Charte d'accès et d'usage du système d'information du Centre Hospitalier de Fougères

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 Centre Hospitalier de Fougères 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 de l'établissement, 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 l'établissement.

Cette Charte a été validée par la Direction de l'établissement. Préalablement à sa mise en œuvre, elle a été notifiée au Comité Technique d'Etablissement et à la Commission médicale d'Etablissement. Elle constitue une annexe au Règlement Intérieur de l'établissement et s'applique à tout nouvel arrivant dès sa prise de fonction dans l'établissement. Les membres du personnel utilisateurs du SIH sont invités à en prendre connaissance. La Charte est mise à leur disposition dans l'outil de gestion électronique de documents et affichée dans les locaux de l'établissement de santé.

2. CHAMP D'APPLICATION

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du Centre Hospitalier de Fougères, 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.

Cette Charte s'applique à l'ensemble du personnel de l'établissement de santé, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (stagiaires, internes, prestataires, fournisseurs, sous-traitants, …) utilisant les moyens informatiques de l'établissement et les personnes auxquelles il est possible d'accéder au système d'information à distance directement ou à partir du réseau administré par l'établissement.

Les intervenants extérieurs sont invités à prendre connaissance et s'engagent à respecter la charte fournisseurs et prestataires du système d'information (QUA-INFP-112).

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, etc.) ;
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services internet de l'établissement.

3. CADRE REGLEMENTAIRE

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.

- **Références réglementaires**

Les lois et textes réglementaires concernées par ce document sont présumés connus : les plus importants qui définissent les droits et obligations des personnes utilisant les moyens informatiques sont :

- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Le décret no 91-1051 du 14/10/1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi no 78-17 du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés
- La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Le décret n° 2005-1309 du 20 octobre 2005 modifié par le décret n° 2007-451 du 25 mars 2007 (décrets d'application de la réforme de 2004)
- La loi n°227-23 du code pénal, qui criminalise le fait, de fixer, d'enregistrer ou de transmettre, en vue de sa diffusion, l'image ou la représentation d'un mineur qui présente un caractère pornographique.

Ces lois et textes ont pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique. Elles définissent les droits des personnes et les obligations des responsables de fichiers contenant des informations nominatives.

- La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique

Cette loi définit les peines encourues par les personnes portant atteinte aux systèmes de données.

- La loi n° 85-660 du 3 juillet 1985 sur la protection des logiciels

Cette loi protège les droits d'auteurs ; elle interdit en particulier à l'utilisateur d'un logiciel, toute reproduction autre que l'établissement d'une copie de sauvegarde gérée par le Service Informatique.

- La directive 96/9CE du 11/03/1996 concernant la protection juridique des bases de données

Elle vise à accorder aux bases de données une protection de droit d'auteur harmonisée.

- La loi n° 2002-303 du 04/03/2002 relative aux droits des malades et à la qualité du système de santé.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1 PRINCIPES

L'établissement de santé héberge des données et des informations médicales et administratives sur les patients (dossier médical, dossier de soins, dossier images et autres dossiers médicotechniques, …), et sur les personnels (paie, gestion du temps, évaluations, 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,...

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 ;
- **Sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder ;
- **Sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

4.2 UNE MISSION SECURITE

Le service Informatique fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble du système d'information 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, le respect du cadre juridique sur l'usage des données personnelles de santé.

Pour cela, le service Informatique 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 (homonymie par exemple), perte de données suite à une erreur d'utilisation d'une application informatique, …). La sécurité repose sur une gestion des risques avec des analyses des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. 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.

5. REGLES DE SECURITE

L'accès au système d'information de l'établissement est défini selon les fonctions assurées par le professionnel et son métier.

Les droits d'accès sont déterminés par le comité de suivi du dossier patient informatisé ou les référents des applications concernées (SGL, traçabilité transfusionnelle, …) pour ce qui concerne les informations médicales et par le responsable du service Informatique pour les autres informations.

Le service Informatique attribue au demandeur son droit d'accès et lui mentionne l'existence de la présente Charte d'accès et d'usage du système d'information qu'il a pour devoir de prendre connaissance et de respecter scrupuleusement.. 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 des dispositions de la présente Charte par l'utilisateur.

L'obtention d'un droit d'accès au système d'information de l'établissement de santé entraîne pour l'utilisateur les droits et les responsabilités précisées dans les paragraphes ci-dessous.

5.1 CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION

Les personnels de l'établissement 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 privées de type courrier électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

La consultation des données relatives aux patients est limitée aux besoins liés à sa prise en charge. En dehors de ce cadre strict, cette consultation porte atteinte au secret professionnel et relève d'une faute professionnelle grave.

L'accès aux données de santé à caractère personnel des patients par des professionnels habilités se fait avec un compte nominatif personnel (login et mot de passe) ; certaines données (consultation des droits à l'Assurance Maladie Obligatoire par exemple) sont accessibles avec une carte CPS.

