Charte d'Utilisation du Matériel et des Ressources Informatiques

Au CH du HAUT BUGEY

1. PREAMBULE

La présente charte a pour objet de définir les règles d'utilisation des moyens et systèmes informatiques du centre hospitalier du Haut Bugey et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.
Elle s'inscrit dans le cadre des lois en vigueur :

- Loi n° 78-17 du 6 janvier 1978 "informatique, fichiers et libertés"
- Loi n° 78-753 du 17 juillet 1978 sur l'accès aux documents administratifs,
- Loi n° 85.660 du 3 juillet 1985 sur la protection des logiciels,
- Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique,
- Loi n° 92-597 du 1er juillet 1992 (code de la propriété intellectuelle).

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, elle a été présentée au Directoire, au Comité Technique d'Etablissement et à la Commission Médicale d'Etablissement.

La présente Charte d'accès et d'usage du système d'information doit être signée par chaque utilisateur de l'outil informatique.

La Charte est mise à leur disposition sur l'Intranet et disponible au Service Informatique.

2. CHAMP D'APPLICATION DE LA CHARTE

La présente Charte concerne les ressources informatiques, les services internet, messagerie et téléphoniques du centre Hospitalier du Haut Bugey, 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.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau
- Ordinateurs portables
- Terminaux portables
- Imprimantes simples ou multifonctions
- Tablettes
- Smartphones

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, doctorants, 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.

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

- **Ressources informatiques**: les moyens informatiques locaux, 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, forum, 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.

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 administratif, 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.
- **Son archivage**

4.2 Une mission sécurité

Le CH du Haut Bugey fournit un système d'information qui s'appuie sur une infrastructure informatique. Il doit assurer la mise en sécurité de l'ensemble c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Il doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont utilisés conformément à leur objectif / mission.

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 centre Hospitalier du Haut Bugey 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 niveau de sécurité efficient.
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 ET DE GESTION DU RESEAU

L'accès au système d'information de l'établissement est soumis à autorisation.
-Une demande préalable de création de compte est requise pour l'attribution d'un accès aux ressources informatiques, aux services Internet et de télécommunication, de la part du responsable hiérarchique de l'utilisateur, ou du service de gestion du personnel. ***(Voir Procédure Accueil d'un nouvel Agent Hospitalier géré par la DRH***).

-Le service informatique attribue alors son compte à l'utilisateur. En fonction de son profil, des droits d'accès ou des ressources sont automatiquement attribuées (messagerie interne ou externe, accès à différentes applications métier, dossiers réseaux partagés,…)

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 indiquées dans les paragraphes ci-dessous.

5.1 Mission des administrateurs

- Les administrateurs sont là pour répondre aux questions éventuelles ou lorsque vous constatez un dysfonctionnement du système d'information, mais en aucun cas pour "réparer" le matériel qui aurait été endommagé par une utilisation non-conforme à cette charte.
- Les administrateurs sont responsables du bon fonctionnement de la machine ou du réseau et de la qualité du service proposé. C'est lui qui ouvre les comptes des utilisateurs.
  Les administrateurs respectent et assurent la confidentialité des fichiers et du courrier électronique des utilisateurs.
- De manière générale, les administrateurs ont le droit et le devoir de mettre en œuvre tous les moyens mis à leur disposition pour assurer le bon fonctionnement du réseau informatique de l'hôpital. Ils informent, dans la mesure du possible, les utilisateurs par circulaire ou par courrier électronique de toute intervention susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.
- Les administrateurs peuvent se connecter et prendre le contrôle des postes clients pour effectuer une maintenance (via Teamviewer), avec l'accord préalable téléphonique de l'utilisateur du poste à maintenir. Seuls les administrateurs ont l'autorisation d'effectuer cette manipulation. Une traçabilité des connexions est assurées par l'outil informatique Teamviewer.
- Les administrateurs n'ouvrent de comptes qu'aux utilisateurs ayant pris connaissance et signé le présent document, et peuvent les fermer s'ils ont des raisons de penser que l'utilisateur viole les règles énoncées ici.
- En particulier, l'administrateur peut explorer les fichiers des utilisateurs en cas de suspicion de violation de la présente charte, de constat d'actes de piratage, ou simplement pour diagnostiquer et corriger des problèmes avec le logiciel. Il réservera toutefois cet usage aux seuls cas nécessités par le bon fonctionnement et la sécurité du système. Il est tenu de ne pas divulguer les informations acquises par ces recherches sauf lorsque la loi l'y oblige ou lorsque le constat d'actes de piratages l'amène à communiquer des extraits de ses recherches à la direction afin d'initier des poursuites. Il peut aussi générer et consulter tout journal d'événements, et enregistrer des traces, si besoin est.
- L'ordinateur est la propriété du CH HAUT BUGEY, que ce soit au niveau du matériel que du contenu. L'administrateur sur décision du Directeur Général peut accéder au contenu de celui-ci au motif de la continuité de service. Il appartient à chaque utilisateur d'identifier les documents qu'il considère personnel avec l'intitulé ' Personnel' ou' Prive'.

