la continuité des soins et le respect du cadre juridique sur l'usage des données personnelles de santé.

Pour cela, le Groupe UNEOS déploie un ensemble de dispositifs techniques mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

⌘ *4-4 : UNE GESTION DES RISQUES*

L'information médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients. Une information manquante, altérée ou indisponible peut constituer une perte de chance pour le patient (exemples : erreur dans l'identification d'un patient, perte de données suite à une erreur d'utilisation d'une application informatique…). La sécurité de l'information repose sur une gestion des risques potentiels et la communication vers les Utilisateurs est un volet important de cette gestion. La présente Charte d'accès et d'usage du système d'information s'inscrit dans ce plan de communication.

CHAPITRE 5

RÈGLES DE SÉCURITÉ

⌘ *5-1 : DROIT D'ACCÈS AU SYSTÈME D'INFORMATION*

L'accès au système d'information de l'établissement est soumis à autorisation.

Ce droit d'accès est personnel et non cessible, même temporairement. Il engage la responsabilité individuelle de chaque utilisateur.

- La saisie du nom d'utilisateur permet l'**identification**
- La saisie du mot de passe **l'authentification**

Ces deux saisies donnent accès aux informations correspondant au **profil utilisateur.**

Pour les accès distants au système d'information hors site UNEOS, une double authentification est requise. Cette technique, appelée 2FA, à savoir, two-factor authentification, ou encore vérification en deux étapes, consiste à renforcer la protection du compte Utilisateur en ajoutant un second moyen d'identification. Cette double authentification s'appuie sur la solution Duo Mobile de Cisco.

Pour chaque Utilisateur, un profil de droit d'accès au système d'information du Groupe UNEOS est établi. Ce profil tient compte de la fonction, du service d'affectation, de la position hiérarchique et des différents domaines accessibles (Patient, Ressources Humaines, Gestion économique, Financière, Logistique, Internet, Messagerie électronique…).

Le droit d'accès est temporaire et limité à des activités conformes aux missions de l'établissement. Il est retiré ou modifié dans les cas suivants :

- l'utilisateur quitte l'établissement.
- la fonction de l'utilisateur ne le justifie plus.
- le non-respect de la présente Charte.

Pour toute attribution de droit d'accès complémentaires, (services internet, accès logiciel, accès messagerie…) ou de matériel supplémentaire (ordinateur portable, écran supplémentaire…). l'Utilisateur exprime sa demande auprès de son responsable hiérarchique. Ce dernier exprimera sa demande par écrit sur le logiciel de Gestion de parc Informatique GLPI.

L'obtention d'un droit d'accès au système d'information du Groupe UNEOS entraîne pour l'Utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous

⌘ *5-2 : USAGE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU ÉQUIVALENT)*

Chaque Utilisateur dispose de compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques du Groupe UNEOS. Ce compte est personnel et chaque Utilisateur est responsable de toute utilisation des ressources informatiques et connexions logicielles ou Internet réalisées à partir de ce compte

L'Utilisateur est donc personnellement responsable de l'utilisation qui peut en être faite et ne doit en aucun cas les communiquer.

Pour utiliser ce compte nominatif, l'Utilisateur dispose soit :

- d'un login et d'un mot de passe,
- utilise une carte CPS ou carte d'établissement équivalent et SSO (Single Sign One) (avec un code personnel)

Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé tous les 6 mois.

Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : collègues, stagiaires, intérimaires, hiérarchie, personnel en charge des systèmes d'information, même pour une situation temporaire.

Chaque Utilisateur est responsable de son compte et son mot de passe, et de l'usage qui en est fait. Il ne doit ainsi pas mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage.

La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médicales et médico-techniques, les applications administratives, le réseau, la messagerie, l'Internet… Il est ainsi possible pour l'établissement de vérifier *a posteriori* l'identité

de l'Utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

C'est pourquoi il est important que l'Utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de :

- fermer ou verrouiller sa session en cas d'absence momentanée
- ne jamais se connecter sur plusieurs postes à la fois
- éteindre son poste informatique en fin de cycle de travail (midi et soir)

Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors des mises en services ou formations Utilisateurs.

Il est strictement interdit d'usurper une identité en utilisant ou en tentant d'utiliser le compte d'un autre Utilisateur ou en agissant de façon anonyme dans le système d'information.

L'Utilisateur s'engage enfin à signaler au service informatique toute tentative de violation de son compte personnel.