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 ou tout autre moyen de communication, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

5.2 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de limiter autant que faire se peut le stockage de ces documents sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux implantés dans des salles protégées. De même, les documents bureautiques produits doivent être stockés de préférence sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit. Le service Informatique se réserve le droit de supprimer automatiquement les fichiers non autorisés stockés sur les serveurs (vidéos, musique, …).

Dans le cas où les documents de l'utilisateur ne sont pas stockés directement sur un serveur réseau mais sur un autre support (disque dur de PC, clé USB, …), l'utilisateur est responsable de la sauvegarde ses fichiers à partir des outils de sauvegardes mis en place par le service Informatique.

Le répertoire Public sur Malibu sert à échanger des documents entre utilisateurs et est accessible à tout le monde en écriture (lecture, modification, suppression). Aussi, il est fortement conseillé de ne pas y enregistrer de documents confidentiels ou des documents sans une copie de sauvegarde à un autre endroit.

La volumétrie des documents conservés sur les serveurs par chaque utilisateur doit être « raisonnable ». Des quotas par utilisateur sont mis en place afin de réguler les espaces disques. En cas de besoin particulier de stockage ou d'archivage, contacter le service Informatique.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smartphone, …) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'une personne non autorisée… ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (clé USB, CD-ROM, disque dur, appareil photographique…). Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les medias de stockage amovibles (clé USB, CD-ROM, disque dur…) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit être fait avec une très grande vigilance. L'établissement se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

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.

5.3 USAGE DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées du Centre Hospitalier de Fougères (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et plus globalement d'installer de nouveaux matériels informatiques.

En cas de besoin d'un nouveau logiciel, en faire la demande au service Informatique.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) 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).

Les logiciels commerciaux acquis par l'établissement ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement. Il doit, de plus, se conformer à l'utilisation définie par l'auteur du logiciel ou bien décrite dans la documentation fournie.

Il est formellement interdit de connecter, ou tenter de connecter, un équipement non fourni par le service Informatique sur le réseau local de l'établissement.

Dans un souci d'économie d'énergie, il est demandé d'éteindre électriquement les équipements lorsque ceux-ci ne seront plus utilisés pendant une période de quelques heures (unité centrale, écran, imprimante).

5.4 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.

- **Usage du téléphone et du fax**

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque 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. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou professionnels.

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.

- **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.

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 données 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. Il est interdit de participer à des forums, blogs et groupes de discussion 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.

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.

Le service Informatique est en capacité de fournir la politique de filtrage des accès Internet sur simple demande écrite. Cette politique de sécurité est validée par les mêmes instances que celles validant la présente charte.

- **Usage de la messagerie**

La messagerie permet de faciliter les échanges entre les professionnels de l'établissement. Les messages ou les documents envoyés par mail sont assimilés aux courriers et documents écrits en matière de gestion courante.

Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre l'hôpital et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « *personnel* » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « *personnel* » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

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

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou de porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.

Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs doivent veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. La volumétrie des messages conservés sur les serveurs par chaque utilisateur doit être « raisonnable ». Des quotas par utilisateur sont mis en place afin de réguler les espaces disques. En cas de besoin particulier de stockage ou d'archivage, contacter le service Informatique.

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 cas d'impossibilité de chiffrement de l'information de bout en bout (destinataire ne disposant pas d'une messagerie sécurisée, …), les informations médicales doivent obligatoirement être rendues anonymes. Les messages électroniques contenant des informations médicales ou nominatives doivent obligatoirement transiter par la messagerie sécurisée mise en place dans l'établissement.

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.

5.5 USAGE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT)

D'une manière générale, chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. 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.

Pour utiliser ce compte nominatif, l'utilisateur soit dispose d'un login et d'un mot de passe, soit utilise une carte CPS ou équivalent (avec un code personnel à 4 chiffres)

Le mot de passe choisi doit être robuste (6 caractères minimum, mélange de chiffres, lettres), de préférence simple à mémoriser, mais surtout complexe à deviner. Le mot de passe est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel en charge de la sécurité des systèmes d'information, même pour une situation temporaire.

Le mot de passe est forcément changé tous les 3 mois par l'utilisateur pour l'accès aux applications médicales. Il est fortement conseillé de le changer régulièrement pour l'ensemble des autres applications.

Ne pas laisser ces mots de passe en évidence (post-it sur le bureau, sur l'écran ou sous le clavier).

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 médicotechniques, 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 d'autre que lui ne puisse se connecter avec son propre compte. Pour cela, sur un poste dédié, il convient de fermer les applications et documents, et fermer ou verrouiller sa session lorsqu'on quitte son poste. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le 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 de formations ou dans les manuels et procédures remis aux utilisateurs.

L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

Certaines applications sont accessibles à partir de comptes génériques, de manière à partager des ressources entre professionnels. Les utilisateurs de ces comptes génériques veilleront au seul accès à l'outil informatique des professionnels habilités (fermeture des locaux, des applications, verrouillage du poste…).

Toute attribution d'un compte générique fait l'objet d'une traçabilité papier par le service délivrant ce compte.

