

	CHARTRE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION		
	DOC-	DQGR	Applicable à partir du : Revu le

CHARTRE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION

TABLE DES MATIERES

1.	PREAMBULE	2
2.	CHAMP D'APPLICATION	2
2.1.	LE PERIMETRE DU SYSTEME D'INFORMATION ET DE COMMUNICATION	2
2.2.	APPLICATION DE LA CHARTE AUX UTILISATEURS	3
2.2.1.	Professionnels du Centre Hospitalier	3
2.2.2.	Professionnels extérieurs au Centre Hospitalier	3
3.	PRINCIPES DE LA SÉCURITÉ.....	3
4.	RÈGLES DE SÉCURITÉ APPLICABLES AUX UTILISATEURS	4
4.1.	ACCES AU SYSTEME D'INFORMATION D'UN NOUVEL UTILISATEUR	4
4.1.1.	Recrutement d'un nouveau professionnel	4
4.1.2.	Evolution des droits d'accès	4
4.2.	CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION	4
4.3.	PROTECTION DE L'INFORMATION	5
4.4.	USAGE DES RESSOURCES INFORMATIQUES	5
4.5.	USAGE DES OUTILS DE COMMUNICATION	6
4.6.	USAGE DES LOGIN ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT).....	8
4.7.	SMARTPHONES ET TABLETTES PROFESSIONNELS.....	8
5.	INFORMATIQUE ET LIBERTÉS	8
6.	SURVEILLANCE DU SYSTÈME D'INFORMATION	9
6.1.	CONTROLE	9
6.2.	TRAÇABILITE	9
6.3.	ALERTES.....	10
6.4.	RESPONSABLE SECURITE DU SI	10
7.	RESPONSABILITÉS ET SANCTIONS	11
8.	Modalités d'approbation, de diffusion et de révision de la charte	11
8.1.	MODALITES D'APPROBATION DE LA CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION.	11
8.2.	REVISION DE LA CHARTE	11
8.3.	DIFFUSION DE LA CHARTE	11

1. PREAMBULE

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation Système d'Information du Centre Hospitalier de Libourne et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Définitions :

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

2. CHAMP D'APPLICATION

2.1. LE PERIMETRE DU SYSTEME D'INFORMATION ET DE COMMUNICATION

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques des Centres Hospitaliers de Libourne et de Sainte-Foy-La-Grande 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 fixe ou portables ;
- Imprimantes simples ou multifonctions ;
- Photocopieurs
- Tablettes ;
- Smartphones ;
- Réseau informatique (serveurs, routeurs, connectique)
- Logiciels
- Fichiers, bases de données
- Système de messagerie
- Intranet, extranet
- Abonnements à des services interactifs

2.2. APPLICATION DE LA CHARTE AUX UTILISATEURS

L'utilisation du système d'information et de communication doit être effectué exclusivement à des fins professionnelles, et tourné vers la performance de l'établissement et de la satisfaction des patients.

Chaque Utilisateur doit être conscient que :

- L'usage de ces ressources obéit à des règles (cadre réglementaire, règles internes, sécurité)
- La négligence ou la mauvaise utilisation des ressources fait courir des risques à l'ensemble de l'infrastructure de l'hôpital et de ses usagers.

2.2.1. Professionnels du Centre Hospitalier

Cette Charte s'applique à l'ensemble du personnel de l'établissement de santé, tous statuts confondus, et notamment

- les agents permanents (titulaires) ou temporaires (contractuels, stagiaires, internes, doctorants,) utilisant les moyens informatiques de l'établissement
- et toute personne ayant la possibilité, dans le cadre de ses fonctions, d'accéder au système d'information à distance directement ou à partir du réseau administré par l'établissement.

2.2.2. Professionnels extérieurs au Centre Hospitalier

Les responsables des Utilisateurs extérieurs s'engagent à faire respecter la présente Charte par leurs propres salariés et éventuelles entreprises sous-traitantes.

3. PRINCIPES DE LA SÉCURITÉ

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.

Quelle que soit la nature des données (médicales, administratives concernant les patients ou les professionnels) et quel que soit le média, la **sécurité de l'information** doit permettre de préserver :

- **La disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin ;
- **l'intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie ;
- **La confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder
- **La traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

La Direction du Système d'Information (DSI) fournit un système d'information dont elle assure la mise en sécurité contre des pannes, des erreurs ou des malveillances. Elle protège les intérêts économiques de l'établissement en s'assurant que ces moyens sont bien au service de la production de soins. Elle est responsable de définir et empêcher les abus en partenariat avec le RSSI.

La présente Charte d'accès et d'usage du système d'information s'inscrit dans le plan de communication de la sécurité du SI.

