SWISS MEDICAL NETWORK

DIRECTIVES RELATIVES A L'UTILISATION DE L'INFORMATIQUE ET DES INSTRUMENTS DE TELECOMMUNICATIONS

des établissements de

SWISS MEDICAL NETWORK SA à Genolier

I. GENERALITES

Art. 1 - Introduction

Les nouvelles technologies de l'information et des télécommunications (téléphones fixes et mobiles, postes de travail multifonctions, serveurs en réseau, messagerie électronique, Internet, etc.) permettent aux entreprises d'augmenter leur productivité et la qualité du service fourni. Pour corollaire, la mise à disposition de ces outils performants pose de nouvelles questions liées à leur utilisation tant du point de vue de la sécurité que des abus pouvant en découler.

L'Internet, ainsi que l'utilisation des réseaux informatiques rendent les entreprises vulnérables à des attaques informatiques venues de l'extérieur qui engendrent des risques tels que l'importation de virus, les attaques de hackeurs (pirates de l'informatique), la révélation de données confidentielles, la surcharge des ressources, etc.; en outre, ces technologies, toujours plus ergonomiques, faciles d'emploi et parfois ludiques, peuvent conduire à des utilisations abusives.

L'exploitation de réseaux informatiques peut notamment porter atteinte aux intérêts de la clinique des manières suivantes :

- capacité de mémoire et largeur de bande du réseau saturé suite à une exploitation excessive de l'Internet et du courrier électronique ;
- sécurité des données et de l'application (disponibilité, intégrité, confidentialité) par l'importation de virus, de vers, de chevaux de Troie ou par l'installation de programmes étrangers ;
- perte d'heures de travail et atteinte aux autres intérêts financiers (perte de productivité, augmentation des frais pour les moyens et/ou prestations supplémentaires, frais de réseaux, etc.) ;
- autres intérêts protégés par la loi, tels que la réputation, les secrets ou la protection des données.

Le présent document a pour but de mettre en place des règles relatives aux modalités d'utilisation des outils mis à disposition ; les postes de travail et autres systèmes de traitement de l'information ne peuvent être utilisés que dans le cadre des activités professionnelles. Une utilisation des ressources informatiques à but privé est tolérée, à condition que le collaborateur donne expressément et sans aucune réserve son consentement au contrôle de l'utilisation de l'informatique et des instruments de télécommunication, ainsi que du contenu des messages; une utilisation à but privé doit rester exceptionnelle et s'inscrire dans les limites du raisonnable.

Art. 2 - Sécurité des données

En complément des mesures de protection techniques, qui priment sur les contrôles personnels, la Direction établit des prescriptions d'utilisation dans le présent document. Le respect scrupuleux et consciencieux des présentes directives est un facteur capital pour garantir et améliorer le niveau de sécurité. Les présentes directives complètent les règles et prescriptions de comportement applicables d'une manière générale aux collaborateurs de la clinique.

SWISS MEDICAL NETWORK

Art. 3 - Champ d'application

Les présentes règles s'appliquent à toutes personnes utilisant l'informatique et les instruments de télécommunication de l'employeur dans le cadre d'un rapport hiérarchique avec celui-ci.

Elles s'appliquent également à toute autre personne soumise par voie contractuelle aux présentes règles.

L'utilisation de l'informatique et des instruments de télécommunication englobe le matériel personnel connecté au réseau informatique dans la mesure où une telle connexion est dûment autorisée le Responsable Informatique.

Art. 4 - Utilisation privée

Sous réserve de cas de force majeure, ou que le collaborateur a donné son accord aux contrôles mentionnés ci-dessus, l'utilisation à des fins privées de l'informatique et des instruments de télécommunication pendant le travail est interdite.

L'utilisation à des fins privées de l'informatique et des instruments de télécommunications est tolérée en dehors des heures de travail à condition que :

- le collaborateur donne expressément et sans aucune réserve son consentement au contrôle de l'utilisation de l'informatique et des instruments de télécommunication, ainsi que du contenu des messages ;
- la fréquence et la durée qui sont consacrées soient minimes et qu'elle n'entraîne qu'une utilisation négligeable des ressources informatiques ;
- elle ne compromette pas l'activité professionnelle ;
- elle n'entrave pas l'activité de l'employeur ;
- elle ne relève pas d'une activité lucrative privée ou de propagande politique ;
- elle ne soit pas contraire à la bienséance ou à la décence

Art. 5 - Définitions

On désigne par :

- « activité professionnelle » : celle prévue par le cahier des tâches du collaborateur et/ou celle réellement effectuée ;
- « moyens de télécommunication » : l'ensemble des téléphones fixes et mobiles ;
- «système d'information» : l'ensemble des moyens techniques, humains et organisationnels permettant à l'employeur de recueillir, conserver, traiter, distribuer et présenter les informations relatives à son activité quels que soient les formes et les supports ;
- « ressources informatiques » : les moyens informatiques (matériel, logiciels et télématique) et de gestion, centraux ou locaux, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade, à partir du réseau de l'employeur ;
- « service Internet » : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations tels le web, les forums, etc.