<u>L'utilisateur reconnaît à l'administrateur le droit</u> :

- D'effectuer des copies de sauvegardes de ses fichiers personnels.
- De surveiller en détail un système informatique, y compris les sessions de travail des utilisateurs de façon à pouvoir déterminer si un utilisateur ne respecte pas la présente charte.
- De changer la priorité ou de stopper l'exécution d'une tâche lancée par un utilisateur et qui utilise des ressources de façon excessive, ceci avec ou sans notification préalable envoyée à l'utilisateur.
- D'effacer ou de comprimer les fichiers qui prennent une place excessive sur disque ou qui n'ont pas de relation avec les missions du CHHB, ceci avec ou sans notification préalable envoyée à l'utilisateur.
- De mettre fin aux sessions de travail inactives pendant une longue période de façon à libérer des ressources.
- D'interdire l'accès à des sites "Grand Public" ou "Exotiques" (Pornographiques, discrimination, anti républicain…)qui ne correspondent en rien aux missions du CHHB.

5.2 Conditions d'accès aux moyens informatiques de l'hôpital

En règle 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 dispose soit d'un login et d'un mot de passe, ou utilise une carte CPS ou une carte d'établissement (avec un code personnel à 4 chiffres, dit code PIN).

-Le mot de passe choisi doit être robuste (il est conseillé qu'il soit constitué de 8 caractères minimum, mélange de : chiffres, lettres majuscules, minuscules, caractères spéciaux), simple à mémoriser, mais surtout complexe à deviner. Il doit, de préférence, être changé tous les 6 mois.
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.
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 ne puisse se connecter avec son propre compte.
Pour cela, sur un poste dédié, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste.
Il ne faut jamais se connecter sur plusieurs postes à la fois.
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.

- Afin d'éviter l'intrusion de virus via l'extérieur, il est interdit d'utiliser des périphériques type clé USB sur un ordinateur du CHHB.

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

-Une politique de sécurité des comptes prévoit une désactivation temporaire ou définitive d'un compte lorsque plusieurs erreurs consécutives de saisie de mot de passe interviennent.
Il appartient à l'utilisateur, dans le cas d'une désactivation définitive, de contacter le référent de l'application concernée, ou le service informatique, pour réactiver le compte.

-Par dérogation, certaines fonctions spécifiques (infirmiers, secrétariats « partagés ») nécessitent l'utilisation d'un compte commun à plusieurs utilisateurs, sur un poste dit de type « kiosque », afin d'accéder à des informations partagées, à caractère organisationnelle (bureautique, agenda, messagerie,…).
Dans ce cas, l'accès aux données de santé à caractère personnel des patients demeure individuel.