4. RÈGLES DE SÉCURITÉ APPLICABLES AUX UTILISATEURS

4.1. ACCES AU SYSTEME D'INFORMATION D'UN NOUVEL UTILISATEUR

4.1.1. Recrutement d'un nouveau professionnel

Pour tout nouveau professionnel de l'établissement, les droits d'accès nécessaires à l'exercice de ses missions sont mis en place au moment de sa prise de fonction.

Le nouveau professionnel s'engage à respecter la présente Charte.

4.1.2. Evolution des droits d'accès

Toute évolution des droits d'accès aux ressources informatiques est soumise à autorisation.

La demande exprimée par l'utilisateur fait l'objet d'une validation préalable par son responsable hiérarchique qui précise les accès nécessaires à son collaborateur et transmet la demande par écrit à la Direction du Système d'Information (DSI).

Celle-ci attribue alors au demandeur son droit d'accès.

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 cessation, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente Charte par l'utilisateur.

4.2. CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION

Les personnels de l'établissement sont soumis au secret professionnel et/ou médical. (cf. règlement intérieur).

Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les personnels sont tenus de faire preuve d'une discrétion absolue dans l'exercice de leur mission, notamment 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 est limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés.

Il est 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 électronique dont l'utilisateur n'est ni directement destinataire, ni en copie. L'accès aux données de santé à caractère personnel des patients par des professionnels habilités se fait par une authentification forte (mot de passe, carte CPS, etc....)

4.3. 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 convient de ne stocker aucune donnée ni aucun document 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 sont stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Le cas échéant, les professionnels qui utilisent un matériel portable (exemples : poste, tablette, smart phone, ...) veillent à ne pas le mettre en évidence pendant un déplacement, et à ne pas exposer son contenu à la vue d'un voisin; le matériel doit être rangé en lieu sûr. De même, tout support mobile de données (exemples : CD, disquette, clé, disque dur, ...) doit être stocké ou rangé de façon sécurisée. Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Les données sont stockées sur différents supports avec des niveaux de sécurité différents

Les disques locaux (par ex : C:\xxxxx) ne sont pas sauvegardés et ne doivent contenir aucune donnée sensible ou critique.

Les disques réseaux (par ex : R:\xxxx et U:\XX) sont sauvegardés tous les soirs en fonction de la politique de sauvegarde définie.

4.4. USAGE DES RESSOURCES INFORMATIQUES

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 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).

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.

4.5. 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.

Aucune information sensible ne peut être communiquée par téléphone, notamment les informations nominatives, médicales ou non, ainsi que les 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.

- **Usage de la messagerie**

L'usage de la messagerie est autorisé à l'ensemble du personnel. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement

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 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 obligations de discrétion professionnelle 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 taille et le nombre de pièces jointes autorisées peuvent être limités par la DSI pour des raisons techniques. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

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.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Dans ce cadre, les salariés sont invités à informer la DSI des dysfonctionnements qu'ils constatent.

La messagerie électronique étant un vecteur majeur de diffusion de programmes malveillants, l'utilisateur est invité à la prudence et au respect des bonnes pratiques quant à son usage.

En cas d'alerte de mail frauduleux ou cyber frauduleux, le RSSI de l'établissement peut demander la suppression massive de ce mail par la DSI.

- **Usage des supports amovibles**

Les supports amovibles (clés USB, disques durs externes) présentent des risques importants de sécurité, tant sur l'intrusion de logiciels malveillants que sur la confidentialité des données, ou sur leur permanence dans le temps.

L'usage de ces supports est soumis à des restrictions.

Par défaut, l'utilisation des supports amovibles sur les équipements professionnels est désactivée par la Direction du Système d'information.

Le recours aux autres moyens à disposition doit être favorisé, en particulier l'usage des disques réseaux partagés.

En cas de difficulté ou de besoin particulier, une demande justifiée doit être adressée à la DSI et au RSSI qui apprécient l'opportunité d'accorder un accès temporaire ou définitif à cette fonctionnalité.

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

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'utiliser le compte d'un autre utilisateur dans le système d'information.

Pour utiliser son 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)

La Direction des Systèmes d'information définit la politique institutionnelle de mot de passe, que l'utilisateur s'engage à respecter. 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. Pour cela, les règles suivantes s'imposent :

- sur un poste dédié, fermer ou verrouiller sa session dès que l'on quitte son poste.
- Ne jamais se connecter sur plusieurs postes à la fois.

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

4.7. SMARTPHONES ET TABLETTES PROFESSIONNELS

Certains professionnels peuvent bénéficier d'équipements mobiles dans le cadre de leurs fonctions (smartphones, tablettes).

Les règles ci-dessus s'appliquent dans les mêmes termes à l'usage de ces équipements mobiles.

5. INFORMATIQUE ET LIBERTÉS

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès de la CNIL (Commission

Nationale Informatique et Libertés). Le DPO est en charge de cette déclaration. Au vu des éléments fournis, la CNIL étudie 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.