⌘ *5-3 : CONFIDENTIALITÉ DE L'INFORMATION ET OBLIGATION DE DISCRÉTION*

Les personnels du Groupe UNEOS sont soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les Utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres Utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations de type courrier électroniques dont l'Utilisateur n'est ni directement destinataire, ni en copie.

Concernant les informations nominatives ou de santé, accessibles dans les dossiers patients informatisés ou autres supports (papiers), l'Utilisateur ne doit accéder qu'aux informations nominatives nécessaires à la prise en charge des patient dont il a la charge. La consultation de données administratives ou de santé en dehors de cette prise en charge est interdite.

L'accès aux données de santé à caractère personnel des patients par les professionnels habilités se fait avec un identifiant et un mot de passe strictement personnels

L'Utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

De même il ne doit pas disposer de copies locales d'informations nominatives de patient (sur disque fixe, disque externe ou clé USB…).

Les membres de l'équipe informatique qui peuvent être conduits par leur fonction à avoir accès à l'ensemble des informations relatives aux Utilisateurs ont obligation de préserver et garantir la confidentialité des informations identifiées qu'ils sont amenés à connaitre.

Toute prise en main à distance par un membre de l'équipe informatique nécessite l'accord préalable de l'Utilisateur du poste de travail.

⌘ 5-4 : PROTECTION DE L'INFORMATION

Les postes de travail du Groupe UNEOS permettent l'accès aux Utilisateurs autorisés, aux applications métier partagées du système d'information. (DIAMM, TELEMIS, JADE, QUALIAC, CERNER, PHARMA, OPTIM, suite bureautique etc).

Ces applications sont installées sur des serveurs centraux et les données sont stockées sur des baies de disques centralisées dans les salles informatiques sécurisées. Aucune donnée produite n'est stockée sur le poste de travail.

Les fichiers professionnels bureautiques produits de façon autonome en dehors des applications métier sont également stockés sur les répertoires des serveurs de fichiers centralisés. Ces fichiers ne doivent pas être stockés par l'Utilisateur sur des répertoires situés sur le disque dur du poste de travail.

Seuls les fichiers présents sur les baies de stockage centralisées sont inclus dans les procédures de sauvegardes mises en place par le service informatique du Groupe UNEOS.

Ces espaces de stockage sont réservés à usage professionnel uniquement. Le stockage de données personnelles sur ces disques réseau est interdit.

L'Utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement.

Périphériques de saisie mobiles, postes nomades :

Les « matériels nomades » (ordinateurs portables, assistants personnels numériques…) répondent aux mêmes dispositions que les matériels fixes quant aux conditions d'accessibilité (mots de passe) et stockage d'informations (pas de stockage sur disques locaux).

Aussi, les Utilisateurs habilités à utiliser des « postes nomades » s'engagent, quel que soit le lieu où ils se trouvent, à sécuriser leur matériel (surveillance, rangement…) et l'accès aux données qu'il contient (mot de passe, mise en veille..).

L'Utilisateur ne doit jamais transporter sur son matériel nomade des fichiers contenant des données nominatives (dossiers médicaux, comptes rendus, dossiers de personnels, etc.) ou qui auraient une valeur stratégique pour le Groupe UNEOS.

Périphériques de stockage amovibles :

Les supports de stockage amovibles comme les clefs USB, disques durs externes, cartes mémoires, CD ROM, etc. présentent des risques très forts pour la sécurité et la pérennité du système d'information du Groupe UNEOS (contamination par des programmes malveillants, risques de pertes de données…). Leur usage est donc par défaut interdit.

L'utilisation exceptionnelle de ces périphériques amovibles demande un contact préalable avec le service informatique pour vérification des supports .

L'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des matériels informatiques.

⌘ 5-5 : USAGE DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées du Groupe UNEOS (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels et de connecter de nouveaux matériels au réseau informatique de l'établissement.

Les configurations mises à disposition des Utilisateurs reposent sur des standards conformes aux règles juridiques, déontologiques et techniques applicables définies par le Groupe UNEOS (standards).

L'Utilisateur s'engage à ne pas modifier les configurations standards (matériels, réseaux, logiciels…) mises à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées de l'établissement (ou par son intermédiaire la société avec laquelle il a contracté).

À des fins de précaution, certaines configurations peuvent être verrouillées par l'Administrateur du Système d'Information (poste de travail, ordinateurs portables, accès réseau etc).

Les logiciels commerciaux acquis par l'établissement ne peuvent faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement.