Art. 6 - Equipement informatique et instruments de télécommunications

L'équipement téléphonique est constitué de téléphones fixes et mobiles.

L'équipement informatique est constitué par du hardware (ensemble des appareils et du matériel informatiques en général) et par des software (ensemble des programmes informatiques). Les équipements informatiques de la clinique sont principalement composés :

- d'ordinateurs fixes et portables ;
- de câbles et d'éléments actifs sur le réseau ;
- de périphériques (imprimantes, écrans, claviers, souris, scanners, modems, etc.) ;
- de logiciels et de progiciels ;
- de tous équipements connexes ou annexes aux précédents ;

permettant le traitement[1] de données, ainsi que l'échange de celles-ci entre utilisateurs internes (collaborateurs) et / ou avec des utilisateurs externes (clients, fournisseurs et tous tiers à la clinique).

[1] Toute opération relative à des données, notamment la collecte, la conservation, la copie, l'exploitation, la modification, la communication, l'archivage ou la destruction

SWISS MEDICAL NETWORK

Art. 7 - Utilisation des moyens de télécommunications et des ressources informatiques

L'informatique et les instruments de télécommunications servent en premier lieu aux buts professionnels, c'est-à-dire à l'accomplissement des tâches attribuées.

L'utilisation de l'informatique et des instruments de télécommunication doit respecter le principe de disponibilité, d'intégrité et de confidentialité.

L'usage abusif de l'informatique et des instruments de télécommunications peut donner lieu à des sanctions internes, civiles et pénales.

Art. 8 - Accès à l'informatique et aux instruments de télécommunications

Les moyens informatiques sont installés, configurées, exploités, maintenus et modifiés exclusivement par les personnes autorisés avec l'accord du Responsable Informatique, conformément à ses directives et standards.

L'accès à l'informatique et aux instruments de télécommunications est strictement personnel, lié à la fonction et intransmissible.

Art. 9 - Responsabilité

Chaque collaborateur est personnellement responsable de l'utilisation de l'informatique et des instruments de télécommunications mis à sa disposition. Il doit, à son niveau, contribuer à la sécurité générale et s'abstenir en particulier de :

- perturber le bon fonctionnement ;
- modifier les paramètres régissant la sécurité (navigateurs, clients messagerie, postes de travail, etc.) ;
- contourner, de quelque façon que ce soit, les mesures de sécurité.

Il est interdit de se livrer à des actes mettant sciemment en péril la sécurité ou le bon fonctionnement d'autres sites et de réseaux de télécommunications.

Dans le cadre d'une utilisation privée des ressources informatiques et des moyens de télécommunication, le collaborateur n'émet pas d'opinions personnelles susceptibles de porter préjudice à l'employeur. Si des opinions personnelles doivent être exprimées, il est explicitement précisé que cette opinion est personnelle et qu'elle n'engage en aucune manière la responsabilité de l'employeur.

Il est interdit de traiter des informations à caractère contraire notamment à l'honneur, au racisme, à la pornographie et à la pédophilie.

Art. 10 - Droit d'accès

Tout ordinateur nécessite de la part de son utilisateur une identification personnelle et un droit d'accès.

Le nom d'utilisateur et les mots de passe sont confidentiels et strictement personnels. Les règles suivantes sont applicables concernant les mots de passe :

- L'utilisateur doit le mémoriser ;
- L'utilisateur n'en garde aucune trace écrite à sa place de travail; le mot de passe ne doit être écrit que pour dépôt, devant être gardé en sécurité dans une enveloppe fermée ;
- Le collaborateur ne doit divulguer à personne son mot de passe ;
- Le collaborateur s'abstient de choisir des combinaisons de chiffres ou de lettres dont l'identification est trop aisée (date de naissance, plaque de voiture, nom, prénom, numéro de téléphone, etc.) ;
- Les mots de passe prédéfinis tels ceux du fabricant au moment de la livraison du système doivent être remplacés par des mots de passe individuel ;
- En cas de découverte ou de soupçon de découverte par une tierce personne du mot de passe, l'utilisateur doit demander immédiatement un nouveau code d'accès au service informatique ou le changer lui-même s'il en a l'autorisation ;
- Les mots de passe ne doivent pas être enregistrés sur les touches de fonction programmables ;
- L'entrée du mot de passe doit se faire sans observation ;
- L'ordinateur doit toujours être protégé de l'accès de tiers lorsque l'utilisateur s'éloigne de sa place de travail.

Il est absolument interdit à toute personne soumise aux présentes règles d'essayer de s'initialiser sur un ordinateur pour lequel un accès ne lui a pas expressément été donné ou d'essayer d'introduire un mot de passe pour entrer dans un compte utilisateur autre que le sien. Il est convenu entre les parties que toute tentative constitue un abus en soi.