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, la DSI est informée et peut 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.

Les Utilisateurs souhaitant réaliser des traitements relevant de ladite loi sont invités à prendre contact avec le DPO afin qu'ils soient traités dans le respect de la législation en vigueur.

Le DPO (dpo@ch-libourne.fr) a un rôle de conseil auprès des utilisateurs sur la gestion des données à caractère personnel. A ce titre, il veille à la bonne application de la loi Informatique et Libertés précitée dans le déploiement de tout projet et propose des solutions permettant de concilier protection des libertés individuelles et intérêt légitime de l'établissement.

6. SURVEILLANCE DU SYSTÈME D'INFORMATION

6.1. 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.

6.2. TRAÇABILITE

La Direction du Système d'Information (DSI) 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 (notamment pour l'accès Internet) ;

Le contrôle des données de connexion a pour objectif notamment :

- la prévention de la mise en péril des systèmes notamment par l'importation de virus ;
- la prévention de l'encombrement du réseau ;
- le contrôle du respect des règles définies par la présente Charte (ex. : usage personnel dans des limites raisonnables) ;
- l'optimisation de la bande passante.

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

Ces opérations peuvent conduire les équipes techniques à prendre connaissance d'informations de nature confidentielle et ce, dans le respect des droits fondamentaux de l'utilisateur (protection des données personnelles, vie privée, secret des correspondances).

Les équipes DSI ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.

De même elles s'engagent à informer l'utilisateur de toute opération inhabituelle tendant à accéder à ses données personnelles, et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf au cas où la discrétion des opérations est imposée par les autorités judiciaires).

Les accès et actions des équipes DSI réalisées sur le SI font l'objet d'un enregistrement sous la forme de traces dans les différents éléments du SI dans le but de permettre une analyse, voire de vérifier qui serait à l'origine d'une action privilégiée.

6.3. 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 à la Direction des Systèmes d'information et au Responsable de la sécurité des systèmes d'information.

6.4. RESPONSABLE SECURITE DU SI

Par sa fonction, le responsable sécurité du SI (RSSI) a capacité à auditer, analyser et surveiller le fonctionnement du SI et la bonne application de la politique de sécurité.

Plus largement, il a la possibilité d'intervenir, au moins en consultation, sur tout ou partie des éléments du système d'information (équipements de sécurité, équipements réseaux, serveurs, postes de travail, terminaux mobiles). Même s'il ne dispose pas au quotidien de tous les accès sur le SI, il est en droit de les obtenir, si l'accomplissement de ses missions le nécessite. Cet accès peut être rendu nécessaire notamment à des fins de diagnostic ou de surveillance d'anomalie. Il s'interdit scrupuleusement de divulguer les informations d'ordre personnelle qu'il serait amené à connaître, sauf en cas d'instruction pénale ou de décision de justice.

7. RESPONSABILITÉS ET SANCTIONS

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 disciplinaires.

8. Modalités d'approbation, de diffusion et de révision de la charte

8.1. MODALITES D'APPROBATION DE LA CHARTRE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION.

La Charte est élaborée par le Comité de sécurité du système d'information.

Elle fait l'objet d'une présentation en Comité social d'établissement (CSE) et en Commission médicale d'Etablissement (CME).

Elle est validée par le Directeur de l'établissement.

8.2. REVISION DE LA CHARTRE

La charte fait l'objet d'une révision annuelle.

En cas de modification, elle fait l'objet d'une approbation suivant les modalités prévues au paragraphe 8.1.

8.3. DIFFUSION DE LA CHARTRE

La présente Charte constitue une annexe du règlement intérieur de l'établissement.

Elle est mise en ligne sur le site intranet de l'établissement.

Elle est disponible dans la gestion documentaire.

ANNEXE 1 : REFERENCES LEGISLATIVES ET REGLEMENTAIRES

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.

Rappel des principales dispositions légales en la matière :

- la loi du 29 juillet 1881 modifiée sur la liberté de la presse ;
 - la loi n°78-17 du 6 janvier 1978 modifiée dite loi « Informatique et Libertés » ;
 - la législation relative aux atteintes aux systèmes de traitement automatisé de données (Notion de fraude informatique) (article 323-1 et suivants du code pénal) ;
 - la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
 - les lois Hadopi I (loi n° 2009-669 du 12 juin 2009) et Hadopi II (loi n° 2009-1311 du 28 octobre 2009) codifiées notamment dans le code de la propriété intellectuelle ;
- ainsi que toutes les autres dispositions du code de la propriété intellectuelle relative à la propriété littéraire et artistique.
- la loi Godfrain (loi n°88-19 du 05/01/1988) relative à la fraude informatique (réprime les actes de criminalité informatique et de piratage)
 - le règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données