Les ressources font parties du patrimoine de l'établissement, aussi, toute information émise, reçue ou stockée sur le poste de travail et les moyens de communication mis à disposition dans le cadre d'une utilisation professionnelle demeure la propriété du Groupe UNEOS à l'exclusion des données explicitement désignées par l'Utilisateur comme relevant de sa vie personnelle. Ainsi il appartient à l'Utilisateur de procéder au stockage éventuel de ses données à caractère personnel dans un répertoire explicitement prévu à cet effet et intitulé « personnel ». Ce répertoire n'entre pas dans les plans de sauvegarde du Groupe UNEOS.

Les Ressources mises à la disposition de tout Utilisateur pourront faire l'objet de vérifications et de contrôles par l'Administrateur du Système d'Information, conformément aux dispositions légales en vigueur.

⌘ 5-6 : USAGE DES OUTILS DE COMMUNICATION

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie sont destinés à un usage exclusivement professionnel.

L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de l'établissement de santé. Il ne doit en aucun cas être porté à la vue des patients ou de visiteurs et accompagnants.

Les outils de communication du Groupe UNEOS ne peuvent être utilisés à des fins promotionnelles à caractère privé

⌘ 5-6.1 : USAGE DU TÉLÉPHONE ET DU FAX

Le téléphone et le fax sont des moyens d'échanges de données qui présentent des risques potentiels, compte tenu du fait que l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.
Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l'identité de l'interlocuteur téléphonique.

La communication d'informations médicales (exemples : résultats d'examens…) aux patients et aux professionnels extérieurs est strictement réglementée. Les Utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'établissement en vigueur

⌘ 5-6.2 : USAGE D'INTERNET

L'accès à l'Internet a pour objectif d'aider les personnels à trouver des informations nécessaires à leur mission usuelle, ou dans le cadre de projets spécifiques.

NAVIGATEUR

L'Administrateur impose une identification nominative à la connexion internet et limite la durée de connexion de l'Utilisateur.

Il définit les configurations de sécurité du navigateur et des limites de taille au téléchargement de contenu.

PARTICIPATION À DES FORUMS, BLOGS, GROUPES DE DISCUSSION

La participation à des forums peut engager la responsabilité du Groupe UNEOS. Dans le cadre de forums professionnels (médicaux…), l'Utilisateur peut participer en son nom propre.

En revanche, pour participer et s'exprimer au nom du Groupe UNEOS, l'Utilisateur doit disposer des autorisations internes nécessaires délivrées par le Directeur Général du Groupe UNEOS.

UTILISATION DES RÉSEAUX SOCIAUX

L'accès et l'utilisation de réseaux sociaux type Facebook, Twitter, Copains d'Avant… est interdit.

TÉLÉCHARGEMENT DE LOGICIELS, OU D'ŒUVRES PROTÉGÉES

Le téléchargement de documents, de logiciels, de vidéo, images animées, fichiers musicaux, fichiers sons non liés à l'activité professionnelle est interdit.

Les téléchargements enfreignant le respect des droits d'auteur, de copie et d'utilisation sont interdits depuis les postes de service, tout comme les installations sous licence qui engagent la responsabilité de l'établissement.

Pour toute installation de programme ou logiciel, l'Utilisateur doit adresser une demande par GLPI au service informatique.

L'Administrateur se réserve la possibilité d'effacer du Système d'Information de l'Hôpital toute trace de ces fichiers, logiciels et œuvres introduites sans autorisation dans le Système d'Information de l'Hôpital.

CONSULTATION D'INTERNET À DES FINS PRIVÉES

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle sous réserve que la durée de connexion n'excède pas un délais raisonnable et présente un intérêt au regard des fonctions exercées ou des missions à mener.

Cependant l'accès Internet à des fins autres que professionnelles est toléré sous réserve que la durée de connexion n'excède pas un délai raisonnable, n'affecte pas la sécurité et le fonctionnement des réseaux et ne porte pas atteinte à l'intérêt et au bon fonctionnement du service.

Toute utilisation du Système d'Information du Groupe UNEOS à des fins de jeux est interdite.

CONSULTATION DE SITES ILLICITES

La consultation, le téléchargement , la diffusion à l'aide des ressources du Groupe UNEOS, notamment de contenu de sites à caractère pornographique, pédophile ou contraires aux bonnes mœurs ou susceptibles de porter atteintes au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs, sont des activités strictement interdites pouvant faire l'objet des sanctions prévues à l'article 8 de la présente Charte.