Le collaborateur signale à son supérieur toute tentative de violation de son compte et, de façon générale, toute anomalie constatée.

Le collaborateur est personnellement responsable de ses informations, du bon usage de ses droits d'accès aux ressources informatiques, notamment son poste de travail, la messagerie et Internet et des droits donnés à d'autres personnes. Comme pour toute opération informatique, une action effectuée sous une identification (login, mot de passe) est attribuée au (à la) propriétaire du mot de passe. Toute activité, même inadmissible est donc attribuée à l'utilisateur annoncé.

Le collaborateur peut, exceptionnellement et avec l'accord du Responsable Informatique, donner ses droits à un autre collaborateur. Dès que le motif de la transmission des droits a disparu, l'identification personnelle doit être changée.

Art. 11 - Supports de données privés ou étrangers

L'intégration de matériel privé ainsi que de supports de données privés ou étrangers est interdit dans le réseau de la clinique, sous réserve du consentement préalable écrit du Responsable Informatique.

L'utilisation de moyens de stockage dit mobile ou amovible (par exemple CD-R, DVD-R, disquette, disque dur externe, caméra numérique, clé USB, etc.) par interface (par exemple USB) est uniquement permise avec le consentement écrit préalable du Responsable Informatique. Dans ce cas, le collaborateur doit cependant s'assurer préalablement que ce support de données n'est pas infecté par un virus; il assume la responsabilité de procéder aux contrôles correspondants. Il est interdit d'installer des jeux sur les ordinateurs de l'employeur.

En cas de découverte de virus sur un stockage amovible, ce dernier doit être immédiatement retiré et ne doit plus être utilisé sur le poste de travail auquel il a été connecté et tout autre poste de travail du réseau informatique. L'utilisateur qui a connecté cet équipement doit immédiatement avertir le Responsable Informatique qui effectuera les opérations de nettoyage nécessaire.

Art. 12 - Supports de données devenus inutiles

Les supports de données devenus inutiles doivent être traités de manière à exclure toute possibilité d'utilisation abusive par des tiers des données qu'ils contiennent. Le collaborateur est rendu attentif au fait qu'un simple effacement de ces données est insuffisant.

Art. 13 - Logiciels

Il est strictement interdit d'installer ou d'utiliser d'autres logiciels que ceux agréés par le Responsable Informatique et régulièrement acquis conformément au processus d'achat en vigueur.

L'installation des logiciels est réservée aux seules personnes habilitées à y procéder, à savoir le Service Informatique.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le contrat d'achat.

Le collaborateur qui contrevient aux règles mentionnées ci-dessus engage directement sa responsabilité personnelle.

Art. 14 - Matériel

Il est interdit au collaborateur de procéder à toute modification physique de l'informatique et des instruments de télécommunications, en particulier à échanger ou à installer des composants.

Art. 15 - Procédure en cas d'acte délictueux

Si un responsable hiérarchique dispose d'éléments donnant lieu de soupçonner qu'un délit a été commis lors de l'utilisation de l'informatique et des instruments de télécommunications, de la messagerie électronique ou d'Internet, il fait sauvegarder les preuves, c'est-à-dire les fichiers journaux, et, éventuellement les sauvegardes (backups) qui, le cas échéant, seront remis aux autorités judiciaires

compétentes.

La Direction décide si une plainte pénale est déposée.

La Direction s'engage à traiter confidentiellement le résultat des enquêtes, en particulier à ne pas le divulguer aux autres collaborateurs.

La violation des règles relatives à l'utilisation de l'informatique et des instruments de télécommunications peut faire l'objet de sanctions disciplinaires ainsi que d'une demande de réparation civile du préjudice subi.

Art. 16 - Sécurité

Pour garantir la sécurité de l'utilisation de l'informatique et des instruments de télécommunications, des mesures techniques de protection doivent être mises en œuvre. Elles sont constamment adaptées en fonction des défauts constatés.

Les moyens informatiques sont installés, configurés, exploités, maintenus et modifiés exclusivement par les personnes autorisées, soit les collaborateurs du Service Informatique ou les partenaires, conformément aux directives et au standard.

Art. 17 - Obligation de déclarer

Le collaborateur est tenu d'informer immédiatement le Responsable Informatique de toute manipulation, perte ou utilisation non autorisée des moyens informatiques et de communication par des tiers, ainsi que de tout message suspect.

Art. 18 - Dérangement technique

Lorsqu'un dérangement technique met en péril la bonne marche de l'informatique et des instruments de télécommunications, le Responsable Informatique est autorisé à prendre toutes les mesures nécessaires à son rétablissement. Les fichiers journaux peuvent être analysés afin d'établir le diagnostic de la panne.

L'administrateur système produit un rapport d'incident à l'intention du responsable de la sécurité informatique.

