Hôpital du Valais
Spital Wallis

Directive institutionnelle

« Utilisation des moyens informatiques et de téléphonie »

(Ordinateur, téléphone, messagerie électronique et Internet)

Pour faciliter la lecture du présent document, les termes génériques sont au masculin. Ils incluent naturellement les personnes de sexe féminin et masculin.

Hôpital du Valais
Spital Wallis

1. Buts et champ d'application

Les présentes directives ont pour but de donner un cadre réglementaire à l'utilisation des moyens informatiques et de téléphonie au sein du Réseau Santé Valais et notamment de fixer les conditions d'utilisation et les mesures de surveillance, ce dans le respect des droits légitimes de l'employeur et des utilisateurs.
Ces directives s'appliquent à tous les responsables, employés ou personnes mandatées par le RSV qui accèdent aux moyens informatiques et de téléphonie du RSV (ci-après : les utilisateurs).
La règlementation des droits d'accès aux données des patients ainsi que celle relative à la transmission de ces données à des tiers fait l'objet de directives distinctes.

2. Conditions générales d'utilisation

Chaque utilisateur porte la responsabilité d'utiliser correctement les moyens informatiques et la téléphonie mis à disposition.
Les ordinateurs, les téléphones, la boîte aux lettres électronique (messagerie) et Internet sont des outils de travail et doivent être utilisés à des fins professionnelles. Ils sont la propriété du Réseau Santé Valais. Un usage personnel à but non lucratif est toléré à condition qu'il n'entraîne que des coûts minimes pour l'employeur et qu'il ne nuise pas au travail (quantité et qualité) de l'employé ou des autres collaborateurs. Lors d'un usage pour des besoins privés, l'utilisateur doit faire en sorte que ce qu'il traite soit clairement identifié comme étant du domaine privé et n'engage en aucune manière la responsabilité du RSV.
Toute personne utilisant des ressources informatiques respecte le Code pénal (CP, RS 311.0), la Loi fédérale sur les droits d'auteurs (LDA, RS 231.1), la Loi sur la santé du canton du Valais (LS, RSVs 800.1), ainsi que la Loi cantonale concernant la protection des données à caractère personnel (LPDCP, RSVs 235.1).
Les utilisateurs ne consultent, ne stockent, ni ne diffusent des documents qui, sous quelque forme que ce soit, constituent une participation à un acte illicite et qui, en particulier, portent atteinte à la dignité de la personne, présentent un caractère pornographique, pédophile, raciste ou violent.
Des mesures de contrôle seront effectuées (cf. chiffre 7) afin d'assurer l'application de ces directives.
La violation des obligations figurant dans ce règlement est passible de sanctions administratives ou de dénonciation pénale.

3. Règles d'utilisation des outils informatiques et de communication

La plupart des activités et des prestations de notre institution reposent sur l'utilisation adéquate des moyens informatiques et de communication mis à disposition des utilisateurs.
Ci-après, nous attirons l'attention sur les comportements inadéquats.

3.1 Ordinateur

Chaque poste de travail est un élément constitutif du système d'information du Réseau Santé Valais.
Toute installation d'un logiciel à usage professionnel fait l'objet d'une demande au Département d'informatique médicale et administrative (DIMA), qui se charge de l'installation. Le DIMA tient à jour une liste de logiciels autorisés, agréée par la Direction générale.
D'une manière générale, les données doivent être stockées sur les serveurs prévus à cet effet. Elles doivent être épurées régulièrement.

Les actions suivantes ne sont pas autorisées et constituent des comportements incorrects

1. Modifier la configuration d'un ordinateur sans l'accord préalable du service informatique compétent en raison des risques importants de dysfonctionnement (économiseurs d'écran, nouveaux périphériques, modem, nouvelles cartes, etc.) ;
2. Installer des programmes téléchargés depuis Internet ou reçus par courrier électronique ou en provenance de toute autre source ;
3. Utiliser des jeux ;
4. Stocker des données professionnelles sur le disque dur du poste de travail. Demeure réservés la synchronisation de répertoires réseau sur les ordinateurs portables et les fichiers d'archives du logiciel de messagerie pour des données non sensibles au sens de la Loi fédérale sur la protection des données.

3.2 Téléphone

L'usage de la téléphonie fixe (ou mobile si elle est payée par l'entreprise) est généralement réservé aux besoins professionnels.
A titre exceptionnel, elle peut être utilisée pour des communications privées urgentes ou qui ne peuvent être effectuées à un autre moment.
Dans tous les cas, les utilisateurs privilégient les appels vers les numéros internes.

3.3 Messagerie électronique

La messagerie permet la transmission de documents ou d'informations entre deux ou plusieurs correspondants.
Les données personnelles et sensibles doivent être préalablement cryptées pour être transmises par la messagerie électronique.

Les actions suivantes ne sont pas autorisées et constituent des comportements incorrects

1. Envoyer des documents ou des messages sans lien direct avec l'activité professionnelle, notamment sous forme de propagande ;
2. Envoyer et faire suivre des documents n'ayant rien à faire avec l'activité de l'utilisateur ;
3. Envoyer des messages en masse par courrier électronique. Sauf autorisation spéciale de la Direction générale, cette pratique est interdite ;
4. Ouvrir des messages douteux (auteur inconnu, nom incongru de l'objet) pouvant contenir des virus. Dans ces cas, surtout ne pas ouvrir la pièce jointe !
5. Toute information sur des virus ou autre logiciel malicieux doit être annoncée uniquement au DIMA, même si vous êtes invités à transmettre le message à tous vos correspondants.