Ces sanctions sont applicables indépendamment des poursuites pénales et / ou civiles qui pourraient être intentées, eu égard au caractère infractionnel de certaines de ces activités.

Il est interdit d'accéder à des serveurs Web traitant de ces sujets. Si l'Utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt et d'informer le service informatique.

L'Utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc.

CONTRÔLES DE L'USAGE D'INTERNET

Le Groupe UNEOS a l'obligation de conserver des informations techniques de connexion.

L'Utilisateur est informé que l'Administrateur exerce un contrôle régulier sur les connexions et les sites visités, dans le cadre de la mission de protection du Système d'Information de l'établissement, du suivi fonctionnel et de la détection des abus conformément à la législation applicable.

Il est rappelé aux Utilisateurs que, lorsqu'ils « naviguent » sur l'Internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et à ne pas mettre en danger l'image ou les intérêts de l'établissement de santé.

Par ailleurs, les informations concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur…) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement.

Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

⌘ *5-6.3 : USAGE DE LA MESSAGERIE*

L'usage de la messagerie professionnelle est réservé au personnel habilité. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement et également les professionnels externes à l'institution.

UTILISATION DE LA MESSAGERIE À DES FINS PRIVÉES

L'utilisation de la messagerie électronique est réservée à un usage strictement professionnel Un usage privé de la messagerie est toléré s'il reste exceptionnel et il appartient au professionnel d'identifier les messages qui sont personnels.

Tout message envoyé ou reçu depuis un poste de travail mis à disposition par le Groupe UNEOS revêt un caractère professionnel sauf s'il est identifié comme étant « personnel ».La nature personnelle du message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

Tout message ou fichier qui n'est pas identifié comme « personnel » est réputé être professionnel donc accessible par l'Administrateur du Groupe UNEOS.

La messagerie électronique du Groupe UNEOS ne peut être utilisée pour des messages d'ordre commercial ou publicitaire, à des fins promotionnelles ou du prosélytisme.

L'usage des listes de diffusion doit être strictement professionnel.

ADRESSE ÉLECTRONIQUE

Chaque Utilisateur autorisé, dispose d'une adresse de messagerie électronique professionnelle composée généralement du prénom et du nom.

Les adresses de messagerie peuvent prendre deux formes :

- « prénom.nom@unoes.fr » pour les adresses individuelles,
- « nom du groupe ou du service@uneos.fr » pour les adresses regroupant plusieurs Utilisateurs ou adresses de service.

En cas d'homonymie, l'Administrateur fixera la règle d'attribution.

En cas de changement de nom, l'Utilisateur pourra demander à l'Administrateur une nouvelle adresse de messagerie électronique.

L'utilisation d'un pseudonyme ou l'usage d'un faux nom est expressément prohibé, sauf autorisation du Directeur Général qui s'assurera du bien-fondé de cette utilisation.

MESSAGE ÉLECTRONIQUE ET POUVOIRS INTERNES

Le message électronique est un écrit pouvant engager le Groupe UNEOS.

Les règles hiérarchiques et d'organisation des pouvoirs internes de signatures devront être respectées.

Aucun message électronique ne devra être envoyé par un Utilisateur à un destinataire extérieur au groupe UNEOS, si l'Utilisateur n'en a pas l'autorité.

CONTENU DU MESSAGE ÉLECTRONIQUE

La courtoisie constitue une des règles de base de l'utilisation de la messagerie, l'Utilisateur ne doit pas écrire un message qu'il s'interdirait d'exprimer oralement ou par tout autre moyen de communication.

Aucun message électronique ne devra comprendre des éléments de nature offensante, diffamatoire, injurieuse, et / ou contraires aux dispositions légales.

En effet, un message électronique peut :

- Être stocké, exploité, réutilisé à des fins auxquelles l'Utilisateur n'aurait pas pensé en le rédigeant,
- Constituer un commencement de preuve par écrit.
- Valoir offre ou acceptation de manière à former un contrat entre Le Groupe UNEOS et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

L'Utilisateur est seul responsable des contenus qu'il communique à tout tiers par l'intermédiaire du Système d'Information, quelle que soit la nature du contenu. Les Hôpitaux Privés de Metz ne sauraient être tenus pour responsables desdits contenus communiqués par l'Utilisateur.

PROTECTION DES INFORMATIONS

Les risques d'interception des messages électroniques exigent de limiter l'utilisation de la messagerie électronique à destination de l'extérieur du Système d'Information de l'Hôpital aux Informations à caractère non confidentiel, non stratégique et non sensible.