Art. 19 - Traces sur la station de travail

Les multiples traces laissées par le navigateur sur la station de travail lors d'un accès à Internet ainsi que celles laissées par le système d'exploitation et les applications sur la station de travail lors de son utilisation ne sont pas collectées à des fins de contrôle, mais peuvent être exploitées lors d'une enquête judiciaire ou interne.

Art. 20 - Signature scannée

L'utilisation de signatures scannées est interdite en raison du risque d'abus.

II. DONNEES PERSONNELLES DU COLLABORATEUR

Art. 21 - Protection des données

Certains collaborateurs peuvent être autorisés à accéder aux données personnelles d'autres collaborateurs de la clinique en fonction de motifs justifiés. Dans ce contexte, l'employeur doit respecter et protéger la personnalité de ses collaborateurs.

Les données personnelles sont toutes les données se référant à une personne définie ou définissable.

On entend par traitement dans le sens de la protection des données toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, comportant notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données. La collecte de données comprend aussi la surveillance, si certaines opérations peuvent être attribuées à une personne individuelle.

Les données ne doivent pas être communiquées à des tiers non autorisés sans le consentement des personnes concernées ou un motif justifié.

En cas d'infraction, l'employeur peut être sanctionné notamment dans les cas suivants:
- traitement illicite de données ;
- surveillance abusive des collaborateurs ;
- contrôle inadmissible par exemple par des programmes espions.

Les collaborateurs sont personnellement responsables de ne pas commettre les infractions précitées.

Art. 22 - Traitement des données personnelles

Le collaborateur autorise l'employeur à traiter les informations qui le concernent sur ses installations informatiques.

L'employeur garantit au collaborateur que les données personnelles le concernant sont traitées de manière licite - conformément aux dispositions de la Loi fédérale sur la Protection des Données du 19 juin 1992 (LPD) - et il l'assure plus particulièrement du respect des principes suivants :
- le traitement des données personnelles est réalisé selon le principe de la bonne foi ;
- le traitement des données personnelles est proportionnel au but visé et se limite à ce qui est nécessaire ;
- le traitement des données personnelles respecte le but pour lequel les données ont été collectées ;
- les données traitées sont protégées par des mesures techniques et organisationnelles contre la perte et le traitement non autorisé ;
- les collaborateurs dont les données personnelles sont traitées ont un droit d'accès qui inclut celui de faire corriger les inexactitudes.

Art. 23 - Procédure d'accès aux données personnelles et corrections des inexactitudes

Les collaborateurs ont le droit d'être renseignés sur le contenu de leur dossier personnel; ils peuvent en faire usage en respectant la procédure suivante :
- le collaborateur fait une demande d'accès par écrit ;
- le collaborateur peut consulter son dossier auprès des Ressources Humaines au plus tôt le jour qui suit sa demande ;
- le cas échéant, le collaborateur notifie par écrit sa demande de correction ;
- l'employeur procède à la rectification justifiée dans les 8 jours qui suivent la demande et en informe le collaborateur.

Afin de sauvegarder l'intérêt prépondérant de l'employeur, les collaborateurs n'ont aucun droit d'accès aux notes que l'employeur a établies à des fins personnelles et qui ne sont pas communiquées à des tiers. Ils ne peuvent pas non plus consulter les dossiers relatifs à la planification du personnel ou aux plans de carrières, ni ceux qui concernent les procédures en cours.

III. CONTRÔLE DES MOYENS DE TELECOMMUNICATIONS FIXES ET MOBILES

Art. 24 - Surveillance

La surveillance des données techniques par l'employeur, effectuée sur une base régulière, sert à vérifier si les présentes règles sont observées. Elle peut porter sur les données suivantes :
- numéro complet de la personne qui appelle ;
- numéro complet d'appels sortants ;
- date et heure des connexions ;
- durée ;
- coût des communications ;
- indication sur la nature de la connexion (réseau fixe ou mobile) ;
- indication sur la région de tarification (communications nationales ou internationales).

Les données techniques concernant les communications téléphoniques sont conservées dans la règle pendant une durée de six mois.

SWISS MEDICAL NETWORK

Art. 25 - Ecoute des conversations professionnelles

L'écoute ou l'enregistrement des conversations professionnelles par l'employeur sont admises dans le but d'obtention de preuve et de contrôle de performance. Sous réserve de l'exception mentionnée ci-dessous, l'écoute et l'enregistrement des conversations sont subordonnés au consentement de tous les participants. Les personnes dont la conversation est enregistrée ou mise sur écoute doivent en être informées sans ambiguïté et en temps utile.

L'employeur peut conserver les enregistrements jusqu'à ce que le but recherché soit atteint et il les détruit ensuite.

