## 1. INTRODUCTION

Toute personne habilitée à utiliser les moyens informatiques du CH de Saumur doit se soumettre aux règles de sécurité et de bon usage du Système d'Information. Ces règles reposent sur la règlementation en vigueur dans le domaine de la sécurité de l'information et sur les droits et libertés reconnus aux utilisateurs.

L'établissement de santé abrite des données personnelles concernant :

- les patients et résidents, ci-après dénommés les patients (informations médicales et administratives),
- ses salariés (paie, gestion du temps de travail, évaluations, données de traces, …).

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. Elle est soumise au secret médical, elle ne doit donc être accessible qu'aux personnes autorisées professionnellement et ce quel que soit le support de stockage de l'information.

Le Service Informatique de l'établissement fournit un Système d'Information s'appuyant sur une infrastructure informatique.
Le Service Informatique doit assurer la disponibilité de l'ensemble des informations et leur mise en sécurité contre différents types de menaces (pannes, erreurs, mauvais usages, actes de malveillance, …). Il doit également s'assurer que l'ensemble des moyens mis à disposition des utilisateurs soit bien au service de la production de soins. Ainsi, des règles de bon usage et de contrôle des abus ont été définies.

## 2. REGLES DE SECURITE ET CONFIDENTIALITE :

Le Service Informatique attribue à chaque nouvel agent des droits d'accès au Système d'Information, en accord avec les responsables des différentes applications (fiche de demande d'habilitation).
Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement, à un tiers.
Tout droit prend fin lors de la cession, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect, par l'utilisateur, des dispositions de la Charte de sécurité pour l'accès et l'usage du Système d'Information.
**Ce droit d'accès entraîne pour l'utilisateur les droits, les obligations et les responsabilités précisés dans les paragraphes ci-dessous, et détaillés dans la Charte de sécurité pour l'accès et l'usage du Système d'Information (accessible sur l'Intranet et dans la gestion électronique de documents qualité) :**

### 2.1. Confidentialité de l'information et obligation de discrétion

Tous les agents du CH sont soumis au secret professionnel et/ou médical. Ils doivent faire preuve d'une discrétion absolue dans l'exercice de leur mission, que ce soit lors de communications écrites ou orales, téléphoniques ou électroniques, au cours d'échanges professionnels ou lors de conversations relevant de la sphère privée ; et ce quel que soit le lieu d'échange.
Notamment, concernant les réseaux sociaux, il ne peut y avoir aucun échange de photos, de vidéos[1], de commentaires sur les patients, les agents, les services, le CH de Saumur dans le cadre de son image et de sa réputation ; dans le cadre professionnel et privé. Le secret médical et le secret professionnel ne doivent pas être enfreints sur les réseaux sociaux.

[1] Il est interdit de prendre des photos et des vidéos au sein de l'établissement sans autorisation préalable de la Direction Générale.

Chaque utilisateur ne doit consulter que les informations auxquelles il est légalement autorisé ; c'est-à-dire :

- pour les médecins, dans le cadre du secret médical partagé, les données des seuls patients pour lesquels ils participent à la prise en charge diagnostique et thérapeutique ;
- pour les équipes travaillant sous la responsabilité du médecin qui prend en charge le patient, aux seules informations nécessaires à leurs missions ;
- pour tous les autres utilisateurs, aux seules informations nécessaires et autorisées dans le cadre de leurs fonctions.

De plus, les utilisateurs doivent assurer la confidentialité des données qu'ils détiennent.
L'accès par les utilisateurs aux informations et documents doit être limité à ceux qui leur sont propres, ainsi que ceux publics et partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs.
L'accès à des données de santé à caractère personnel par d'autres professionnels de santé extérieurs à l'établissement est autorisé à la condition que celles-ci soient anonymisées et que cette pratique ait été préalablement autorisée par la Direction Générale ainsi que le médecin responsable du Service d'Information Médicale.

### 2.2. Protection de l'information

Les postes de travail sont un moyen mis à disposition des utilisateurs pour accéder aux applications du Système d'Information et aux espaces de stockage sur des serveurs de fichiers. Le contenu des disques durs locaux de ces postes de travail n'est pas sauvegardé ; notamment le répertoire local « Téléchargements » est vidé automatiquement à chaque fermeture de session.
Les données et documents professionnels ne doivent donc pas être stockés sur ces postes de travail, mais sur les serveurs, eux-mêmes installés dans des salles protégées. Pour ce faire chaque utilisateur bénéficie d'un espace personnel (U:\) et d'espaces partagés (soumis à droits d'accès) sur le lecteur réseau G:\ permettant les échanges de documents professionnels en interne ; **ces espaces sont à usage professionnel uniquement**.
Chaque utilisateur doit s'assurer que tous les documents et informations qu'il détient et qui sont nécessaires à la continuité de service sont stockés dans un espace partagé par toutes les personnes en ayant besoin ; ceci est d'autant plus important en cas d'absence ou de départ de l'utilisateur.

**Aucune donnée (de santé ou non) à caractère personnel ne doit être stockée sur des postes ou périphériques personnels.**

Les écrans des postes de travail (fixes ou portables) doivent être orientés de telle sorte que les personnes non autorisées ne puissent pas lire ce qu'ils affichent. Les possibilités de visibilité depuis l'arrière de l'utilisateur (fenêtres, cloisons transparentes, …) doivent être prises en compte.
Les ordinateurs portables doivent être attachés à un point fixe ou lourd (bureau) en l'absence de leur utilisateur ; à défaut, ils doivent être systématiquement rangés dans des locaux réservés aux professionnels de santé (p. ex. dans le poste infirmier) en l'absence de leur utilisateur.
De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, disquette, clé USB, disque dur, …). Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les supports de stockage amovibles (exemples : clés USB, CD-ROM, disques durs, …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus), risques de perte ou de vol de données, … Leur usage doit être fait avec une très grande vigilance.
L'usage de supports de stockage amovibles personnels n'est pas autorisé.
L'usage de supports de stockage amovibles est autorisé lorsque l'utilisateur a besoin d'emmener des documents à l'extérieur, p. ex. pour une présentation, **à la stricte condition qu'ils ne contiennent aucune donnée (de santé ou non) à caractère personnel.** Dans ce cas, l'utilisateur doit se rapprocher du service informatique afin qu'une clé USB à usage professionnel lui soit attribuée.