6. RESPECT DE LA DEONTOLOGIE INFORMATIQUE

6.1 Règles de base

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier le mot de passe d'un autre utilisateur ;

- de modifier ou de détruire des informations ne lui appartenant pas sur un des systèmes informatiques ;
- d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation ;
- de porter atteinte à l'intégrité d'un autre utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants ;
- d'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au réseau ;
- de se connecter ou d'essayer de se connecter sur un site internet sans y être autorisé.
- Sur le répertoire Commun du serveur. (Rappel : ce répertoire est un répertoire partagé ou tous les utilisateurs du réseau ont accès). Dans ce répertoire doivent paraître uniquement des informations à contenu professionnel et pouvant être connues de l'ensemble du personnel de l'établissement.

La réalisation d'un programme informatique ayant de tels objectifs est également interdite.
Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à constituer des fichiers, il est rappelé que la loi " informatique et libertés" impose, préalablement à leur constitution, que les fichiers comportant un traitement de données nominatives fassent l'objet d'une déclaration ou d'une demande d'avis auprès de la Commission Nationale Informatique et Libertés (CNIL).

6.2 Utilisation de logiciels et respect des droits de la propriété

Seules des personnes habilitées de l'établissement de santé (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.
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).
- Ne pas faire de copies des logiciels commerciaux acquis par l'établissement, ces dernières ne pouvant être effectuées que par les personnes habilitées de l'établissement.
- Ne pas installer, télécharger ou utiliser sur le matériel, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, et sans autorisation des personnes habilitées de l'établissement.
- Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques...).
- Se conformer aux dispositifs et procédures mis en place par le service informatique pour lutter contre les virus et les attaques par programmes malveillants.
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés.

Dans le cas où un logiciel « pirate », (c'est-à-dire un produit n'appartenant pas à l'établissement du CH du HAUTBUGEY) est installé sur un poste, ce logiciel sera directement détruit sur le poste concerné.

6.3 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 occasionnel et raisonnable, tant dans la fréquence que dans la durée ; qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à la sécurité et à l'intégrité du système d'information ainsi qu'à l'image de marque de l'établissement de santé.

6.4 Internet

L'accès à 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 Internet, leur identifiant est enregistré.

Il conviendra donc d'être particulièrement vigilant lors de l'utilisation d'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 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 , 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 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.
Tout téléchargement de fichiers, notamment de sons, d'images, de vidéos sur le réseau Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle (Loi ADOPI).

Le CH du Haut Bugey se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information, code malicieux, programmes espions ...).

6.5 Messagerie

La messagerie permet de faciliter les échanges entre les professionnels de l'établissement.
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 « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle.
Les messages marqués « privé » 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 provoquants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou 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.
Pour les mêmes raisons, il est attendu de chaque utilisateur, une gestion de ses messages (suppression, archivage, effacement périodique).
Il doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles en tant qu'éléments de preuve.
Il est rappelé que le réseau Internet n'est pas un moyen de communication sécurisé.
Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair.
En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

6.6 Stockage réseau et sauvegardes :

Les utilisateurs doivent stocker ou copier leurs fichiers et dossier de travail professionnels dans le dossier « Mes Documents » du poste de travail ainsi que sur les emplacements réseau mis à leur disposition. (SRVDATANS20 : Commun, Communs des services, répertoires partagés). Ceci permettra de sauvegarder ces documents et de les retrouver en cas d'incident informatique quelconque.
En effet, une sauvegarde sur bande est effectuée tous les jours. Nous pouvons remonter à 1 mois d'ancienneté pour retrouver vos éléments. Il convient de faire cette demande au service informatique le plus rapidement possible. Cependant, le CHHB ne garantit pas que les données puissent être ou soient restaurées. Bien que tout soit fait pour maintenir un niveau de sécurité adéquat, le CHHB ne peut être tenu pour responsable de tout défaut de confidentialité, de tout vol d'information, de détérioration ou perte de données résultant directement ou indirectement de l'absence ou du mauvais fonctionnement d'un mécanisme de protection.