Art. 26 - Surveillance en cas d'infraction

Lorsque l'employeur a de bonnes raisons de soupçonner qu'une infraction a été commise ou va être commise par téléphone, il s'assure de la journalisation des données techniques liées à l'usage du téléphone. Si les soupçons peuvent reposer sur un comportement qui, au-delà d'un manquement au contrat de travail ou au règlement concernant l'utilisation du téléphone, remplit les conditions d'une l'infraction, par exemple une atteinte à la réputation de l'employeur ou en cas de harcèlement sexuel sur le lieu de travail, l'employeur n'a aucune obligation de dénonciation ; cependant, afin d'éviter tout risque de complicité, il dénonce les infractions poursuivies d'office.

Art. 27 - Enregistrement de conversations téléphoniques dans les relations d'affaires

Lorsqu'une affaire s'effectue en masse et qu'une certaine rapidité est nécessaire, l'enregistrement des conversations téléphoniques, dans le cadre des affaires, n'est pas punissable lorsque la conversation porte sur des commandes, des mandats, des réservations ou d'autres transactions commerciales de même nature; il est en de même lorsque la conversation implique des services d'assistance, de secours ou de sécurité. Ni information préalable au sujet de l'enregistrement, ni consentement de la personne concernée ne sont requis dans ces cas.

Ces enregistrements ne peuvent être utilisés que pour leur valeur de preuve. La transmission de tels enregistrements à des tiers reste punissable.

IV. CONTRÔLE DE LA STATION INFORMATIQUE

Art. 28 - Analyse de configuration

Lors d'inventaires effectués périodiquement, il convient de procéder à des analyses de la configuration de la station de travail pour en recenser les composants matériels, les périphériques et les logiciels.

Les informations concernant l'inventaire sont conservées tant qu'elles sont pertinentes.

Le Responsable Informatique communique à la Direction les éléments laissant présumer d'un abus.

Art. 29 - Enregistrement des sessions

Pour chaque session avec un serveur, les données suivantes sont enregistrées :
- identité de l'utilisateur ;
- date et heure du début de la session ;
- date et heure de fin de la session ;
- volume des données sur le serveur.

En plus, lorsque l'on accède de l'extérieur au réseau interne de l'employeur par une connexion sécurisée à distance, les données suivantes sont enregistrées :
- identité de l'utilisateur ;
- date et heure du début de la connexion ;
- date et heure de la fin de la connexion.

Ces données sont conservées durant une période de 6 mois. Au-delà de cette période, elles sont détruites ou anonymisées et ne peuvent plus être utilisées à des fins de contrôle.

Elles peuvent être conservées dans le cas où une enquête judiciaire est ouverte avant la date d'échéance. Les données sont détruites à l'issue de la procédure.

SWISS MEDICAL NETWORK

Art. 30 - Ordinateur mobile

Toutes les données commerciales gérées par les ordinateurs mobiles doivent être enregistrées sur les unités de serveur de la clinique selon les procédures et explications définies par le Responsable Informatique ; cette mesure assure que les données sont intégrées dans le cycle de la sauvegarde de la clinique.

En dehors du réseau de la clinique, les ordinateurs mis à disposition des collaborateurs dits « mobiles » ne doivent être utilisés pour accéder à l'Internet public ou à un autre réseau qu'à des fins commerciales et dans une mesure limitée au strict minimum. Il est interdit de remettre l'ordinateur à des tiers (amis, connaissances, famille etc.). De plus, toute modification au niveau de la configuration est interdite sans l'autorisation du Responsable Informatique. Dans le principe, les connexions mises à disposition par GSMN sont à utiliser.

Par ailleurs, les dispositions générales du règlement d'utilisation des moyens informatiques font foi.

V. CONTRÔLE DES ESPACES DE STOCKAGE

Art. 31 - Analyse du contenu des espaces de stockage

Des contrôles sur le contenu des espaces de stockage (locaux et en réseau) sont effectués régulièrement pour en vérifier le bon usage.

Les informations collectées sont :
- la localisation du fichier ;
- sa taille ;
- son propriétaire ;
- son type ;
- la date de création ;
- la date de dernière utilisation.

Art. 32 - Droit d'accès

Nulle autre personne que son titulaire ne peut accéder à un espace de stockage de service si elle n'est au bénéfice des droits nécessaires.

L'employeur peut, dans le cadre de son pouvoir de contrôle, consulter les espaces de stockage professionnels. Il est autorisé à ouvrir les fichiers des collaborateurs pour y extraire les informations professionnels.

Si aucune indication ne permet de distinguer les fichiers privés des fichiers professionnels et que les éléments ne permettent pas de déterminer si le fichier est de nature privée ou non, l'employeur part du principe, comme il le ferait pour un courrier postal, que le fichier est de nature professionnelle.

Art. 33 - Confidentialité

Les informations confidentielles doivent être codées si elles sont stockées sur des espaces de stockages en dehors de la clinique.

Art. 34 - Protection antivirus

Tous les fichiers traités doivent être analysés par un logiciel antivirus. Les fichiers suspectés de contenir un virus, ainsi que ceux dont l'analyse n'a pas été possible, sont mis en quarantaine. Dans ce cas, l'utilisateur en est avisé.