### 2.3. Usage des ressources informatiques

Toute connexion de nouveau matériel au réseau de l'établissement, toute installation de nouveau logiciel sur les postes informatiques de l'établissement, ainsi que toute modification de configuration des ressources informatiques doit être réalisée par une personne habilitée du Service Informatique.

### 2.4. Usage des outils de communication

Les outils de communication (téléphone, fax, Internet et messagerie) sont destinés à un usage strictement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il reste très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne porte pas atteinte à l'image de marque de l'établissement.
Aucune information sensible (information nominative, médicale ou non ; information relative au fonctionnement interne de l'établissement) ne doit être transmise par téléphone ou par fax. La communication d'informations médicales aux patients et aux professionnels extérieurs est strictement règlementée, les utilisateurs concernés doivent s'y conformer.

L'accès Internet a pour but d'aider les professionnels dans l'exercice de leurs missions. Dans ce cadre, il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est recommandé de ne pas communiquer ses coordonnées professionnelles sur Internet, sauf en cas de nécessité professionnelle. Il est interdit de participer à des forums, blogs, réseaux sociaux et groupes de discussions à des fins non professionnelles et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraire à l'ordre public.

L'usage de la messagerie a pour but de faciliter les échanges entre les professionnels de l'établissement. Toutefois, il faut éviter l'envoi massif de pièces jointes volumineuses. **La messagerie (sauf comptes de messagerie sécurisés) n'est pas un moyen de transport sécurisé, il ne faut donc pas échanger d'informations médicales nominatives en clair.** La messagerie ne doit pas être utilisée comme moyen de propagande au sein de l'établissement.

### 2.5. Usage des login et mot de passe (ou cartes CPS ou équivalent)

Chaque utilisateur dispose d'un compte nominatif (login/mot de passe, ou carte CPS ou équivalent) pour accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est interdit d'utiliser ou de tenter d'utiliser le compte d'un autre utilisateur.
Le mot de passe choisi doit être robuste : il doit comporter de 6 à 8 caractères et mélanger des caractères de type différent (majuscules, minuscules, chiffres). Il doit être simple à mémoriser, mais surtout complexe à deviner : il ne doit pas être en lien avec l'utilisateur lui-même (ne pas comporter le nom, la date de naissance, …). De plus, il doit être changé régulièrement.
Le mot de passe est strictement confidentiel, il ne doit jamais être communiqué.
**Le mot de passe ne doit être écrit sur aucun support** (ni papier, ni informatique, …) et l'utilisateur ne doit pas configurer les logiciels pour qu'ils retiennent les mots de passe : le mot de passe doit être saisi à chaque nouvelle authentification.

Chaque utilisateur doit veiller à ne pas mettre à disposition d'un tiers non autorisé un accès aux systèmes et réseaux de l'établissement. C'est pourquoi, sur un poste dédié, il convient de fermer ou verrouiller sa session, dès qu'on s'absente de son poste de travail.

## 3. TRACABILITE :

Le Service Informatique assure une traçabilité des accès et des opérations réalisés sur l'ensemble des applications (médicales, médico-techniques et administratives) et ressources informatiques (réseau, messagerie, Internet) mises à disposition des utilisateurs, sur la base du compte nominatif utilisé pour ces accès. Cette traçabilité répond à des exigences règlementaires.
Le Service Informatique respecte la confidentialité de ces données de traces mais il peut être amené à les utiliser, en situation d'urgence ou sur la demande de la direction générale, pour mettre en évidence certaines infractions commises par les utilisateurs.

Par ailleurs, une cellule de surveillance des usages déviants est mise en place au sein de l'établissement. Elle a pour mission de contrôler les accès non autorisés aux données de santé à caractère personnel, à partir de l'analyse des données de traces.

## 4. PROTECTION DES DONNNES PERSONNELLES :

Dans le cadre du respect du RGPD et de la loi Informatique et Libertés, toute création ou modification de fichier comportant des données nominatives doit être signalée au Délégué à la Protection des dOnnées (DPO).
Ainsi, préalablement à la mise en œuvre du fichier, le DPO pourra vérifier la conformité de ce recueil d'information aux exigences de la CNIL et procèdera aux opérations règlementaires (inscription ou mise à jour du traitement de données personnelles au registre des traitements de données à caractère personnel de l'établissement, demande d'autorisation, information, …). L'absence de déclaration de fichier comportant des données à caractère personnel est passible de sanctions financières et de peines d'emprisonnement. Le DPO est en droit de mettre fin à tout traitement ne respectant pas les obligations relatives au RGPD et à la loi Informatique et Libertés.

## 5. RESPONSABILITES ET SANCTIONS :

En cas de manquement aux règles de la Charte de sécurité pour l'accès et l'usage du Système d'Information, l'utilisateur responsable de ce manquement s'expose à des sanctions pouvant aller jusqu'au licenciement, voire des actions civiles ou pénales en fonction de la gravité de ses actes.

Document approuvé le 25/03/2022

par le Directeur Général
du CH de Saumur

Jean-Paul QUILLET