3.4 Internet

L'Internet donne à l'utilisateur le moyen d'obtenir des informations générales ou particulières sur un ou plusieurs domaines d'activités nécessaires à l'exercice de sa fonction. L'accès exceptionnel à Internet à des fins privées est toléré dans la mesure où il est bref et qu'il s'inscrit dans les principes généraux énoncés.

Les actions suivantes ne sont pas autorisées et constituent des comportements incorrects

1. Utiliser de façon abusive la permission d'accès à Internet ;
2. Discuter sur des « chats » ou des forums n'ayant aucun lien avec la fonction de l'utilisateur ;
3. Télécharger des fichiers sans rapport avec l'activité professionnelle.
4. Ecouter des émissions de radio, visionner des émissions TV ou des vidéos sans rapport avec l'activité professionnelle.

Hôpital du Valais
Spital Wallis

4. Blocages techniques

Le DIMA est chargé de faire le nécessaire pour que seuls les moyens informatiques autorisés, compte tenu également des limitations spécifiques d'utilisation, soient à disposition des utilisateurs.
Le DIMA est notamment chargé de bloquer l'accès aux sites Internet non autorisés, principalement ceux qui correspondent à la description faite dans le point 2. Le fait qu'un site qui devrait être bloqué puisse malgré tout être consulté ne diminue en rien la responsabilité de l'utilisateur et l'importance des éventuelles sanctions qui pourraient être prises.

5. Mot de passe

Le mot de passe est nécessaire pour sécuriser l'ensemble des systèmes informatiques : accès aux réseaux, aux applications et aux données.
Il protège l'accès et la gestion des données relatifs aux droits assignés à l'utilisateur. En outre, il l'authentifie sur les actions faites dans la plupart des systèmes informatiques.

Le mot de passe est personnel et confidentiel. En ce sens, il ne doit être communiqué à personne. Le mot de passe doit être modifié régulièrement par l'utilisateur, conformément aux Directives du DIMA, de manière à s'assurer que personne ne pourra l'utiliser à son insu.
L'employé a le devoir d'informer sa hiérarchie et le DIMA s'il constate ou suspecte que son compte a été usurpé ou en cas de perte du mot de passe.

Les actions suivantes ne sont pas autorisées et constituent des comportements incorrects

1. Communiquer un mot de passe à d'autres personnes, même proches ;
2. Afficher ou stocker son ou ses mots de passe à proximité de l'ordinateur;
3. Créer des mots de passe faciles à trouver (nom de famille/prénom des enfants/date de naissance/etc.) ;
4. Utiliser un mot de passe ou un compte qui n'appartient pas à l'utilisateur.
5. Essayer, sans droit, d'accéder à des données pour lesquelles il n'a pas d'autorisation

6. Publication et distribution

La présente Directive est publiée sur l'intranet du Réseau Santé Valais.
Elle est notifiée par la Direction générale à l'ensemble des utilisateurs.
La directive est également transmise pour lecture et signature par la Direction de centre à chaque nouvel utilisateur au moment de son engagement.

7. Contrôles et sanctions

Sur proposition de la Direction de centre ou en tout temps, la Direction générale peut décider de faire effectuer au DIMA des contrôles statistiques anonymisés et non-annoncés de l'utilisation des moyens informatiques ou de la téléphonie mis à disposition des utilisateurs. Le DIMA n'est autorisé à effectuer des contrôles que sur mandat de la Direction générale.
En cas de non-respect présumé des présentes directives, révélé par les contrôles précités ou d'autres éléments, la Direction générale peut décider, de sa propre initiative ou sur proposition de la Direction de centre, de faire procéder à des contrôles individualisés portant sur l'utilisation de moyens informatiques et de la téléphonie.
Sous réserve des cas de soupçon d'infraction pénale, ce contrôle ne pourra pas porter sur le contenu des fichiers et messages identifiés comme étant de nature exclusivement privée. Les utilisateurs doivent être informés préalablement des contrôles individualisés, sauf s'il y a suspicion d'actes relevant du droit pénal.

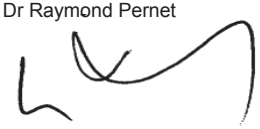
Si les soupçons de non-respect des présentes directives sont avérés, le contrôle pourra être étendu à la période antérieure à l'information.
Lorsqu'il y a suspicion d'actes pouvant relever du droit pénal, le DIMA avertit la Direction générale, qui décide des mesures à prendre.
Le Service ou l'établissement concerné, en collaboration avec le DIMA, prend toutes les mesures nécessaires pour la sauvegarde des éléments de preuve pertinents, en vue de l'ouverture d'éventuelles procédures administratives ou pénales. Il traite confidentiellement le résultat et les données recueillies pour les besoins des enquêtes. Lorsqu'il est certain que les données individualisées ne serviront pas à d'éventuelles procédures, elles devront être détruites dans les quatre semaines.
Lorsqu'un dérangement perturbe ou met en péril le bon fonctionnement des moyens informatiques et de la téléphonie, le DIMA est autorisé à prendre toutes les mesures nécessaires pour rétablir une situation normale, à l'exclusion de la prise de connaissance des données ressortant comme étant d'ordre privé. Les fichiers journaux peuvent être analysés afin d'établir le diagnostic de problèmes techniques.
En cas de confirmation des soupçons de non-respect de la présente directive, la Direction générale décide, sur proposition de la Direction de centre des sanctions administratives (blâme, avertissement ou licenciement), d'une action civile, ou d'une dénonciation à l'autorité pénale.

8. Approbation et entrée en vigueur

La présente Directive entre en vigueur le 1er juin 2008.

Approuvé en séance du Conseil d'administration le 19 mai 2008.

Dr Raymond Pernet



Président du Conseil d'administration

Dietmar Michlig

Directeur général