Art. 35 - Sauvegarde des espaces de stockage

Pour répondre aux exigences de continuité d'exploitation et de sauvegarde de preuves dans le cas d'enquêtes pénales, le contenu des espaces de stockages mis à disposition de l'utilisateur est sauvegardé régulièrement. Les sauvegardes doivent être définitivement détruites après 24 mois. La restauration de l'intégralité des fichiers est décidée par la Direction.

La restauration d'un espace de stockage spécifique peut être effectuée à la demande écrite de son propriétaire.

Lors d'une enquête pénale, l'autorité judiciaire peut demander la restauration d'un espace de stockage et accéder à l'intégralité de son contenu.

VI. UTILISATION ET SECURITE DE LA MESSAGERIE

Art. 36 - Utilisation

La messagerie électronique est réservée à un usage professionnel.

Les envois de masse à des fins privées, la propagation de messages « chaînés » et de fausses rumeurs (Hoax) sont interdits.

Les abonnements à des « Newsletter » ou listes de distribution doivent être en rapport avec l'activité professionnelle.

La diffusion de documents électroniques de l'employeur est réservée à l'usage professionnel.

Art. 37 - Messagerie électronique

Les boîtes aux lettres électroniques de la clinique, malgré le caractère personnel de leur adresse, peuvent être ouvertes par différents collaborateurs afin de ne pas arrêter, notamment en cas d'absence du titulaire, la nécessaire circulation de l'information. Les mentions suivantes doivent être utilisées concernant la confidentialité ou le caractère privé d'un mail :

- confidentiel : un mail dont le « concerne » contient ce mot peut être ouvert uniquement par les collaborateurs ayant un accès explicite, en lecture, à la boîte aux lettres. L'information doit alors être traitée de la même manière qu'un courrier papier initialisé comme « confidentiel ».
- privé : un mail dont le « concerne » contient ce mot ne peut être ouvert que par la personne à qui le mail est destiné (celle dont le nom figure dans le texte ou fait partie de la désignation de la boîte aux lettres). Il ne doit, dans ce cas, contenir aucune information professionnelle.

Les collaborateurs sont responsables d'informer les personnes susceptibles de leur faire parvenir exceptionnellement des messages à caractère privé de la manière de rédiger le titre du message. Ils ne peuvent en aucun cas se retourner contre l'employeur ou un collègue si un message mal libellé est ouvert par erreur.

Le Responsable Informatique se réserve le droit de prendre des mesures techniques et organisationnelles adéquates pour éviter des abus.

Art. 38 - Droit d'accès

Nulle autre personne que son titulaire ne peut accéder à une boîte aux lettres de service si elle n'est au bénéfice des droits nécessaires.

L'employeur peut, dans le cadre de son pouvoir de contrôle, consulter les messages professionnels reçus par courrier électronique. Il est autorisé à ouvrir la boîte aux lettres électroniques des collaborateurs absents pour y extraire les messages professionnels déjà reçus et introduire une réponse automatique renseignant les futurs expéditeurs sur l'absence du titulaire et l'adresse de son remplaçant.

Si aucune indication ne permet de distinguer les messages privés des messages professionnels et que les éléments d'adressage ne permettent pas de déterminer si le message est de nature privée ou non, l'employeur part du principe, comme il le ferait pour un courrier postal, que le message est de nature professionnelle.

Art. 39 - Utilisation des systèmes de messagerie tiers

L'utilisation de systèmes de messagerie personnels disponibles à travers des services de messagerie, tels que gmail, hotmail, bluewin, etc., est strictement interdit depuis le réseau de l'employeur.

L'utilisation d'une messagerie privée pour un usage professionnel est tolérée en dehors des heures de travail et pendant la pause, pour autant que le contenu du message n'engage pas l'employeur vis-à-vis de tiers et que les autres conditions des présentes directives sont remplies.

SWISS MEDICAL NETWORK

Art. 40 - Confidentialité

Les informations confidentielles doivent être codées si elles sont transmises par messagerie en dehors de la clinique.

Art. 41 - Signature et authentification

Les messages qui contiennent un engagement juridique ou financier de l'employeur doivent être certifiés par un moyen d'authentification expressément autorisé, communiqué au destinataire indépendamment de la transmission des données, et conforme au droit de signature en vigueur.

VII. CONTROLE DE LA MESSAGERIE

Art. 42 - Protection antivirus

Tous les messages émis ou reçus doivent être analysés par un logiciel antivirus. Les messages suspectés de contenir un virus, ainsi que ceux dont l'analyse n'a pas été possible, sont mis en quarantaine. Dans ce cas, l'expéditeur ou le destinataire en est avisé.

Art. 43 - Taille des messages

Tous les messages émis ou reçus dépassant la taille maximale autorisée sont rejetés. Dans ce cas, l'expéditeur ou le destinataire en est avisé.