5.6 REGLES DE GESTION DES ACCES AU DOSSIER PATIENT INFORMATISE (DPI)

Le compte d'accès au DPI est créé avec des droits d'accès répondant au plus près des besoins du profil de l'utilisateur pour l'exercice de son activité métier (médical, para-médical, médico-technique, médico-social, administratif, …).

Ces droits d'accès sont définis par application au cœur du processus de soins dans des matrices accessibles dans la gestion documentaire de l'établissement.

Les applications intégrant un système de renouvellement de mot de passe imposent automatiquement et à fréquence régulière aux utilisateurs qu'ils modifient ce mot de passe.

Pour l'accès aux applications médicales, des comptes génériques sont également utilisés pour gérer les cas particuliers suivants :

- Elèves stagiaires IDE et aides-soignants
- Arrivée d'un remplaçant (médecin, interne, IDE, aide-soignant) en dehors des heures d'ouverture du service informatique
- Utilisateur ayant un compte nominatif mais ne pouvant l'utiliser (perte des informations de connexion, compte bloqué,…) et besoin d'accéder aux applications en dehors des heures d'ouverture du service informatique
- Utilisateur pour lequel il est impossibilité de créer un compte nominatif (information DPRS manquante ou dossier administratif incomplet)

5.7 MODALITES D'OUVERTURE ET DE FERMETURE DES ACCES

Lors de son arrivée, le nouvel utilisateur du système d'information informe au plus tôt le service Informatique sur ses besoins en termes de ressources informatique nécessaires à la réalisation des tâches qui lui incombent. Il fournit également toutes les données requises pour la création des comptes d'accès (nom, prénom, profil, service, mot de passe initial si nécessaire, …)

Lors de son départ, il informe le service Informatique pour que celui-ci puisse réaliser les actions de clôture de son compte (fermeture des droits d'accès aux applications). Il indique en particulier les actions à mener pour le traitement des données appartenant (d'un point de vue informatique) à l'utilisateur :

- Documents bureautique : suppression, archivage ou transfert des documents vers un autre utilisateur identifié ?
- Messages électroniques : suppression, archivage ou transfert des messages vers un autre utilisateur identifié ?

5.8 IMAGE DE MARQUE DE L'ETABLISSEMENT

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.

6. INFORMATIQUE ET LIBERTES

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du Correspondant Informatique et Libertés (CIL) de l'établissement de santé, à défaut le Responsable de la Sécurité du Système d'Information (RSSI), qui étudie alors la pertinence des données recueillies, la finalité du fichier, 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 CIL 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 CIL 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.

7. SURVEILLANCE DU SYSTEME D'INFORMATION

7.1 CONTROLE

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.

Les contrôles sur les accès aux données médicales sont sous la responsabilité du médecin DIM.

7.2 TRAÇABILITE

Le Service informatique assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle 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 supprimées des bases de données en réseau et/ou des applications de l'hôpital ;
- La durée de la connexion et le volume de données échangé ou consulté (notamment pour l'accès Internet) ;

Le délai de conservation des informations de connexion et des actions réalisées est :

- **Pour les applications** : toute la durée d'utilisation de l'application dans l'établissement
- **Pour les accès Internet** : 6 mois

- **Pour la messagerie** : selon capacité de stockage des serveurs (seules les informations d'entête des messages sont tracées, l'objet et le contenu du message ne sont pas enregistrés)

Le personnel de la Direction du système d'information respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

7.3 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 aux Responsable de la Sécurité du Système d'Information et Responsable du Service Informatique.

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.

8. DIFFUSION, RESPONSABILITES ET SANCTIONS

La procédure de diffusion de la charte et du recueil de l'engagement à la respecter est formalisée et accessible dans la gestion documentaire (QUA-PR-191).

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, ASIP Santé, ...).

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 pouvant être :

- Un rappel ou un avertissement accompagné ou non d'un retrait partiel ou total, temporaire ou définitif, des moyens informatiques ou téléphoniques ;
- Des sanctions disciplinaires pouvant conduire jusqu'à la radiation ou au licenciement et éventuellement des actions civiles ou pénales, selon la gravité du manquement.

Outre ces sanctions, la Direction du Centre Hospitalier de Fougères est tenu de signaler toutes infractions pénales commises par son personnel au procureur de la République.

La Directrice du Centre Hospitalier de Fougères

Madame Laurence JAY-PASSOT

Centre Hospitalier
FOUGERES

ANNEXE 1

Déclaration d'engagement personnel à respecter la charte d'accès et d'usage du système d'information du Centre Hospitalier de Fougères

En tant qu'utilisateur du système d'information du Centre Hospitalier de Fougères,

Je, soussigné (Nom, Prénom) :

Qualité :

Service :

Déclare avoir pris connaissance de la charte d'accès et d'usage du système d'information du Centre Hospitalier de Fougères,

M'engage à respecter les dispositions légales en la matière ainsi que les règles édictées par le Centre Hospitalier de Fougères telles que précisées dans cette charte.

Fait à Fougères, le

Signature