Si l'Utilisateur est contraint d'adresser à l'extérieur du Groupe UNEOS des informations contenant des données médicales nominatives ou permettant d'identifier directement ou indirectement une personne, il devra utiliser les procédures de transmission par messagerie sécurisée mise à disposition par le Groupe UNEOS.

FORMAT ET TAILLE DES MESSAGES ÉLECTRONIQUES

Afin de ne pas surcharger les serveurs de messagerie et les échanges réseau, les Utilisateurs doivent veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées.

Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé. Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

L'Administrateur limite le format, le type et la taille des messages électroniques y compris les pièces jointes envoyées.

Il est interdit d'envoyer des messages ne respectant pas le format, le type et la taille prescrits par l'Administrateur.

RÈGLES DE CONSERVATION DE LA MESSAGERIE

Le Groupe UNEOS incite l'Utilisateur à supprimer les messages contenus dans sa messagerie.

⌘ 5.7 IMAGE DE MARQUE DE L'ÉTABLISSEMENT

Les Utilisateurs de moyens informatiques ne doivent pas nuire à l'image de marque de l'établissement en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de l'établissement ou du fait de leurs accès à Internet.

CHAPITRE 6

INFORMATIQUE ET LIBERTÉS

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée par messagerie (dpo@uneos.fr) auprès du DPO du Groupe UNEOS, qui étudie alors la pertinence des données recueillies, la finalité du traitement, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le DPO procède ensuite aux opérations de déclaration et d'information réglementaires.

Il est rappelé que l'absence de déclaration de fichiers comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement.

En cas de non-respect des obligations relatives à la loi Informatique et Libertés, le DPO serait informé et pourrait prendre toute mesure temporaire de nature à mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

Conformément à la loi n°78-17 du 6 janvier 1978 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, modifiée par la loi n°2004-801 du 6 août 2004, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant.

CHAPITRE 7

SURVEILLANCE DU SYSTÈME D'INFORMATION

⌘ 7.1 CONTRÔLE

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

⌘ 7.2 TRAÇABILITÉ

L'Administrateur assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'il met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée
- Les informations ajoutées, modifiées ou supprimée des bases de données en réseau et/ ou des applications métier ;
- La durée de la connexion (notamment pour l'accès Internet)

Le personnel du service en charge du système d'information respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les Utilisateurs.

⌘ 7.2 ALERTES

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette Charte doit être signalé au Directeur du Système d'Information.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque Utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle des personnels soient respectées.

CHAPITRE 8

RESPONSABILITÉS ET SANCTION

Les règles définies dans la présente Charte ont été fixées par la Direction Générale de l'établissement de santé dans le respect des dispositions législatives et réglementaires applicables (CNIL, ANSI...).

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un Utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrites dans la Charte.

En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions laissées à la libre appréciation du Directeur Général eu égard à la gravité du ou des manquements constatés et /ou de leur éventuel caractère répétitif.

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, des moyens informatiques ainsi que des sanctions disciplinaires.
- Un licenciement et éventuellement des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction du Groupe UNEOS est tenue de signaler toutes infractions pénales commises par son personnel au procureur de la République.

CHAPITRE 9

AFFICHAGE ET FORMALITÉS – ENTRÉE EN VIGNEUR

En tant qu'annexe au Règlement Intérieur, la Charte de bon usage des technologies de communication du Groupe UNEOS sera affichée sur les panneaux réservés à l'affichage du règlement intérieur conformément à l'article R. 1321-1 du Code du travail.

La présente Charte fera l'objet de mises à jour et il appartient à l'Utilisateur de prendre connaissance de toute nouvelle version qui sera publiée sur l'Intranet du Groupe UNEOS et affichée aux panneaux réservés au règlement intérieur.

La présente Charte entrera en vigueur à compter de sa notification, dans la mesure où elle a été présentée préalablement pour avis au CSE dans la séance du 28/02/2023 et approuvée par le BCA dans la séance du 27/09/2023.

VALIDATION DE LA CHARTE

Rédaction	Validation	Approbation
BOUR Pierre	**BUSSEY Julie**	**DELPORTE Georges Hubert**
Directeur du Système Informatique	*Directeur Qualité et Communication*	*Directeur Général du Groupe Hospitalier Associatif UNEOS*

Ce document a été validé électroniquement.