Art. 44 - Type d'attachement

Le Responsable Informatique définit les types d'attachement autorisés.

Tous les messages reçus contenant une pièce jointe de type non autorisé, dont l'expéditeur est inconnu ou dont l'extension est inusitée ou peu plausible, sont mis en quarantaine puis supprimés après une certaine période. Dans ce cas, le destinataire est avisé qu'il lui est possible de récupérer la pièce jointe pour autant que l'activité professionnelle le justifie.

Art. 45 - Vérification de la taille de la boîte aux lettres

Le Responsable Informatique fixe la taille maximale autorisée pour chaque boîte aux lettres. Lorsque cette limite est presque atteinte, un message est envoyé invitant à nettoyer la boîte aux lettres. Au-delà de cette limite, l'usage de la boîte aux lettres est restreint.

Art. 46 - Enregistrement des transactions

Pour chaque message reçu ou envoyé, les données suivantes sont enregistrées :

- l'expéditeur
- le destinataire
- date et heure de la transaction
- taille du message (pièce jointe incluse).

Ces données sont conservées durant une période de 6 mois. Elles ne sont plus utilisées à des fins de contrôle au-delà de cette période.

Le contenu des messages n'est pas inclus dans la journalisation des transactions.

Art. 47 - Sauvegarde des messages

Pour répondre aux exigences de continuité d'exploitation et de sauvegarde de preuves dans le cas d'enquêtes pénales, le contenu des boîtes aux lettres est sauvegardé régulièrement. Les sauvegardes doivent être définitivement détruites après 24 mois. La restauration de l'intégralité des messages est décidée par l'employeur.

La restauration d'une boîte aux lettres spécifique peut être effectuée à la demande écrite de son propriétaire.

Lors d'une enquête pénale, l'autorité judiciaire peut demander la restauration d'une boîte aux lettres et accéder à l'intégralité de son contenu.

Art. 48 - Départ définitif d'un collaborateur

En cas de départ planifié d'un collaborateur, l'employeur s'assure que, au jour de son départ, sa boîte aux lettres a été vidée de tout message personnel et que le contenu professionnel a été transmis dans le cadre de la remise des dossiers (papiers, fichiers, etc.).

En cas de départ avec effet immédiat, le nettoyage de la boîte aux lettres s'effectue en présence de la personne concernée sous le contrôle de l'employeur.

A l'issue de cette procédure, l'employeur fait désactiver la boîte aux lettres et met à jour l'annuaire de la messagerie.

Art. 49 - Absence prolongée

En cas d'absence prolongée, l'employeur doit s'assurer que la personne a pris les mesures nécessaires à la continuité des activités du service, tels que la délégation des droits d'accès, l'avis d'absence informatique, etc. Si des mesures adéquates n'ont pas été prises, l'employeur doit veiller à ce que les mesures nécessaires soient prises.

VIII. UTILISATION D'INTERNET

Art. 50 - Utilisation

L'accès à Internet est réservé à un usage professionnel. Pour des raisons de sécurité, il peut être limité à des sites de confiance sur la base d'une liste préétablie et régulièrement mise à jour par la Direction et le Responsable Informatique.

Il est expressément interdit:

- D'accéder ou de divulguer des contenus illicites, violant le droit d'auteur, érotiques, pornographiques, pédophiles, insultants, violents, racistes ou humiliants;
- D'interroger, d'ouvrir et/ou de télécharger des e-mails existants dans des comptes e-mail privés de tiers pourvoyeurs (gmail, bluewin, bluemail, etc.) à moins que l'opération ne soit effectuée par un collaborateur du Service Informatique dans le cadre de l'exécution des tâches qui lui sont attribuées;
- D'utiliser des moyens interactifs (par exemple chat, messagerie);
- D'effectuer des transactions financières (notamment l'utilisation de sites payants).

Art. 51 - Pages personnelles

La création de sites ou de pages à des fins non professionnelles est interdite.

Art. 52 - Fourniture d'informations

Le collaborateur ne doit pas utiliser les services Internet pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contrevenant à la législation.

Art. 53 - Téléchargement

Le téléchargement d'informations depuis Internet est réservé à l'activité professionnelle. Il doit être réduit au strict minimum et ne provenir que de sites autorisés ou de sources sûres.

IX. CONTRÔLE D'INTERNET

Art. 54 - Contrôle

Pour contrôler le respect des présentes directives, la journalisation est effectuée sous forme anonyme ou pseudonyme. L'évaluation anonyme représente l'analyse statistique des journalisations. Cette évaluation ne permet pas d'identification et est effectuée en permanence.

Lors de l'évaluation pseudonyme, il n'est pas possible de tirer des conclusions directes sur l'utilisateur. Ce genre d'évaluation n'est effectué qu'à titre de contrôle aléatoire. Pour garantir le pseudonyme, les journalisations et la liste des correspondances (liste permettant de retracer une personne) sont gardées

séparément, physiquement aussi bien que fonctionnellement.