Remarques importantes:
L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il dispose.

6.7 Utilisation équitable des moyens informatiques :

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le responsable du matériel informatique de toute anomalie constatée.

Un utilisateur ne doit jamais quitter un poste de travail sans se déconnecter (fermer ou verrouiller sa session).

Les activités risquant d'accaparer fortement les ressources informatiques (impression de gros documents, sauvegarde de fichiers, utilisation intensive du réseau,...) devront être effectuées aux moments qui pénalisent le moins la communauté.

L'édition des documents est autorisée uniquement pour les documents professionnels, l'impression doit donc concerner uniquement les documents strictement nécessaires.

L'utilisateur s'engage à informer le service informatique s'il pense que l'accès aux données a pu être violé, ou si les données ont pu être corrompues.

7. VIDEOPROTECTION

Le CH du Haut Bugey et les 2 EHPAD d'Oyonnax et de Nantua sont équipés d'un système de vidéo protection, avec enregistrement.
La durée de conservation des images, hormis le cas d'une enquête en flagrant délit, d'une enquête préliminaire ou d'une information judiciaire, est de 30 jours.
Le système de vidéo protection a fait l'objet d'une autorisation par arrêté préfectoral en date du 27/01/2015.
Les personnes habilitées à la relecture des images ont été déclarées à la préfecture :
-DJAMAKORZIAN Eric : Directeur Général
-MIKULOVIC Emmanuel : Directeur Système d'Information
-SEMLALI Toufik : Directeur des Services Techniques
-WENISCH Bernard : Directeur des Finances et des Services Economiques.

En cas d'urgences le Directeur Général peut déléguer au cadre de garde.

8. Les informations médicales :

Depuis janvier 2011, l'ensemble du dossier patient est progressivement informatisé (logiciel CORA). L'informatisation permet d'accéder aux informations médicales à tout moment et quel que soit le lieu de prise en charge.

L'accès à ces informations médicales reste cependant soumis au secret médical et professionnel définis par le code de la santé publique (Article L.1110-4), et rendus obligatoires pour tous les professionnels de santé par le code pénal (articles 226-13 et 226-14) :

→ toute personne prise en charge par un établissement […] a droit au respect de sa vie privée et du secret de l'ensemble des informations la concernant. Il n'y a pas de renseignement anodin dès lors qu'il est venu à la connaissance d'un membre du personnel hospitalier dans le cadre de son activité professionnelle.

→ les personnels, quel que soit leur métier, n'ont pas le droit d'accéder aux informations de l'ensemble des patients qui viennent dans l'établissement : c'est la participation à la prise en charge et aux soins qui légitime la consultation des données du patient, sous réserve que le patient ait donné son accord et sous réserve de ne rechercher que les seules informations nécessaires et pertinentes au regard de l'intérêt du patient. Les droits donnés sur l'accès au dossier patient ne constituent pas un droit à la curiosité personnelle.

Les règles d'accès au Dossier Patient Informatisé sont définies par le Groupe Projet Cora en fonction des métiers et missions spécifiques des utilisateurs et font l'objet d'une validation en CME. Les droits utilisateurs sont créés et gérés par le Département d'Information Médicale (DIM).

Des procédures de contrôle sont définies ; tout agent intervenant sur un dossier est identifié et tracé par le service informatique. Le fait de s'identifier avec un nom d'utilisateur et un mot de passe est considéré comme une signature. L'utilisation d'un code utilisateur est de la responsabilité de la personne à qui il a été attribué. Il est donc interdit de communiquer ses codes de connexion à qui que ce soit.

➢L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique ainsi qu'aux poursuites, disciplinaire et pénal, prévues par les textes législatifs et réglementaires en vigueur.

Nom :…….
Prénom :…….
Service :……..
Fonction :……

Date :…….

Signature (Précédée de « Lu et Approuvé ») :