Si un abus est relevé lors des évaluations anonymes ou pseudonymes, ou s'il existe des soupçons d'abus, les évaluations des journalisations sont effectuées nominalement par renouement avec la liste des correspondances. On entend par abus une violation du règlement d'utilisation ou d'une autre réglementation qui sera sanctionné. Si les soupçons d'abus ne se corroborent pas, l'évaluation nominale de la journalisation est suspendue immédiatement.

Art. 55 - Filtrage

L'accès depuis le réseau est bloqué aux sites sans aucune pertinence ou qui ne sont pas utilisés pour l'activité professionnelle, notamment ceux ayant pour thème la pornographie, la pédophilie, le racisme et la violence.

Art. 56 - Limitation des fonctionnalités

L'accès à certaines fonctionnalités d'Internet peut être bloqué.

Art. 57 - Enregistrement des transactions

Pour chaque communication avec Internet, les données suivantes sont enregistrées :
- identité de l'utilisateur (dans certains cas)
- adresse IT de l'émetteur
- adresse IP du destinataire
- date et heure de la transaction
- URL du destinataire
- taille du message.

Ces données sont conservées durant une période de 6 mois. Au-delà, elles sont détruites ou anonymisées et ne peuvent plus être utilisées à des fins de contrôle. Elles peuvent être conservées au-delà de cette échéance dans le cas où une enquête judiciaire est ouverte avant la date d'échéance. Les données sont détruites à l'issue de la procédure.

X. DISPOSITIONS FINALES - SANCTIONS

Art. 58 - Généralités

Le non respect des règles énoncées dans le présent document, en particulier celles relatives à :
- la diffusion d'informations confidentielles ;
- la consultation de sites non autorisés ;
- la destruction ou la soustraction, par négligence ou volontaire, d'informations et de matériel ;
- la tentative d'accès non autorisé à des informations ou à du matériel ;
- les chargements de fichiers et de programmes ayant entraîné des problèmes techniques ;
- l'utilisation de l'informatique pour développer une activité concurrente à la clinique ;
- l'utilisation de la messagerie à des fins de harcèlement sexuel ou psychologique ;
- l'utilisation de la messagerie ou d'Internet à des fins privées ;
- la destruction d'informations par méconnaissance des règles énoncées ;

est considéré comme une faute professionnelle et sanctionné par l'employeur.

En cas de contravention aux présentes directives, la Direction peut initier des sanctions contre les contrevenants. L'accès à l'informatique et des instruments de télécommunications peut être restreint (par exemple par barrage de l'accès Internet) une réprimande peut être signifiée ou, en cas de faute grave, le contrat de travail peut être résilié avec effet immédiat pour de justes motifs au sens de l'art. 337 CO. La sanction est proportionnelle à la gravité de la faute.

Art. 59 - Protection des données

Les violations du traitement des données d'entreprise et personnelles, les secrets commerciaux ainsi que de la personnalité des personnes physiques et morales peuvent entraîner des sanctions civiles et pénales en application de la loi fédérale sur la concurrence déloyale (LCD) et de la loi fédérale sur la protection des données (LPD).

SWISS MEDICAL NETWORK

Art. 60 - Droit d'auteur

Lorsque des œuvres sont protégées par le droit d'auteur, tels des programmes informatiques, des textes, des images, des graphiques, des photographies, de la musique, des œuvres d'art, des logos, etc., elles jouissent d'une protection absolue. Toute violation du droit d'auteur peut entraîner des sanctions civiles et/ou pénales.

Art. 61 - Droit pénal

Le code pénal prévoit des sanctions notamment dans les cas suivants :

- Soustraction de données ;
- Accès indus à un système informatique ;
- Détérioration de données ;
- Utilisation frauduleuse d'un ordinateur.

Par ailleurs, lors de l'utilisation d'Internet, il existe un risque d'infractions pénales, notamment dans les cas suivants :

- Représentation de la violence ;
- Diffamation ;
- Calomnies ;
- Pornographie ;
- Provocation publique au crime ou à la violence ;
- Atteinte à la liberté de croyance et des cultes ;
- Discrimination raciale.

Art. 62 - Réparation de préjudice

Tout acte contrevenant aux règles mentionnées dans les présentes directives et/ou provoquant des dégâts matériels ou logiciels entraîne une facturation au collaborateur du matériel remplacé ou réparé ainsi que des heures de travail par le service informatique ou, selon facture, par des fournisseurs.

Art. 63 - Dérogation

Toute dérogation aux présentes directives doit être faite en la forme écrite.

Art. 64 - Abrogation

Les présentes directives abrogent et remplacent toutes règles antérieures contraires.

Art. 65 - Entrée en vigueur

Les présentes directives entrent en vigueur le 1er juin 2007.

Swiss Medical Network SA